

<p style="text-align: center;">Comité sectoriel de la sécurité sociale et de la santé Section “sécurité sociale”</p>
--

CSSS/12/089

RECOMMANDATION N° 12/01 DU 8 MAI 2012 RELATIVE À L'APPLICATION WEB DOLISIS

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, notamment son article 46, § 1^{er};

Vu le rapport d'auditorat de la Banque Carrefour de la sécurité sociale du 25 avril 2012;

Vu le rapport du président.

A. OBJET DE LA DEMANDE

1. Dans le cadre de divers contrôles et d'enquêtes antifraudes, les communautés et les régions ont besoin de moyens afin de pouvoir obtenir une communication électronique de données à caractère personnel, de façon sécurisée, efficace et uniforme à partir du réseau de la sécurité sociale.
2. Les services d'inspection fédéraux de la sécurité sociale utilisent à cette fin l'application GENESIS, une application web consultant directement les données à caractère personnel auprès de l'Office national de sécurité sociale ou auprès de l'Office national de sécurité sociale des administrations provinciales et locales (voir la délibération n° 04/44 du 7 décembre 2004). D'autres services d'inspection et d'administration ne peuvent plus se connecter à cette application, étant donné que l'échange de données à caractère personnel via GENESIS ne se déroule pas à l'intervention de la Banque Carrefour de la sécurité sociale.
3. La nouvelle application web DOLISIS a été développée afin de satisfaire aux besoins précités. Cette application qui est basée sur GENESIS, vise à optimiser la lutte contre la fraude et à harmoniser les moyens de fonctionnement des services d'inspection concernés.

4. Le groupe cible de DOLSIS comprend un nombre limité de services publics qui souhaitent demander certaines données à caractère personnel disponibles dans le réseau de la sécurité sociale et qui, vu le nombre limité de consultations, ne peuvent pas prévoir un développement propre pour l'intégration et la consultation via les flux standards et les services web.
5. Au sein du projet DOLSIS, le besoin de base actuel consiste à identifier un travailleur et un employeur et à recevoir un aperçu en ligne des données à caractère personnel actuelles relatives à l'occupation. Pour l'identification de personnes physiques, l'application renverra au Registre national des personnes physiques et/ou aux registres Banque Carrefour (subsidiaires et complémentaires). Pour l'occupation, il s'agit de données à caractère personnel de l'Office national de sécurité sociale et de l'Office national de sécurité sociale des administrations provinciales et locales, plus précisément de données à caractère personnel contenues dans le fichier du personnel des employeurs, le répertoire des employeurs, le cadastre LIMOSA et la banque de données DIMONA.
6. Il existe deux types d'utilisateurs de DOLSIS: d'une part, les services d'inspection et d'autre part, les services administratifs (à l'exception du personnel administratif de soutien qui travaille à la demande des services d'inspection).

Les utilisateurs qui recherchent des données à caractère personnel sur la base de l'identité de l'employeur et de l'identité du travailleur (typique pour les services d'inspection) peuvent effectuer des consultations relatives à des personnes physiques (via le nom et/ou le numéro d'identification de la sécurité sociale) et des consultations relatives à des personnes morales (via la dénomination et/ou le numéro d'entreprise). L'application web DOLSIS permet de naviguer, à partir d'un travailleur, d'un employeur vers un autre employeur. Une intégration préalable dans le répertoire des références de la Banque Carrefour de la sécurité sociale n'est pas requise pour les personnes physiques qui font l'objet d'une consultation.

Un deuxième type d'utilisateurs recherche uniquement des données à caractère personnel sur la base de l'identité de la personne physique (typique pour les services administratifs). A cette fin, une intégration préalable du dossier dans le répertoire des références de la Banque Carrefour de la sécurité sociale est requise. Sur la base du nom et/ou du numéro d'identification de la sécurité sociale, l'utilisateur peut consulter les données à caractère personnel spécifiques relatives à l'occupation et les données à caractère personnel relatives à l'identification de l'employeur y afférent. Ce type d'utilisateur ne peut pas demander, sur la base de l'identité de l'employeur, des données relatives à tous les travailleurs ou naviguer de façon libre. La consultation se limite aux données à caractère personnel utiles relatives aux personnes physiques concernées.

