24 octobre 2006

Règlement à l'usage des utilisateurs en vue de l'accès et de l'utilisation du système informatique de l' Etat fédéral et des institutions publiques de sécurité sociale par les entreprises et leurs mandataires

Article 1er - Champ d'application

Ce règlement à l'usage des utilisateurs régit l'accès au système informatique de l'Etat fédéral et des institutions publiques de sécurité sociale (appelé ci-après Système d'Information) et son utilisation par les entreprises et leurs mandataires, en ce compris les Services que ce système dispense.

Article 2 – Désignation obligatoire d'un gestionnaire local

Toute entreprise qui souhaite accéder au Système d'Information et l'utiliser doit désigner un seul et unique gestionnaire.

Article 2 bis - Définition

Par Carte d'Identité Electronique au sens du présent règlement, il est entendu la carte d'identité électronique, visée par les articles 6 et suivants de la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, sur laquelle les certificats d'identité et de signature sont activés.

Article 3 - Services dispensés et canaux disponibles

Les services dispensés sont accessibles par différentes voies :

1. Tous les utilisateurs ont la possibilité d'effectuer une déclaration Dimona par le serveur vocal.

2. Via le site-portail de la sécurité sociale (www.securitesociale.be)

   a) tous les utilisateurs ont accès aux applications "Dimona", "Demandes de détachement" (Gotot), "Déclaration de travaux", "Obligation de retenue 30bis", "Formulaire électronique de demande d'accès" et "Consultation publique du répertoire des employeurs" ;

   b) chaque utilisateur désigné par une entreprise en tant que gestionnaire local et disposant d'un Nom d'Utilisateur et d'un Mot de Passe a accès à l'application "Routing Consult" ;

c) chaque curateur qui est désigné en tant que gestionnaire local ou chaque utilisateur désigné par ce curateur et qui dispose d'un Nom d'Utilisateur et d'un Mot de Passe a accès à l'application "WEBCUR" ;

d) chaque utilisateur désigné par une entreprise en tant que gestionnaire local et disposant d'un Nom d'Utilisateur et d'un Mot de Passe a accès, soit après l'introduction de ceux-ci, soit sans leur introduction s'il utilise une Carte d'Identité Electronique, aux applications "Consultation de l'e-Box", "Fichier du personnel", "Déclaration-ONSS (DMFA)", "Déclaration-ONSSAPL (DmfAPPL)", "Déclaration risque social (DRS)", "Consultation déclarations de travail", "Chômage temporaire et livre de validation", "Consultation sécurisée du répertoire des employeurs", "Cotisations pour les mandats publics", "Règles de routage" et "Consultation du fichier des vacances" ;

e) chaque utilisateur qui est désigné par le gestionnaire local d'une entreprise et qui dispose soit d'un Nom d'Utilisateur et d'un Mot de Passe, soit d'une Carte d'Identité Electronique a accès aux applications à l'utilisation desquelles il a été habilité par le gestionnaire local d'une entreprise, sans pour autant que cet accès puisse être plus large que celui réservé au gestionnaire local lui-même;

f) chaque utilisateur qui est désigné par une entreprise en tant que gestionnaire local ou désigné par le gestionnaire local d'une entreprise et qui dispose soit d'un Nom d'Utilisateur, d'un Mot de Passe, d'une Clé Privée, d'un Certificat qualifié au sens de l'article 2, 4° de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification ou de tout autre type de certificat qui figure sur la liste des certificats acceptés publiée sur le site-portail de la sécurité sociale, soit d'une Carte d'Identité Electronique, a par ailleurs accès aux applications "Modification d'une déclaration-ONSS (DMFA)" et "Modification d'une déclaration-ONSSAPL (DmfAPPL)".

