

DÉLIBÉRATION N° 07/018 DU 24 AVRIL 2007 RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL À LA SOCIÉTÉ FLAMANDE DES TRANSPORTS DE LIJN EN VUE DE LA DISTRIBUTION D'ABONNEMENTS À CERTAINES CATÉGORIES DE PERSONNES

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

Vu le rapport d'auditorat de la Banque Carrefour de la sécurité sociale du 16 mars 2007 ;

Vu le rapport de monsieur Willem Debeuckelaere.

A. OBJET DE LA DEMANDE

1.1. La société flamande des transports De Lijn souhaite réaliser une importante simplification administrative en ce qui concerne la vente de ses abonnements aux guichets. Cette simplification devra surtout bénéficier aux groupes sociaux les plus vulnérables. En outre, elle souhaite aussi réaliser la vente d'abonnements via son site Internet.

Lors de la vente d'un abonnement, la société De Lijn a besoin de certaines données à caractère personnel qui doivent, pour le moment, être fournies par l'intéressé même, par exemple au moyen de sa carte d'identité ou de certaines attestations. Il s'agit plus précisément de l'âge et de la composition du ménage de l'intéressé, de son domicile et de ses données d'adresse.

Les tarifs des abonnements de la société De Lijn sont basés sur l'âge et/ou la *composition du ménage* de l'intéressé : les personnes âgées de moins de vingt-cinq ans et les personnes âgées de soixante ans ou plus bénéficient d'une réduction, pour le deuxième abonnement « jeune » au sein d'un même ménage, il est accordé une réduction de vingt pour cents et les abonnements « jeune » sont gratuits à partir du troisième jeune au sein du même ménage. Pour l'octroi des réductions familiales, la société De Lijn se base, à l'heure actuelle, encore sur des attestations spécifiques que l'intéressé doit se procurer auprès de sa commune.

Les communes ont la possibilité d'instaurer un système de tiers payant et de donc prendre en charge le prix des abonnements de leurs habitants. La société De Lijn doit donc connaître avec certitude le *domicile* des intéressés. À l'heure actuelle, les communes communiquent à cet effet les données à caractère personnel utiles à la société De Lijn.

Enfin, la société De Lijn a besoin des *données d'adresse* de l'intéressé pour pouvoir mentionner l'adresse sur l'abonnement et l'envoyer par la poste à l'intéressé.

Or, la société De Lijn souhaite à présent pouvoir recueillir elle-même ces données à caractère personnel.

- 1.2.** Pour certains groupes cibles, la société De Lijn prévoit par ailleurs des réductions tarifaires. Pour pouvoir bénéficier de ce type de tarif, les intéressés (ou dans certains cas, un tiers) doivent, pour l'instant, fournir la preuve qu'ils appartiennent à un groupe cible déterminé au moyen d'une attestation spécifique. La société De Lijn souhaite cependant examiner elle-même l'appartenance à un groupe cible donné, sans qu'il ne doive encore être fait appel à des attestations spécifiques.

Les catégories de personnes suivantes bénéficient donc d'une réduction tarifaire : les bénéficiaires de l'intervention majorée de l'assurance obligatoire soins de santé et indemnités, les personnes handicapées, les personnes bénéficiant d'un revenu d'intégration, les personnes séjournant dans une initiative locale d'accueil, les personnes bénéficiant d'un revenu garanti aux personnes âgées ou d'une garantie de revenus aux personnes âgées, les jeunes vivants seuls avec assistance et les enfants de moins de douze ans.

Pour chacune de ces catégories, il existe à l'heure actuelle encore un système de preuve spécifique (attestation des centres publics d'action sociale, carte de réduction « Familles nombreuses », ...).

- 1.3.** Dans le cadre de la simplification administrative précitée, la société De Lijn souhaite pouvoir disposer de plusieurs données à caractère personnel relatives à ses « clients », c'est-à-dire les personnes qui se sont adressées à elle pour obtenir un abonnement, de quelque manière que ce soit (au guichet, sur le site Internet de la société De Lijn, ...).