B. MESURES DE SÉCURITÉ

7. Pour l'accès (en ligne), deux moyens sont mis à la disposition des différents services.

D'une part, l'*application web DOLSI*S pour le service sans développement propre, qui permet de consulter des données à caractère personnel qui sont enregistrées dans le réseau de la sécurité sociale.

D'autre part, le *service web DOLSI*S, qui peut être appelé par l'application web DOLSI. Le service web est également mis à la disposition des utilisateurs finaux qui réalisent une présentation de données propre. Ensuite, il est intégré dans une application propre.

8. Ces communications de données à caractère personnel se dérouleront, à l'intervention de la Banque Carrefour de la sécurité sociale, conformément à l'article 14 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*.

La Banque Carrefour de la sécurité sociale coordonne les requêtes adressées aux différentes sources authentiques de données à caractère personnel. Chaque membre concerné du réseau de la sécurité sociale s'occupe de la coordination de ses sources de données à caractère personnel.

La réponse obtenue est traitée et filtrée par la Banque Carrefour de la sécurité sociale en fonction du destinataire des données à caractère personnel (certains destinataires ne peuvent, par exemple, pas disposer de toutes les données à caractère personnel de la DMFA disponibles) selon les autorisations spécifiques de la section sécurité sociale du Comité sectoriel de la sécurité sociale et de la santé.

9. L'application web DOLSI est disponible sur le site portail de la sécurité sociale, dans la partie destinée aux professionnels. En vue de la gestion intégrée des utilisateurs et des accès (identification, authentification et autorisation), il est fait appel aux services de base, tels qu'ils ont été élaborés pour le portail de la sécurité sociale grâce au système du « *user and access management* » (UAM) destiné aux professionnels. L'utilisateur doit s'authentifier de manière univoque à l'aide du certificat d'authentification présent sur sa carte d'identité électronique (il se connecte au portail à l'aide de sa carte d'identité électronique). Après une authentification réussie et un contrôle positif des autorisations via le système UAM du portail de la sécurité sociale, l'application web DOLSI fait appel au service web DOLSI sous-jacent.

La protection au niveau du transport est assurée par l'utilisation du HTTPS via "*two-way SSL*" (pour l'authentification du client et du serveur).

Si l'entité concernée souhaite utiliser une application web propre pour l'affichage du service web DOLSI, les mêmes mesures de sécurité qui s'appliquent à l'application web DOLSI, doivent au moins être respectées: une authentification forte de l'utilisateur (au moyen de la carte d'identité électronique), une connexion sécurisée au service web DOLSI ("*two-way SSL*"), une vérification de l'autorisation via l'UAM et la garantie de la conservation de fichiers journaux (voir infra).

La documentation permettant d'évaluer la sécurité de l'application web développée par l'entité concernée, doit toujours être tenue à la disposition de la section sécurité sociale du Comité sectoriel de la sécurité sociale et de la santé.

10. Un conseiller en sécurité de l'information doit être désigné auprès de l'entité concernée. Ce conseiller en sécurité de l'information est chargé, en vue de la sécurité des données à caractère personnel qui sont traitées par son mandataire et en vue de la protection de la vie privée des personnes auxquelles ces données à caractère personnel ont trait, de fournir des avis qualifiés à la personne chargée de la gestion journalière et d'exécuter les missions qui lui ont été confiées par cette dernière. Il a une mission de conseil, de stimulation, de documentation et de contrôle en matière de sécurité de l'information.

Il remplit également la fonction de préposé à la protection des données, visé à l'article 17bis 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*.