3. Via le site-portail de l'autorité fédérale (www.belgium.be)

a) tous les utilisateurs ont accès à l'application 'consulter les données des entreprises';

b) chaque utilisateur désigné par une entreprise en tant que gestionnaire local et disposant d'un Nom d'Utilisateur et d'un Mot de Passe a accès aux applications "Consulter des données de mon entreprise", "Enquête de mobilité domicile – travail", "Fonds Online", "Vigilis (e-guichet)" et "La Déclaration Unique pour les Starters (DEUS)" ;

c) chaque utilisateur désigné par une entreprise en tant que gestionnaire local et disposant d'un Nom d'Utilisateur, d'un Mot de Passe et du numéro du répertoire du mandant a accès aux applications 'Tax-on-web" (TOW) et "Consultation de la déclaration Tax-on-web" pour les personnes pour lesquelles il dispose d'un mandat afin d'utiliser ces applications pour leur compte et en leur nom et dont il a mis ce mandat à la disposition de la direction régionale des contributions directes compétente pour le bureau de taxation du mandant ;

d) chaque utilisateur qui est désigné par le gestionnaire local d'une entreprise et qui dispose d'un Nom d'Utilisateur et d'un Mot de Passe et, en ce qui concerne les applications mentionnées au point 3 c), du numéro du répertoire du mandant a accès aux applications qu'il a été autorisé à utiliser par le gestionnaire local d'une entreprise

sans pour autant que cet accès puisse être plus large que celui réservé au gestionnaire local lui-même ;

e) chaque utilisateur qui est désigné par une entreprise en tant que gestionnaire local ou désigné par le gestionnaire local d'une entreprise et qui dispose d'un Nom d'Utilisateur, d'un Mot de Passe, d'une Clé Privée et d'un Certificat qualifié au sens de l'article 2, 4° de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification ou de tout autre type de certificat qui figure sur la liste des certificats acceptés publiée sur le site-portail de la sécurité sociale, a par ailleurs accès aux applicationx "Belcotax-on-web" et "PLDA – Paperless Douane en Accijnzen".

4. Par le biais du système de transmission de fichiers en (S)FTP, à l'aide de MQSeries ou d'autres canaux acceptés, chaque utilisateur qui est désigné par une entreprise en tant que gestionnaire local ou par un gestionnaire local et qui dispose d'un Nom d'Utilisateur, d'un Mot de Passe, d'une Clé privée et d'un Certificat qualifié au sens de l'article 2, 4° de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification ou de tout autre type de certificat qui figure sur la liste des certificats acceptés publiée sur le site- portail de la sécurité sociale, dont le certificat de signature activé de la Carte d'Identité Electronique, peut effectuer des "Déclarations Dimona", des "Déclarations-ONSS (DMFA)", des "Déclarations-ONSSAPL (DmfAPPL)", des "Demandes de détachement (Gotot)", des "Modifications d'une déclaration-ONSS (DMFA)", des "Modifications d'une déclaration-ONSSAPL (DmfAPPL)" et des "Déclarations de risques sociaux (DRS) ".

La teneur des services et l'accès à ces services peuvent être modifiés à tout moment.

Article 4 – Accès au Système d'Information

L'utilisateur a accès au Système d'Information, sans qu'il soit pour autant garanti que cet accès et celui aux services offerts soient assurés en tout temps et qu'ils ne soient entachés d'aucune erreur ou ne s'accompagnent d'éventuelles difficultés techniques.

L'accès au Système d'Information et aux Services dispensés par le biais du système peut, à tout moment, être complètement ou partiellement interrompu (notamment pour des raisons d'entretien). Dans les limites du raisonnable, l'utilisateur sera informé préalablement d'une telle interruption.

L'utilisateur est responsable de la mise à disposition et de la maintenance du Terminal nécessaire à l'utilisation du Système d'Information. Les fournisseurs d'accès du Système d'Information ne sont pas responsables du Terminal ni de l'utilisation qui en est faite et ils ne sont pas tenus d'en assurer le support sous quelque forme que ce soit.