Il s'agit plus précisément des données d'identification, des données à caractère personnel relatives à la composition du ménage et des données relatives au statut en matière de sécurité sociale. Dans un premier temps, ces données seraient uniquement communiquées en vue de la mise en production de l'application web développée par la société De Lijn.

La communication de ces données à caractère personnel à d'autres finalités (à savoir la vente d'abonnements aux guichets de la société De Lijn et auprès du Service Abonnements) ferait l'objet d'une demande d'autorisation ultérieure par la société De Lijn.

- 1.4.** Une personne qui souhaite acheter un abonnement auprès de la société De Lijn au moyen de l'application précitée, doit d'abord s'annoncer sur le site web de la société De Lijn, au minimum au moyen du token fédéral ou de la carte d'identité électronique. Avant la connexion, cette personne est toutefois expressément avertie du fait que l'application web fait appel à des données à caractère personnel enregistrées dans des banques de données externes.

Une fois l'intéressé connecté, les membres de son ménage s'affichent à l'écran et il lui est offert la possibilité de sélectionner un ou plusieurs membres du ménage, plus précisément les membres pour lesquels il souhaite se procurer un abonnement. Ses données d'adresse s'affichent également.

Ensuite, l'intéressé doit sélectionner la date de prise de cours et la période de validité des abonnements et il lui est également offert la possibilité d'ajouter des données

d'adresse et de contact. A défaut, les abonnements sont envoyés à l'adresse de l'intéressé dont la société De Lijn dispose et qui, pour rappel, s'affiche automatiquement à l'écran de l'intéressé.

Enfin, l'intéressé reçoit un résumé de sa commande (qui indique notamment le type et la durée de validité des abonnements) et il peut procéder au paiement.

L'application web de la société De Lijn tiendra également compte du statut en matière de sécurité sociale des intéressés afin de leur distribuer un abonnement gratuit ou un abonnement à un tarif réduit.

- 1.5.** Vu ce qui précède, la société De Lijn a besoin pour toute personne faisant appel à l'application web précitée des données à caractère personnel suivantes: le numéro d'identification de la sécurité sociale, le nom, le prénom, la date de naissance, le sexe, l'adresse (et la date de prise de cours), le code pays et la composition du ménage.

En vue de la distribution d'un abonnement à un tarif réduit aux intéressés, la société De Lijn doit par ailleurs disposer d'une indication selon laquelle ils ont ou non droit à l'intervention majorée de l'assurance obligatoire soins de santé et indemnités (toutefois sans indication de la sous-catégorie en question). En effet, les bénéficiaires de l'intervention majorée de l'assurance obligatoire soins de santé et indemnités ont droit à une réduction tarifaire lors de l'achat d'un abonnement. La société De Lijn souhaite par conséquent savoir par intéressé s'il appartient ou non à cette catégorie (générale).

La société De Lijn établirait une liste de ses agents qui peuvent disposer des données à caractère personnel et la mettrait à la disposition du Comité sectoriel de la sécurité sociale et de la santé. Ces agents sont tenus de signer une déclaration par laquelle ils s'engagent à garantir le respect du caractère confidentiel des données à caractère personnel.

Les données à caractère personnel ne seraient pas communiquées à des tiers.

- 1.6.** La société De Lijn invite le Comité sectoriel de la sécurité sociale et de la santé à l'autoriser à obtenir les données à caractère personnel précitées à l'intervention du réseau de la Banque Carrefour de la sécurité sociale.

B. EXAMEN DE LA DEMANDE

- 2.1.** Il s'agit d'une communication de données à caractère personnel qui doit faire l'objet d'une autorisation de principe de la section sécurité sociale du Comité sectoriel de la sécurité sociale et de la santé en vertu de l'article 15, § 1^{er}, alinéa 2, de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale*.