Il est par ailleurs chargé de l'exécution de la politique en matière de sécurité de l'information de son mandataire. Le cas échéant, il peut avoir recours à cette fin au document « *Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel* » de la Commission de la protection de la vie privée.

11. L'entité concernée doit par ailleurs tenir compte des normes minimales de sécurité qui ont été définies par le Comité général de coordination de la Banque Carrefour de la sécurité sociale et qui ont été approuvées par le Comité sectoriel de la sécurité sociale et de la santé.
12. Il doit ressortir des pièces communiquées par le demandeur que l'entité concernée dispose d'une politique en matière de sécurité de l'information et que cette politique est dans la pratique aussi mise en œuvre sur le terrain. Il y a lieu d'accorder suffisamment d'attention à la sensibilisation relative à la problématique de la sécurité et aux formations nécessaires relatives à la sécurité de l'information.
13. En ce qui concerne la procédure d'identification et d'authentification, il doit ressortir du dossier communiqué quel type d'infrastructure est utilisé. Il convient de faire une distinction à cet égard entre d'une part, le poste de travail (tant des ordinateurs fixes que des ordinateurs portables) disposant d'une connexion physique directe au réseau interne de l'entité concernée, et d'autre part, les ordinateurs portables sans connexion directe (une connexion via VPN), en vue d'accéder aux banques de données à caractère personnel du réseau de la sécurité sociale.
14. Le télétravail (c'est-à-dire, la possibilité de se connecter à distance au réseau interne de l'entité concernée, souvent à partir de l'endroit où la mission de surveillance est exercée) et l'utilisation d'un ordinateur portable constituent deux facteurs essentiels du mode de travail des services d'inspection. Les services administratifs peuvent aussi offrir le télétravail comme méthode de travail à leur personnel.
15. Dans le cadre du développement d'une politique de sécurité de l'information commune, le groupe de travail Sécurité de l'information du Comité général de coordination a rédigé et approuvé plusieurs polices de sécurité concernant les principaux domaines suivants: "Politique

de sécurité pour les ordinateurs portables”, “Politique pour la protection des postes de travail” et “Politique d’accès à distance – Politique technique pour les institutions clientes et les utilisateurs finaux”.

16. Le Comité sectoriel de la sécurité sociale et de la santé insiste sur la nécessité d’appliquer les règles qui ont été formulées par le groupe de travail Sécurité de l’information dans la police “Politique pour la protection des postes de travail” lorsqu’il est fait usage d’un poste de travail (tant des ordinateurs personnels fixes que des ordinateurs portables) qui est ou non relié au réseau de la sécurité sociale.
17. Le Comité sectoriel de la sécurité sociale et de la santé insiste également sur la nécessité pour l’entité concernée, en cas d’usage d’un ordinateur portable qui est ou non relié au réseau de la Banque Carrefour de la sécurité sociale, d’appliquer les règles qui ont été formulées par le groupe de travail Sécurité de l’information, notamment les règles suivantes:
 - l’ordinateur portable et ses périphériques qui sont mis à la disposition de l’utilisateur dans le cadre de ses activités professionnelles sont la propriété de l’institution concernée et le restent;
 - lorsqu’il quitte l’institution ou change de fonction, l’utilisateur doit restituer l’ordinateur portable et les périphériques qui ont été mis à sa disposition;
 - sauf autorisation explicite de la personne chargée de la gestion journalière de l’institution et moyennant le respect des conditions complémentaires prévues dans la police "Politique d'accès à distance - Politique technique pour les institutions clientes et les utilisateurs finaux", seul l'utilisateur désigné peut utiliser l'ordinateur portable et les périphériques mis à sa disposition, même s'il n'est pas fait usage d'une connexion au réseau;
 - il est interdit à l’utilisateur de connecter d’autres périphériques que ceux qui ont été fournis en même temps que l’ordinateur portable, sans le consentement explicite du service compétent;
 - la mise à la disposition d’un ordinateur portable à un utilisateur ne signifie pas qu’il recevra davantage de droits d’accès que ceux lui attribués dans le cadre de l’usage d’un ordinateur personnel fixe. Ceci vaut tant pour l’accès aux applications que pour l’usage du courriel et d’Internet ou de toute autre fonctionnalité. Cependant, des mesures peuvent être prises afin de modifier les droits d’accès;
 - afin de garantir la sécurité du matériel lui confié, l’utilisateur doit agir en tant que bon père de famille et mettre tout en œuvre pour sécuriser le matériel et les données informatiques. La police fixe à cet effet des règles très strictes;
 - l’utilisateur doit notamment éviter de laisser son ordinateur portable sans surveillance. Il est recommandé de le conserver sous clé dans une armoire ou un bureau. Lorsqu’il quitte temporairement le local dans lequel son ordinateur portable est actif,