Article 5 – Usage du Nom d'Utilisateur et du Mot de Passe

Un utilisateur désigné par une entreprise en tant que gestionnaire local reçoit son Nom d'Utilisateur et son Mot de Passe dans des messages séparés, envoyés par Eranova, le Centre de Contact des institutions publiques de sécurité sociale. Un utilisateur qui n'a pas été désigné

comme gestionnaire local par une entreprise se voit attribuer son Nom d'Utilisateur et son Mot de Passe par le Gestionnaire local d'une entreprise.

Le Nom d'Utilisateur et le Mot de Passe sont strictement personnels et intransmissibles.

Chaque utilisateur est tenu de modifier le plus rapidement possible après réception ou du moins au moment de la première utilisation, le Mot de Passe qu'il s'est vu attribuer par le Centre de Contact des institutions publiques de sécurité sociale ou par un gestionnaire local. Ensuite, chaque Utilisateur devra modifier régulièrement son Mot de Passe.

Un Mot de Passe sécurisé est composé de 15 signes et contient des caractères et des symboles alphanumériques placés dans un ordre difficile à déceler. Chaque utilisateur doit veiller à ce que le Mot de Passe choisi réponde à ces conditions. La responsabilité de chaque utilisateur est engagée lorsqu'un Mot de Passe qui n'a pas été composé en respectant ces règles, est décelé et/ou utilisé de manière illicite.

Il appartient à chaque utilisateur de faire un usage judicieux de ses Noms d'Utilisateur et Mot de Passe et d'assurer le secret en ce domaine. Chaque utilisateur assume la responsabilité de tout usage approprié ou non de ses Nom d'Utilisateur et Mot de Passe, en ce compris l'usage par des tiers.

Lorsqu'un utilisateur est au courant de la perte de son Nom d'Utilisateur et/ou Mot de Passe ou d'une quelconque utilisation inappropriée de son Nom d'Utilisateur et/ou Mot de Passe par des tiers ou lorsqu'il soupçonne une telle perte ou utilisation inappropriée, il doit prendre immédiatement toutes les mesures nécessaires.

Tout utilisateur qui est désigné par une entreprise en tant que gestionnaire local doit, entre autres, signaler immédiatement cette perte ou cette utilisation inappropriée au Centre de Contact des institutions publiques de sécurité sociale, Eranova (02/511.51.51 ou par le site-portail de la sécurité sociale (www.securitesociale.be)). Dans les plus brefs délais de la réception de cette communication et dans les limites du raisonnable, tout sera mis en œuvre pour rendre le Nom d'Utilisateur et le Mot de Passe de l'utilisateur inactifs.

Tout utilisateur qui n'est pas désigné par une entreprise comme gestionnaire local est tenu, entre autres, de signaler immédiatement cette perte ou cet usage inapproprié au gestionnaire local dont il a reçu le Nom d'Utilisateur ou le Mot de Passe. Dès réception de ce message, ce dernier doit, dans les limites du raisonnable, mettre tout en œuvre pour rendre inactif le Nom d'Utilisateur et le Mot de Passe de l'utilisateur.

Chaque utilisateur continue à assumer la responsabilité de tout dommage (direct ou indirect) causé par l'utilisation (appropriée ou non) de son Nom d'utilisateur et/ou de son Mot de Passe avant l'inactivation du Nom d'Utilisateur et du Mot de Passe.

En cas de blocage du Nom d'Utilisateur et/ou du Mot de Passe, l'Utilisateur désigné par une entreprise comme gestionnaire local doit demander par écrit un nouveau Nom d'Utilisateur et un nouveau Mot de Passe auprès de Eranova, Centre de Contact des institutions publiques de sécurité sociale. Ensuite, un nouveau Nom d'Utilisateur et un nouveau Mot de Passe sont fournis.