- 2.2.** Si une personne utilise l'application web de la société De Lijn, il est informé, avant la connexion, du fait que l'application web a recours à des données à caractère personnel enregistrées dans des banques de données à caractère personnel externes. A ce moment, la possibilité lui est offerte, en cas de désaccord avec l'usage annoncé de

données à caractère personnel enregistrées dans des banques de données à caractère personnel externes, de quitter l'application web à ce stade (« *opting-out* »)

- 2.3.** Conformément à l'article 6, § 3, 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*, le titulaire d'une carte d'identité a le droit de prendre connaissance des données à caractère personnel qui sont conservées à son sujet dans le Registre national.

A l'instar de la Commission de la protection de la vie privée, le Comité sectoriel de la sécurité sociale et de la santé estime qu'une application web, grâce à laquelle des données à caractère personnel enregistrées dans le Registre national seraient également accessibles dans le chef des intéressés après une authentification sur seule base du token fédéral – ce qui est prévu dans le cas présent – est contraire à la disposition précitée de la loi du 19 juillet 1991.

Lors de l'utilisation du token fédéral, l'utilisateur doit prouver l'identité qu'il prétend posséder au moyen d'un mot de passe et d'une des vingt-quatre combinaisons de lettres mentionnées sur le token fédéral. Par rapport à l'usage de la carte d'identité électronique, cette procédure offre cependant moins de garanties qu'il s'agit bien de la personne avec l'identité prétendue qui utilise l'application web (si une personne entre en possession d'un nom d'utilisateur, du mot de passe et d'une copie du token fédéral d'une autre personne, il peut passer pour ce dernier). La carte d'identité électronique par contre offre un système d'authentification – le processus contrôlant qu'un utilisateur est effectivement celui qu'il prétend être – plus solide. Dans ce cas, l'utilisateur doit en effet être en possession de sa carte d'identité électronique (et des certificats y afférents) pour prouver son identité et par conséquent recevoir accès.

Ce qui précède signifie que l'intégration des données à caractère personnel issues du Registre national dans son application web telle que demandée par De Lijn (où les données à caractère personnel relatives à l'intéressé sont remplies au préalable dans les divers écrans de l'application web) n'est possible que dans la mesure où l'utilisateur de l'application web s'authentifie au moyen de sa carte d'identité électronique.

Dans la mesure où l'utilisateur s'identifie au moyen de son token fédéral, les données à caractère personnel en question ne peuvent cependant pas être remplies au préalable par l'application web dans les divers écrans. Il est vrai que la société De Lijn peut être en possession de ces données à caractère personnel en vue de la distribution et de la gestion d'abonnements mais elle ne peut les mettre à la disposition de l'utilisateur.

- 2.4.** En ce qui concerne toute personne pour laquelle il est demandé un abonnement au moyen de l'application web visée, les données à caractère personnel suivantes seraient dans un premier temps communiquées à la société De Lijn : le numéro d'identification de la sécurité sociale, le nom, le prénom, la date de naissance, le sexe, l'adresse (et la date de prise de cours) et le code pays.

Ces données à caractère personnel seraient, en ce qui concerne la personne qui utilise l'application web de la société De Lijn, complétées de sa composition du ménage.

Il est par ailleurs communiqué par intéressé s'il a ou non droit à l'intervention majorée de l'assurance obligatoire soins de santé et indemnités (sans indication de la sous-catégorie en question).

Il y a lieu de remarquer que la Société flamande des transports a été autorisée par l'arrêté royal du 5 septembre 1994 à accéder aux données à caractère personnel visées à l'article 3, alinéa 1^{er}, 1^o à 9^o inclus, et alinéa 2, de la loi du 8 août 1983 *organisant un Registre national des personnes physiques*, en vue de l'accomplissement de ses tâches relatives aux transports en commun urbains et suburbains.

Par la délibération n°04/2006 du 1^{er} mars 2006, la société De Lijn a par ailleurs été autorisée par la Commission de la protection de la vie privée *loco* le Comité sectoriel du Registre national à utiliser le numéro d'identification du Registre national en vue notamment de la vente via Internet, de la simplification administrative et de la distribution d'abonnements gratuits.