l'utilisateur doit verrouiller son ordinateur portable ou activer le screensaver avant de quitter le local;

- en cas de perte ou de vol, l'utilisateur doit immédiatement avertir le service compétent de son institution et suivre les directives;
 - sauf avis contraire de la personne chargée de la gestion journalière, seul le service compétent est chargé de l'installation et de la maintenance d'un logiciel sur l'ordinateur portable ou de sa configuration;
 - les règles en matière de définition, de fréquence des modifications et de mode d'enregistrement des moyens d'authentification (par exemple, mot de passe) doivent être appliquées strictement;
 - les données à caractère personnel sensibles doivent être enregistrées dans le réseau, ou respecter les règles qui sont définies dans la policy "Politique d'accès à distance – politique technique pour les institutions clientes et les utilisateurs finaux". En toute hypothèse, il y a lieu d'éviter de sauvegarder les données à caractère personnel sensibles sur l'ordinateur portable et il y a lieu de les enregistrer, dans les plus brefs délais, dans le réseau;
 - les données à caractère personnel sensibles peuvent uniquement être conservées de manière cryptée sur l'ordinateur portable et sur ses périphériques. Si le périphérique (par exemple, clé USB) ne permet pas un enregistrement chiffré, l'enregistrement de données à caractère personnel sur ce périphérique est explicitement interdit;
 - les données à caractère personnel du portable sont enregistrées (back-up) selon la stratégie qui a été fixée pour l'usage d'ordinateurs personnels fixes. Seules les données du réseau sont enregistrées de manière automatique. Une attention toute particulière doit être consacrée au back-up du disque local.
- 18.** En ce qui concerne l'usage d'un ordinateur personnel fixe dans un bâtiment de l'institution, l'entité concernée ne peut, en aucun cas, déroger aux règles applicables et doit s'en tenir à la politique qui a été définie dans les normes minimales de sécurité du réseau de la Banque Carrefour de la sécurité sociale, qui prévoit notamment dans son chapitre "*Protection de l'accès logique*" que toute instance connectée au réseau de la Banque Carrefour de la sécurité sociale doit sécuriser l'accès aux données à caractère personnel nécessaires à l'exécution de ses missions par un système d'identification, d'authentification et d'autorisation.
- 19.** La section sécurité sociale du Comité sectoriel de la sécurité sociale et de la santé insiste également sur la nécessité pour l'entité concernée, en cas d'usage d'un ordinateur portable à partir d'un endroit externe (donc pas de connexion physique directe possible avec le réseau), d'appliquer les règles qui ont été formulées par le groupe de travail Sécurité de l'information, notamment les règles suivantes:

Politique au niveau du système

- L'usage d'un protocole VPN est obligatoire lors de toute connexion avec le réseau local de l'entité concernée en vue de la consultation des banques de données à caractère personnel concernées;
- Le système VPN utilisé doit au moins satisfaire aux conditions de sécurité telles que décrites dans la police de sécurité rédigée par le groupe de travail Sécurité de l'information "Politique d'accès à distance – Politique technique pour les institutions clientes et les utilisateurs finaux";
- Le service chargé de la gestion des ordinateurs personnels doit prendre l'initiative d'un contrôle régulier des ordinateurs portables afin de vérifier le respect de la configuration, y compris la configuration du logiciel de sécurité. En cas de non-respect, la hiérarchie de l'utilisateur ou du service compétent pour la gestion des ordinateurs personnels doit établir un rapport à l'attention du service de sécurité de l'institution sur des dommages éventuels pour ce dernier.

Politique pour les utilisateurs finaux

- Il y a lieu de respecter les différents niveaux d'authentification tels que fixés dans la police de sécurité "Politique d'accès à distance – Politique technique pour les institutions clientes et les utilisateurs finaux";
 - Il y a également lieu d'observer la recommandation relative à la protection des données à caractère personnel.
 - La configuration de l'ordinateur portable doit obligatoirement comprendre les différents outils de sécurité requis dans la politique de sécurité "Politique d'accès à distance – Politique technique pour les institutions clientes et les utilisateurs finaux" et doit intégralement respecter les règles fixées concernant l'installation, la configuration, le contrôle de la version du logiciel et l'usage de ces outils.
 - Les règles en matière d'usage des périphériques doivent être respectées.
 - L'entité concernée doit veiller à ce que les inspecteurs et les collaborateurs administratifs concernés suivent une formation appropriée sur l'usage de leur ordinateur portable à l'occasion de laquelle les risques de sécurité leur sont expliqués.
20. Il y a lieu de déduire du dossier introduit que la situation auprès de l'entité en question est conforme aux conditions d'utilisation d'un ordinateur personnel fixe ou d'un ordinateur portable qui est ou non connecté au réseau de la Banque Carrefour de la sécurité sociale.
21. En ce qui concerne l'entité concernée, il y a lieu d'attirer son attention sur le fait qu'elle doit informer le comité sectoriel et lui fournir de la documentation en cas d'évolution vers de nouvelles techniques ou de nouveaux modes d'accès aux banques de données à caractère personnel du réseau de la sécurité sociale, dans le cadre des travaux de ses services d'inspection et/ou de ses services administratifs.

22. L'application web DOLSIS conserve des fichiers journaux contenant, par communication, une indication de quelle personne a obtenu quelles données à caractère personnel, concernant quelle personne, à quel moment et pour quelle finalité.

Ces fichiers journaux sont accessibles via l'application portail IRIS. L'accès à ces fichiers journaux requiert une authentification forte au moyen de la carte d'identité électronique.

Lorsque l'entité concernée utilise une application web qu'elle a développée, elle doit prévoir un système similaire de fichiers journaux.

23. Ces fichiers journaux seront conservés pendant dix ans au moins, en vue du traitement de plaintes éventuelles ou de la constatation d'irrégularités éventuelles en ce qui concerne le traitement des données à caractère personnel.

Les fichiers journaux mêmes doivent être protégés au moyen de mesures garantissant la confidentialité, l'intégralité et la disponibilité.

Ils sont transmis au Comité sectoriel de la sécurité sociale et de la santé et à la Banque Carrefour de la sécurité sociale à leur demande.

24. Le Comité sectoriel de la sécurité sociale et de la santé souligne le rôle du conseiller en sécurité de l'information de l'entité concernée, qui doit veiller à s'assurer que les moyens techniques mis à la disposition des inspecteurs et/ou des services administratifs soient conformes, d'une part, aux polices de sécurité élaborées par le groupe de travail Sécurité de l'information du Comité général de coordination, et, d'autre part, à la politique de sécurité de l'information spécifique de l'entité concernée.
25. C'est pourquoi le conseiller en sécurité de l'information de l'entité concernée veillera à l'application stricte des politiques de sécurité relatives à l'utilisation d'un ordinateur portable, au télétravail (accès à distance), à l'utilisation du courrier électronique et d'Internet, à l'utilisation de moyens d'authentification et à l'activation, la conservation et l'archivage des fichiers journaux garants de la traçabilité des accès.
26. Par ailleurs, le conseiller en sécurité veillera, si non encore existant, à mettre en place l'organisation d'un processus qui l'assure d'être informé:

- sur l'application correcte des mesures communiquées au Comité sectoriel de la sécurité sociale et de la santé, en cas d'absence de longue durée ou de départ d'un inspecteur;
- sur l'inventaire et l'état des lieux du parc informatique et du matériel connexe mis à la disposition des inspecteurs et du personnel administratif de soutien;
- sur les incidents propres à l'utilisation des ordinateurs portables et du matériel connexe;
- sur l'utilisation adéquate, au sein du service d'inspection concerné, des autorisations accordées en fonction des besoins réels de chaque inspecteur.

C. PROCÉDURE DE CONTRÔLE

27. Un fichier journal garantit l'intégrité des utilisateurs du réseau de la Banque Carrefour de la sécurité sociale. Il est dès lors primordial de toujours pouvoir justifier les notions "qui", "quoi" et "quand" et de pouvoir confronter, dans le contexte des inspecteurs, ces informations aux rapports de missions.

Afin de garantir au Comité sectoriel un usage légitime des autorisations accordées dans le cadre des consultations par les services d'inspection qui ne requièrent pas une intégration préalable dans le répertoire des références de la Banque Carrefour de la sécurité sociale, une procédure de contrôle spécifique est prévue pour les services d'inspection concernés, par analogie aux services fédéraux d'inspection sociale (voir la délibération n° 04/32 du 5 octobre 2004). Ce contrôle aura lieu dans deux contextes bien précis.

28. *Dans le cadre d'une procédure automatique de suivi des rapports de missions et du respect des principes de finalité et de proportionnalité.*

Les contrôles ont trait aux consultations effectuées au fil du temps dans les banques de données à caractère personnel, soit par les inspecteurs du service d'inspection concerné (à partir de différents endroits), soit par le personnel administratif de soutien des inspecteurs à la demande de ce dernier (au bureau dans le bâtiment de l'entité concernée, pendant les heures de travail ou via télétravail).

Sur la base d'un pourcentage significatif de dossiers traités, la probité dans la démarche suivie par l'inspecteur sera contrôlée. A cette fin, dans le cadre d'un processus organisé en concertation avec son conseiller en sécurité de l'information, le service d'inspection concerné demandera d'extraire, selon le mode de travail utilisé, dans les fichiers journaux, les données de journalisation pour un nombre déterminé de dossiers pertinents de l'inspecteur en question. Il comparera ensuite les résultats obtenus avec les différents rapports de missions et vérifiera la légitimité des consultations effectuées, eu égard aux autorisations accordées par le Comité sectoriel. Par « dossiers significatifs », il y a lieu d'entendre les dossiers qui s'étalent sur différentes périodes de l'année, différents dossiers confiés à différents inspecteurs et des dossiers représentatifs pour les autorisations accordées, les données à caractère personnel consultées et les missions du service.

29. *Dans le cadre d'un incident ou d'une plainte.*

Toutes les plaintes ou incidents doivent faire l'objet d'un contrôle spécifique. Par incident, on entend tout évènement majeur dans l'activité d'un inspecteur tel que la non-transmission de ses rapports de missions, la perte, le vol ou l'inutilisation définitive de son PC portable ou de tout matériel sensible qui lui est confié dans le cadre de sa fonction.

Différents scénarios sont possibles:

- sur base du numéro d'identification de l'inspecteur ou d'un agent administratif de soutien, analyser les données de journalisation relatives à une période d'inactivité (congé ou maladie). Sauf dérogation ou justification, le résultat devrait être nul.

