Avis sur la notification d'un contrôle préalable reçue du Délégué à la protection des données de la Banque européenne d'investissement à propos du dossier "Sous-traitance partielle de la caisse de maladie".

Bruxelles, le 16 septembre 2008 (dossier 2008-323)

1. Procédure

En date du 27 mai 2008 une notification pour contrôle préalable a été adressée par le Délégué à la protection des données (DPD) de la Banque européenne d'investissement au Contrôleur européen de la protection des données (CEPD), concernant le dossier "Sous-traitance partielle de la Caisse de maladie".

Par e-mail en date du 20 juin 2008, des questions sont posées au DPD. Les réponses sont fournies le 7 juillet 2008. Des questions supplémentaires sont posées le 10 juillet et les réponses fournies le 11 juillet. L'avis a été envoyé au DPD pour commentaires le 9 septembre 2008. Ces derniers ont été reçus le 15 septembre 2008.

2. Faits

Il a été décidé d'instaurer une sous-traitance partielle de la caisse de maladie. La société choisie pour cette sous-traitance "GMC -Garantie Médicale et Chirurgicale- du groupe Henner" est une société française enregistrée à la CNIL (Commission Nationale Informatique et Libertés).

Finalité : le but de cette sous-traitance est de laisser aux affiliés le choix entre continuer à soumettre leur frais médicaux à la caisse de maladie au sein de la Banque[1] ou soumettre leur frais médicaux à un prestataire extérieur, les barèmes de remboursement étant identiques dans les deux solutions, mais avec l'avantage d'un remboursement plus rapide, de l'anonymat du traitement des données électroniquement vis à vis de la BEI. L'affilié aura la possibilité, mais une seule fois, de pouvoir réintégrer le système caisse de maladie en interne. Le rôle de la société s'occupant de cette sous-traitance, tout en respectant l'exécution des dispositions légales, réglementaires et administratives en vigueur, comporte la saisie des données, la création des dossiers, le classement et l'archivage des dossiers, les virements bancaires des remboursements, l'établissement d'une prise en charge en cas d'hospitalisation, fournir à la caisse de maladie BEI les statistiques comptables nécessaires.

Description de la catégorie ou des catégories de personnes concernées : sont concernés par cette procédure potentiellement les membres du personnel actifs et post-actifs ainsi que les personnes à leur charge affiliées à la CM à titre principal ou à titre complémentaire.

Description des données ou des catégories de données : dès qu'un affilié opte pour la sous-traitance, il doit compléter un formulaire avec toutes les données nécessaires au traitement du dossier (N° de personnel, date de naissance, actif ou pensionné et date d'engagement, adresse,

[1] Ceci a déjà fait l'objet d'un avis du CEPD. Voir avis 2004-305 du 6 avril 2005 sur le site web du CEPD.

Adresse postale : rue Wiertz 60 - B-1047 Bruxelles
Bureaux : rue Montoyer 63
E-mail : edps@edps.eu.int - Site Internet: www.edps.eu.int
Tél.: 32-2-283 19 00 - Fax : 32-2-283 19 50

ayants droits, si affiliation à titre principal ou complémentaire, compte bancaire). L'Administration du personnel BEI se chargera d'informer GMC de toutes nouvelles modifications d'affiliation. Dans certains cas la caisse de maladie BEI devra communiquer à GMC l'historique des dossiers (ex. lunetterie, orthodontie etc.), afin de permettre à GMC de respecter les délais de remboursement des quantités autorisées par le barème de remboursement de la caisse de maladie.

Informations destinées aux personnes concernées : la réglementation concernant les remboursements de la caisse de maladie est exposée dans les Dispositions Administratives, sur Intranet (page Ressources Humaines) et au moyen des notes de service. Les séances d'informations ont été organisées pour informer les membres du personnel. La division RH publiera sur intranet une liste des questions/réponses qui reviennent régulièrement. Lorsqu'un affilié opte pour la sous-traitance, il doit obligatoirement compléter et signer un formulaire. Ce formulaire comporte, en outre, une clause concernant la protection des données[2].

Procédures garantissant les droits des personnes concernées : les données sont gardées par GMC qui est enregistrée à la CNIL (Commission Nationale Informatiques et Libertés). Pour les affiliés qui optent pour GMC, la réglementation sur le remboursement des soins reste la même, ils auront la possibilité de suivre l'évolution de leur dossier et les modalités à suivre sur le site Web de GMC par le biais d'un username et d'un mot de passe personnalisé. Le formulaire mentionné au point précédent mentionne également les droits d'accès, d'opposition et de rectification accordés à la personne concernée. Par souci de confidentialité, toute consultation sur place, sur le site GMC, des dossiers se fait avec la présence du personnel habilité des Services généraux.