Les données à caractère personnel seraient extraites du Registre national, respectivement des registres Banque Carrefour visés à l'article 4 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale*. En ce qui concerne la communication de données à caractère personnel figurant dans le Registre national, une autorisation est, pour rappel, déjà disponible. Le Comité sectoriel de la sécurité sociale et de la santé doit, dans le cas présent, se borner à l'évaluation de la communication des données à caractère personnel concernées enregistrées dans les registres Banque Carrefour qui sont complémentaires et subsidiaires par rapport au Registre national.

- 2.5. Le numéro d'identification de la sécurité sociale permet une identification univoque et unique de l'intéressé et garantit à ce dernier que, sur base de sa situation personnelle, il aura droit à l'abonnement le plus avantageux qui lui donne accès aux services de la société De Lijn.
- 2.6. Le nom, le prénom et l'adresse (rue, numéro de maison, numéro de boîte, code postal et commune) de l'intéressé doivent être inscrits sur l'abonnement (un abonnement est toujours personnalisé et, en cas de contrôle dans le véhicule, le titulaire doit pouvoir s'identifier comme étant un voyageur en possession d'un billet de transport valide).

Ces données à caractère personnel complétées du sexe doivent permettre à la société De Lijn d'envoyer l'abonnement à l'intéressé par la poste. Le sexe offre à la société De Lijn la possibilité d'utiliser, lors de l'envoi de l'abonnement par la poste, le titre correct (madame, monsieur) sur la lettre d'accompagnement. Ce titre n'est toutefois pas mentionné sur l'abonnement même.

Selon la société De Lijn, la capture électronique de l'adresse contribue largement à la réduction de la marge d'erreurs dues à la réintroduction manuelle des données. La société De Lijn doit aussi connaître la date de prise de cours de l'adresse afin d'offrir, le cas échéant, au demandeur le bénéfice avec effet rétroactif de certains avantages lorsqu'il y a droit en vertu du système du tiers payant.

Le code postal et la commune permettent à la société De Lijn de vérifier si le demandeur a éventuellement droit à une intervention de sa commune dans le prix de l'abonnement, dans le cadre du système du tiers payant. En effet, en fonction de son

code postal et de la commune, le titulaire a droit à une intervention supplémentaire dans le prix de l'abonnement si un système de tiers payant a été conclu entre cette commune et la société De Lijn.

En ayant recours aux données à caractère personnel enregistrées dans le Registre national ou dans les registres Banque Carrefour, la société De Lijn peut garantir au titulaire de l'abonnement que son titre de transport personnel et valide lui offre l'accès aux services de la société De Lijn.

- 2.7.** La société De Lijn a par ailleurs besoin de la date de naissance de l'intéressé afin de pouvoir déterminer le type d'abonnement correct ainsi que le tarif exact.

En vertu de l'article 70 de l'arrêté du Gouvernement flamand du 14 mai 2004 *relatif à l'exploitation et aux tarifs de la Vlaamse Vervoersmaatschappij*, les tarifs sont soumis à l'approbation du ministre flamand du Transport, sur la proposition du conseil d'administration de la *Vlaamse Vervoersmaatschappij*. Les conditions générales de voyage de la société De Lijn ont été approuvées par le conseil d'administration de la société De Lijn (en date du 20 décembre 2006) et par le ministre du Transport (en date du 31 janvier 2007).

Conformément à ces conditions générales de voyage, les personnes de moins de vingt-cinq ans et les personnes de plus de soixante ans ont droit à des tarifs avantageux.

Les personnes de moins de vingt-cinq ans entrent également en considération pour une réduction familiale. Les personnes âgées de plus de soixante-cinq ans reçoivent un abonnement gratuit.

Le titulaire d'un abonnement a donc droit, en fonction de son âge, à un tarif adéquat pour son abonnement.

- 2.8.** Étant donné qu'une partie des abonnés de la société De Lijn habitent dans un autre pays (et utilisent l'abonnement gratuit à des fins professionnelles ou touristiques), la société De Lijn doit également pouvoir disposer du code pays de l'intéressé.