Article 6 – Utilisation du Système d'Information

En ce qui concerne l'utilisation du Système d'Information et des Services dispensés via ce système, chaque utilisateur :

1. doit fournir des informations qui sont complètes, exactes et véritables et qui ne sont pas susceptibles d'induire en erreur;
2. doit respecter les prescriptions prescrites par voie de loi, de règlement, de décret, d'ordonnance ou d'arrêté pris par les instances fédérales, régionales, locales ou internationales;
3. doit s'abstenir de manipuler les informations fournies, et ce de quelque manière que ce soit ou en recourant à une technique quelconque;
4. ne peut, via le Système d'Information, envoyer aucune donnée, ni avis, ni document de quelque manière que ce soit, ni charger des données ou des documents par ce biais :
   a) opérations qui porteraient atteinte aux droits (dont les droits de la personnalité ou de la propriété intellectuelle) de tiers ou des fournisseurs du Système d'Information;
   b) dont le contenu est illicite, source de dommages, diffamatoire, violent, obscène ou déshonorant ou qui porte atteinte à la vie privée de tiers;
   c) dont l'utilisation ou la possession par l'utilisateur est interdite par la loi ou par convention;
   d) qui contiennent des virus ou des instructions susceptibles de causer des dommages aux fournisseurs du Système d'Information et/ou au Système d'Information et qui pourraient mettre en péril ou perturber les services dispensés par le biais du Système d'Information.

Article 7 – Utilisation du certificat

L'accès de l'utilisateur à certains services suppose soit l'utilisation d'une Carte d'Identité Electronique, soit, outre l'utilisation d'un Nom d'Utilisateur et d'un Mot de Passe, celle d'une Clé privée et d'un Certificat qualifié au sens de l'article 2, 4°, de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification ou de tout autre type de certificat qui figure sur la liste des certificats acceptés publiée sur le site-portail de la sécurité sociale.

Un même certificat peut être utilisé pour l'authentification et pour l'apposition d'une signature électronique visée à l'article 1322, alinéa 2, du Code civil. Cependant, dans l'hypothèse de l'accès aux services dispensés via une Carte d'Identité Electronique, l'authentification est réalisée par le certificat d'identité de la Carte et la signature électronique est apposée via le certificat de signature de la Carte.

Dès le moment de la création des données afférentes à la création de signature, le titulaire du certificat est seul responsable de la confidentialité de ces données. En cas de doute quant au maintien de la confidentialité des données afférentes à la création de signature ou de perte de conformité à la réalité des informations contenues dans le certificat, le titulaire est tenu de faire révoquer le certificat. Lorsqu'un certificat est arrivé à échéance ou a été révoqué, le titulaire de celui-ci ne peut, après l'expiration du certificat ou après révocation, utiliser les données afférentes à la création de signature correspondantes pour signer ou faire certifier ces données par un autre prestataire de service de certification.

Tout utilisateur doit donc user judicieusement de la Clé privée et du Certificat ainsi que du Mot de Passe éventuel nécessaire à l'utilisation de la Clé privée et du Certificat. L'utilisateur est responsable de tout usage approprié ou non de la Clé et du Certificat, en ce compris toute utilisation par des tiers. L'utilisateur doit conserver la Clé privée et le Certificat sur un support sécurisé, de préférence une carte à puce qui ne permet pas d'exporter la Clé privée.

Le Système d'Information est en mesure de valider des certificats et des types délivrés par les autorités de certification qui figurent dans la liste publiée sur le site-portail de la sécurité sociale (www.securitesociale.be). Les certificats délivrés par d'autres autorités de certification ne peuvent être acceptés que dans la mesure où les adaptations nécessaires à la validation de ces certificats auront été apportées au Système d'Information. Un utilisateur souhaitant à tout prix utiliser un certificat qualifié au sens de l'article 2 de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, qui a été délivré par une autorité de certification différente de celles mentionnées dans le site-portail de la sécurité sociale, peut en faire la demande en faisant usage de son Nom d'Utilisateur et son Mot de Passe par le biais du formulaire réservé à cet effet sur le site-portail de la sécurité sociale. Dans les limites du raisonnable et pour autant que l'autorité de certification en question apporte sa nécessaire collaboration, tout sera mis en œuvre pour que le Système d'Information valide également les certificats de l'autorité de certification susvisée. Une fois ces opérations réalisées, les certificats de l'autorité de certification en question pourront être utilisés.