Procédures de traitement automatisées / manuelles : l'affilié qui a opté pour la sous-traitance, pourra soumettre les frais à GMC électroniquement et leur faire suivre par la suite les originaux. Dès que le dossier sera traité, GMC fera parvenir à l'affilié un extrait détaillant les remboursements soit électroniquement, soit par courrier, selon le choix de l'affilié.

GMC dispose de sa propre base de données et ne peut en aucun cas, se connecter aux serveurs internes de la Banque. Les données concernant les agents BEI et leur famille affiliée sont ceux transmis par les agents mêmes lors de leur affiliation à GMC et repris sur le formulaire de demande d'affiliation. Le traitement des données est effectué à Paris. Il n'y a pas de traitement effectué au sein de la BEI.

[2] La réponse à ces questions est obligatoire pour adhérer au régime remboursement des soins de santé de la Banque Européenne d'Investissement géré par GMC Services (GMC). Ces données sont destinées à GMC Services et à GMC Gestion en tant que responsables du traitement, et à la Banque européenne d'investissement, uniquement aux fins de gestion de votre garantie et sont traités en conformité avec la loi française n° 78-17 transposant la Directive (CE) 95/46 du 24 octobre 1995. Elles pourront être transférées aux établissements de soins situés à l'étranger aux fins de remboursement des soins que vous aurez reçus sur place. Ce transfert n'est susceptible d'être réalisé qu'à votre demande et dans votre intérêt et uniquement lorsque celui-ci est nécessaire à l'exécution de votre régime remboursement de soins de santé. Ces données sont destinées à être conservées durant le temps de gestion de votre régime, jusqu'à complet paiement des sommes dues. Elles sont susceptibles d'être conservées conformément aux règles de prescription applicables, et aux délais nécessaires à l'établissement des statistiques et des états de contrôle. Vous disposez d'un droit d'accès, d'opposition et de rectification qui s'exerce au 10 rue Henner, 75009 Paris ; ou par e-mail au info@henner.com. Vous pouvez également saisir le Contrôleur européen de la protection des données, sis 60, Rue Wiertz MO 63 B-1047, Bruxelles, conformément au règlement CE n° 45/2001 du 18 décembre 2000 relatif à la protection physiques à l'égard du traitement des données à caractère personnel par le institutions et organes communautaires et à la libre circulation de ces données, ainsi que la CNIL, Commission nationale informatique et libertés, 8 rue Vivienne, CS 30223, 75083 Paris Cedex 02, conformément à la loi française n° 78-17 dite Loi Informatique et libertés.

Support de stockage des données : concernant le stockage des données, les informations fournies par GMC reposent principalement sur les points suivants :

1. l'architecture du système de sauvegarde permet de sauvegarder l'ensemble des serveurs (Paris et Province) du Groupe et permet une simplification de l'administration et du suivi des comptes rendus des sauvegardes réalisées. Le logiciel de sauvegarde utilise des fonctions avancées tel que la compression ou la navigation temporelle pour une recherche plus rapide des données à restaurer. Il utilise une base de données qui contient l'ensemble des informations nécessaires à la gestion des bandes et des rôles. Cette dernière est elle aussi sauvegardée sur bandes tous les jours.
2. Les données à sauvegarder sont réparties en grands domaines. A chacun de ces domaines est appliquée une politique de sauvegarde qui définit :
    - la durée de rétention des données à l'intérieur de la librairie de sauvegarde,
    - le type de sauvegarde :
        - Totale (intégralité des données),
        - Totale synthétique (reconstitution à partir de sauvegardes synthétiques),
        - Synthétique (sauvegarde des différences entre deux sauvegardes).

Les applications du traitement reposent sur les logiciels (9 au total) qui sont des applications de gestion, des applications à des fins statistiques, des logiciels de rapprochement bancaire, de comptabilité générale, de suivi de la trésorerie, ainsi que des logiciels qui permettent la mise en place de nouveaux contrats (lien entre commerciaux et gestion), de stocker les login et mots de passe des affiliés pour les accès Internet, de mettre à disposition des affiliés 2 ans d'historique de leur décompte et enfin qui effectuent la saisie des éléments permettant l'émission d'une prise en charge.