Pour que ce groupe cible puisse recevoir l'abonnement correctement, le pays doit également être mentionné dans les données d'adresse, conformément aux prescriptions de La Poste. Le code pays (à savoir l'abréviation internationalement reconnue d'un pays exprimée en lettres) sera toujours lié au nom du pays en question écrit en toutes lettres, et ce afin de satisfaire aux instructions en matière d'envoi correct d'abonnements aux clients séjournant à l'étranger. Si le code pays tel que décrit ci-dessus n'est pas disponible, le code INS du pays serait utilisé (soit l'identification d'un pays exprimée par un ensemble de chiffres).

- 2.9.** La société De Lijn doit connaître la composition du ménage de l'intéressé étant donné que le demandeur peut, en fonction de la composition de son ménage, avoir droit à une réduction de la société De Lijn sur le prix de son abonnement « jeune ». Pour le deuxième abonnement « jeune » au sein d'un même ménage, il est accordé une réduction de vingt pour cents et les abonnements « jeune » sont gratuits à partir du troisième jeune au sein du même ménage.

La société De Lijn vérifiera dans sa propre banque de données à caractère personnel le nombre d'abonnements « jeune » qui ont déjà été distribués au sein du ménage.

Par ailleurs, la liste des membres du ménage est également soumise à l'intéressé par le biais de l'application web de sorte qu'il puisse sélectionner les membres du ménage pour lequel il souhaite demander un abonnement.

- 2.10.** En vertu de l'article 76 de l'arrêté du Gouvernement flamand du 14 mai 2004 *relatif à l'exploitation et aux tarifs de la Vlaamse Vervoersmaatschappij*, les bénéficiaires d'une intervention majorée de l'assurance obligatoire soins de santé et indemnités ont droit à une réduction tarifaire lors de l'achat d'un abonnement de la société De Lijn. En vue de la distribution d'un abonnement à un tarif réduit, la société De Lijn souhaite donc savoir par intéressé s'il appartient ou non à la catégorie des bénéficiaires d'une intervention majorée de l'assurance obligatoire soins de santé et indemnités.

Il y a lieu d'observer que le statut précis de l'intéressé ne serait pas communiqué. La communication se limiterait au contraire à la simple indication du fait que l'intéressé a ou non droit à l'intervention majorée de l'assurance obligatoire soins de santé et indemnités (donc sans spécification de la catégorie précise).

- 2.11.** La communication poursuit des finalités légitimes. Les données à caractère personnel en question sont pertinentes et non excessives par rapport à ces finalités.

Sur base des données à caractère personnel communiquées, la société De Lijn essaiera de trouver pour le demandeur l'abonnement et le tarif les plus appropriés. Le demandeur ne doit donc pas communiquer ces données à caractère personnel au préalable.

En ce qui concerne le statut de bénéficiaire de l'intervention majorée de l'assurance obligatoire soins de santé et indemnités, la société De Lijn doit recevoir de la Banque Carrefour de la sécurité sociale uniquement la confirmation qu'un demandeur appartient à la catégorie concernée et entre donc en considération pour une réduction tarifaire. La société De Lijn ne doit pas savoir quel est le statut précis de l'intéressé (c'est-à-dire la catégorie à laquelle il appartient précisément).

- 2.12.** Le Comité sectoriel de la sécurité sociale et de la santé insiste toutefois sur le fait que la société De Lijn, sauf nouvelle autorisation de sa part, ne peut utiliser les données à caractère personnel en question que pour les finalités précitées, c'est-à-dire en vue de la distribution et de la gestion d'abonnements, à l'exclusion de toute autre finalité.

C. MESURES DE SÉCURITÉ

- 3.1.** La Banque Carrefour de la sécurité sociale conserve des traces relatives aux communications effectuées à partir du réseau de la sécurité sociale à la société De Lijn. Sont notamment conservées dans ces traces quelles données à caractère personnel relatives à *quelle personne* ont été communiquées à *quel moment* pour la finalité précitée. La Banque Carrefour de la sécurité sociale ne sait cependant pas à quel collaborateur concret de la société De Lijn les données à caractère personnel sont communiquées. Cette tâche incombe à la société De Lijn.