Article 8 – Utilisation des signatures électroniques et justification (les utilisateurs titulaires d'un certificat).

Les messages envoyés via le Système d'Information par l'utilisateur qui dispose soit d'un Certificat qualifié au sens de l'article 2, 4° de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification ou de tout autre type de certificat qui figure sur la liste des certificats acceptés publiée sur le site-portail de la sécurité sociale, soit d'une Carte d'Identité Electronique, sont accompagnés d'une signature électronique visée à l'article 1322, alinéa 2, du Code civil.

L'utilisateur reconnaît expressément que tous les messages qui sont envoyés par le Système d'Information et qui sont accompagnés d'une signature électronique ont la même force probante qu'un acte sous seing privé au sens du Code civil.

L'utilisateur reconnaît expressément que toutes les informations relatives à des messages et sauvegardées par les fournisseurs du Système d'Information de manière durable et sans qu'elles puissent être modifiées, ont la même force probante qu'un acte sous seing privé au sens du Code civil, et ce jusqu'à preuve du contraire.

L'utilisateur reconnaît expressément comme étant la sienne la signature qui a été apposée sur la base de la clé privée et du certificat qui lui a été attribué, sauf en cas d'abus, de perte ou de vol, pour autant que la procédure spécialement prévue à cet effet ait été respectée.

Article 9 – Obligation de contrôle de l'utilisateur

L’utilisateur est responsable du contrôle du contenu des messages qu’il a envoyés par le Système d’Information et de leur suivi dans le cadre des messages qui sont transmis par les fournisseurs du Système d’Information à l’utilisateur et qui ont trait au(x) message(s) envoyé(s) par l’utilisateur.

L'erreur (les erreurs) matérielle(s) contenue(s) dans un message envoyé par l’utilisateur, dans un accusé de réception y afférent ou dans tout autre message ou document qui a trait à l’utilisateur et qui est accessible par le Système d’Information, est (sont) rectifiée(s) à la demande de l’utilisateur par le biais d’une procédure de rectification prévue à cet effet.

Article 10 – Propriétés intellectuelles

L’utilisateur reconnaît et accepte que le Système d’Information et les services ainsi que le logiciel développé pour ce Système d’Information et ces services sont protégés par des droits en matière de propriété intellectuelle (droits d’auteur, droit des marques, droit de brevet, etc.) qui appartiennent aux fournisseurs du Système d’Information (ou à leurs fournisseurs de brevet).

L’utilisateur bénéficie du droit non-exclusif d’utiliser le Système d’Information aux fins stipulées dans le règlement à l’usage des utilisateurs. Sauf autorisation expresse, il est interdit à l’utilisateur de copier de quelque manière que ce soit ou sur un quelconque support, tout ou partie du Système d’Information, de l’adapter, de le traduire, de le donner en location, de le prêter, de le communiquer au public et de créer des travaux dérivés des éléments susvisés.

Article 11 – Mesures transitoires

Pour l’heure, le certificat de signature de la Carte d’Identité Electronique ne peut être utilisé que via le système de transmission de fichiers en (S)FTP, à l’aide de MQSeries ou d’autres canaux acceptés, et ne permet pas l’accès aux et l’utilisation des services dispensés sur le site-portail de la sécurité sociale et sur le site-portail de l’autorité fédérale, sauf pour ce qui concerne l’utilisation de l’application “Formulaire électronique de demande d’accès”.