Sous traitant : un contrat entre la société GMC et la Banque européenne d'investissement a été signé en avril 2008 avec notamment les clauses suivantes :

1. Article 7 – Protection des données

Sans préjudice du § 11 des modalités générales et des conditions, le prestataire de services justifie que la banque à tout moment, comme un résultat direct ou indirect de tout acte ou omission du prestataire de services, ne sera en violation d'aucune de ses obligations en vertu du règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 sur la protection des personnes physiques en ce qui concerne le traitement des données à caractère personnel par les institutions communautaires et les organismes et sur la libre circulation de telles données.

Le prestataire de services s'engage à se conformer à tout besoin résultant des conditions imposées à la banque par le contrôleur européen de la protection des données (EDPS).

2. § 11. de l'appendice C du contrat : Confidentialité et protection des données personnelles

Le consultant traitera comme confidentiel toutes les informations, qu'il acquiert, de la banque ou de toute autre personne au cours de l'exécution de ses services. Néanmoins, l'obligation déjà citée de la confidentialité ne s'appliquera à aucune information qui était dans la possession du consultant avant le commencement de ses services, ou qui est ou entre plus tard dans le domaine public exception faite de révélations illégales du consultant. Le consultant ne mettra en référence ni la banque ni l'existence et les termes du contrat sans l'approbation écrite préalable de la banque.

Le consultant se conformera aux dispositions appropriées de la législation de la protection de données à caractère personnel de la Communauté européenne, notamment au règlement (CE) 45/2001 du 18 décembre 2000 et aux dispositions de la législation nationale appropriée mettant en œuvre la directive 95/46 de la (CE) du 24 octobre 1995. Le consultant obtiendra à partir de chacun de ses employés affectés au projet et, s'il y a lieu, à partir de chaque sous-traitant un engagement écrit (annexe III) qu'il renverra à la banque dûment exécuté.

3. Annexe 3 du contrat signé entre GMC et la BEI relative aux règles pour la protection des données

Cette annexe 3 du contrat concerne les règles relatives à la protection des données. Elle détaille l'ensemble des provisions applicables, en matière de traitement des données, à l'ensemble du personnel du contractant appelé à travailler dans le cadre du projet objet de la sous-traitance. Le personnel est rappelé à des obligations de confidentialité, de non divulgation, de non copie ou transmission. L'attention est attirée sur le fait que la responsabilité personnelle peut être invoquée si le personnel viole les règles de confidentialité précitées et qu'il est susceptible d'être poursuivi par la BEI. Cette dernière demande de recevoir par retour une copie de cette annexe, dûment approuvée par les soussignés et contresignée par le représentant légal du contractant.

Base légale et licéité du traitement : le règlement du personnel; les dispositions administratives, le règlement du régime de pension du personnel, le contrat entre la BEI et GMC, la décision du Comité de Direction.

Destinataires auxquels les données sont susceptibles d'être communiquées : certaines données de la caisse de maladie sont communiquées au médecin-conseil ou médecin dentiste conseil. Sont soumis au médecin- conseil pour avis les dossiers concernant les maladies graves, la perte d'autonomie, les cures, le remboursement de certains médicaments, des dossiers pour avis divers. Sont soumis au médecin dentiste conseil les devis dentaires et orthodontiques. Lorsque pour les dossiers traités par GMC l'avis d'un des médecins-conseils est nécessaire, GMC adressera le dossier directement au médecin-conseil sous plis strictement confidentiels, sans transiter par la caisse de maladie.

Politique de conservation des données personnelles : GMC devra respecter les mêmes délais de conservation des données que la caisse de maladie (10 ans). Une note a été établie par la société GMC reprenant les informations relatives à la durée de conservation, la méthode d'archivage, les demandes d'archivage et les demandes de consultation des archives.

Mesures prises pour assurer la sécurité du traitement : [...]

Des mesures de sécurité informatiques font l'objet de l'annexe 2 du contrat signé entre la BEI et GMC. [...]

3. Aspects légaux

3.1. Contrôle préalable

La notification reçue par courrier le 27 mai 2008 représente un traitement de données à caractère personnel ("toute information concernant une personne identifiée ou identifiable" - article 2.a). Le traitement de données présenté est effectué pour le compte d'une institution et est mis en œuvre pour l'exercice d'activités relevant du champ d'application du droit

communautaire (article 3.1). Le traitement est automatisé en partie et les dossiers de remboursement font l'objet d'un archivage sur support papier appelé à figurer dans un fichier. L'article 3.2 est donc applicable en l'espèce.