Les traces précitées (les traces relatives aux communications effectuées à partir du réseau de la sécurité sociale à la société De Lijn) ne sont accessibles que selon une procédure stricte qui implique l'intervention du conseiller en sécurité de l'information de la Banque Carrefour de la sécurité sociale. Elles peuvent être utilisées en vue du traitement de plaintes éventuelles ou de la constatation de certaines irrégularités.

La société De Lijn doit, quant à elle, conserver des traces plus précises, avec par communication une indication de *quelle personne* a obtenu *quelles données à caractère personnel concernant quelle personne, à quel moment et pour quelles finalités*.

Afin de pouvoir aisément détecter des irrégularités éventuelles, la société De Lijn souhaite conserver via quelle adresse IP externe un utilisateur s'est connecté au site web de la société De Lijn.

Ces traces doivent être gérées en vue du traitement de plaintes éventuelles ou de la constatation d'irrégularités éventuelles.

Préalablement à la mise en production de cette application web, la société De Lijn doit soumettre au service Audit interne et Sécurité de l'information de la Banque Carrefour de la sécurité sociale le rapport d'évaluation concernant l'exécution des tests relatifs à ces traces.

- 3.2.** Pour rappel, la société De Lijn conserve systématiquement des traces relatives au traitement des données à caractère personnel concernées (c'est-à-dire les données à caractère personnel que la société De Lijn reçoit de la Banque Carrefour de la sécurité sociale) par les membres de son personnel. Ces traces doivent être sécurisées au moyen de mesures garantissant la confidentialité, l'intégrité et la disponibilité.

Ces traces doivent être conservées pendant dix ans au moins et comprennent au moins les renseignements suivants : la date à laquelle les données à caractère personnel ont été traitées par un agent de la société De Lijn, l'identité de l'agent concerné et les personnes auxquelles les données à caractère personnel traitées se rapportent.

Ces traces sont communiquées au Comité sectoriel de la sécurité sociale et de la santé et à la Banque Carrefour de la sécurité sociale lorsqu'ils en font la demande.

Conformément à l'article 16 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*, la société De Lijn prend les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre tout traitement non autorisé.

- 3.3.** L'utilisateur a accès à l'application web après s'être annoncé au moyen du token fédéral ou de sa carte d'identité électronique.

Le Comité sectoriel de la sécurité sociale et de la santé réitère toutefois que dans la mesure où l'utilisateur s'authentifie au moyen de son token fédéral, les données à caractère personnel en question ne peuvent pas être remplies au préalable dans les

différents écrans par l'application web. La société De Lijn peut utiliser ces données à caractère personnel mais ne peut les mettre à la disposition.

- 3.4.** La société De Lijn désigne parmi les membres de son personnel un conseiller chargé de la sécurité de l'information et de la protection de la vie privée qui remplit notamment 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*.

Ce conseiller en sécurité est responsable de l'exécution de la politique de sécurité telle que définie dans le document « *Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel* ».

La société De Lijn doit également tenir compte des normes minimales de sécurité telles que définies par le Comité général de coordination de la Banque Carrefour de la sécurité sociale.

- 3.5.** Le site web de la société De Lijn et en particulier l'application web examinée doivent être sécurisés de manière optimale selon l'état de la technique en la matière afin d'éviter tout abus en matière d'accès aux données à caractère personnel. Cela implique notamment la conservation de l'intégrité des pages web, la détection et la prévention de tentatives d'attaque, l'adoption d'une « patch policy » pour les logiciels et systèmes utilisés, des tests réguliers de pénétration, l'utilisation d'un reverse-proxy et l'utilisation d'une application pare-feu. Cette énumération n'est nullement exhaustive.

Par ces motifs,

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

autorise la Banque Carrefour de la sécurité sociale à communiquer les données à caractère personnel précitées, aux conditions précitées, à la société flamande des transports De Lijn, pour la seule finalité de distribution et de gestion d'abonnements à certaines catégories de personnes.

Willem DEBEUCKELAERE
Président