- sur la base du numéro d'identification de l'inspecteur ou d'un agent administratif de soutien, analyser les données de journalisation relatives à la semaine qui précède et qui suit la disparition de son ordinateur personnel ou de son token d'accès et confronter le résultat aux rapports de missions. Dans le cas d'une plainte, il y a lieu de confronter le contenu des données de journalisation aux éléments fournis par le plaignant et aux rapports de missions.

30. Annuellement et au plus tard pour le 28 février (tout retard dans l'introduction du rapport annuel devant faire l'objet d'un avis et d'une demande de dérogation écrite auprès du Comité sectoriel), le service d'inspection concerné transmet au Comité sectoriel, par un courrier à la signature du fonctionnaire dirigeant, un rapport succinct précisant les informations suivantes:

31. *Généralités.*

Il y a lieu de fournir à la section Sécurité sociale du Comité sectoriel de la sécurité sociale et de la santé un tableau de bord reprenant les éléments suivants:

- le nombre de collaborateurs du service d'inspection concerné auquel s'applique l'autorisation accordée;
- les mouvements du personnel (nombre d'entrées et de sortie) au sein du service durant l'année écoulée;
- le nombre d'accès réalisés, à fournir par le service informatique chargé de la tenue des fichiers journaux;
- le nombre de recherches dans les fichiers journaux concernant le suivi des dossiers et le respect des règles de finalité et de proportionnalité;
- le nombre d'incidents et de plaintes et les recherches dans les fichiers journaux concernés.

32. *Rapport sur les contrôles d'accès.*

Le service d'inspection concerné informe le Comité sectoriel de la sécurité sociale et de la santé, dans un format libre, sur le résultat de la confrontation aux rapports de missions, des différentes recherches réalisées dans les fichiers journaux. Sont décrits, dans un chapitre spécifique, les investigations réalisées dans le cadre de plaintes ou d'incidents et les résultats obtenus dans le cadre de plaintes ou d'incidents ainsi que les éventuelles sanctions prises.

Dans ses conclusions, le service d'inspection concerné informe le Comité sectoriel sur les mesures éventuelles qui ont été mises en place pour améliorer le contrôle au sein du service.

Le rapport indiquera également pour chaque banque de données sociales concernée son taux d'utilisation (quelle est le pourcentage de la consultation d'une banque de données déterminée par rapport à l'ensemble des consultations de banques de données tombant sous l'application de la délibération).

Par ces motifs,

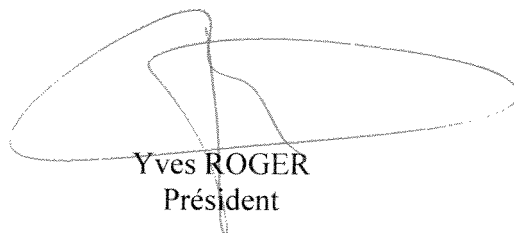
la section sécurité sociale du Comité sectoriel de la sécurité sociale et de la santé

décide

que toute instance qui souhaite accéder via DOLSIS aux données à caractère personnel qui sont enregistrées dans le réseau de la sécurité sociale doit introduire une demande d'autorisation spécifique auprès du Comité sectoriel de la sécurité sociale et de la santé, qui contient une liste des données à caractère personnel et qui mentionne explicitement la finalité

et

qu'une autorisation ne peut être accordée que dans la mesure où les mesures de sécurité précitées soient respectées et à condition que l'instance concernée soit autorisée à accéder au Registre national des personnes physiques et à utiliser le numéro d'identification du Registre national des personnes physiques.



Yves ROGER
Président

Le siège du Comité sectoriel de la sécurité sociale et de la santé est établi dans les bureaux de la Banque Carrefour de la sécurité sociale, à l'adresse suivante: chaussée Saint-Pierre 375 - 1040 Bruxelles (tél. 32-2-741 83 11)