Dès lors, ce traitement tombe sous le champ d'application du Règlement (CE) 45/2001.

L'article 27.1 du Règlement 45/2001 soumet au contrôle préalable du Contrôleur européen de la protection des données tout "traitement susceptible de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités". Le traitement rencontre par ailleurs les dispositions de l'article 27.2.a : "les traitements susceptibles de présenter de tels risques sont les suivants : les traitements de données relatives à la santé ...", ce qui est le cas en l'espèce s'agissant des remboursements de soins de santé et à ce titre est soumis au contrôle préalable du CEPD.

En principe, le contrôle effectué par le CEPD est préalable à la mise en place du traitement. Dans ce cas, le contrat ayant été signé en avril 2008, le CEPD regrette que ce traitement ne lui ait pas été soumis avant sa mise en place. A défaut, le contrôle devient par la force des choses ex-post. Ceci n'enlève rien à la mise en place souhaitable des recommandations présentées par le CEPD.

La notification officielle a été reçue par courrier le 27 mai 2008. Par e-mail en date du 20 juin 2008, des questions sont posées au DPD. Les réponses sont fournies le 7 juillet 2008. Des questions supplémentaires sont posées le 10 juillet et les réponses fournies le 11 juillet. Conformément à l'article 27.4 du règlement, le délai des deux mois au sein duquel le CEPD doit rendre son avis est suspendu. L'avis a été envoyé au DPD pour commentaires le 9 septembre 2008. Ces derniers ont été reçus le 15 septembre 2008. Le CEPD rendra par conséquent son avis au plus tard le 22 septembre 2008, le 21 étant un dimanche (28 juillet plus 24 jours de suspension + mois d'août).

3.2. Licéité du traitement

L'article 5.a du Règlement (CE) 45/2001 prévoit que "*le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités ou relevant de l'exercice légitime de l'autorité publique dont est investi l'institution*". Les remboursements des frais de santé gérés par la Caisse Maladie de la Banque européenne d'investissement concernant le personnel, les pensionnés et les ayant-droits de la banque rentrent dans le cadre de l'exercice légitime de l'autorité publique dont est investie l'institution, et sont nécessaires à la gestion des services de santé, c'est pourquoi le traitement est licite.

La banque européenne d'investissement bénéficie, en application de ses Statuts, de l'autonomie de décision au sein du système institutionnel communautaire. Conformément à l'article 29 du Règlement intérieur de la banque, le Conseil d'administration arrête les règlements relatifs au personnel. Le Règlement du personnel fixe les conditions générales d'emploi du personnel.

La base légale de ce traitement repose sur les règlements régissant les relations de l'institution avec son personnel, les dispositions administratives, le règlement du régime de pension du personnel, le contrat entre la BEI et la société GMC ainsi que la décision du Comité de Direction.

Le règlement du régime de pension du Personnel a été arrêté par le Conseil d'administration de la BEI en application de l'article 36 du Règlement du personnel.

La base juridique est conforme et vient à l'appui de la licéité du traitement.

Enfin, dans le cadre des remboursements de soins de santé, le dossier de la personne concernée peut révéler des données qualifiées dans l'article 10 du Règlement (CE) 45/2001 de "catégories particulières de données". Le dossier peut révéler des données relatives à la santé.

3.3. Traitement portant sur des catégories particulières de données

L'article 10 du règlement prévoit que le traitement de données à caractère personnel relatives à la santé est interdit, à moins qu'il ne soit justifié par des motifs visés à l'article 10, paragraphes 2 et 3, du règlement (CE) 45/2001. Le présent dossier porte très clairement sur le traitement de données à caractère personnel relatives à la santé.

L'article 10.2.b s'applique en l'espèce : "le paragraphe 1 (interdiction du traitement des données relatives à la santé) ne s'applique pas lorsque le traitement est nécessaire afin de respecter les obligations et les droits spécifiques du responsable du traitement en matière du droit du travail, dans la mesure où il est autorisé par les traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités ...". Il s'agit effectivement de la Banque européenne d'investissement en tant qu'employeur, qui respecte l'article 10.2.b en effectuant le traitement des données soumis.

En raison de leur fonction, le médecin conseil ou le médecin dentiste-conseil de la Banque européenne d'investissement sont soumis au secret professionnel et ils sont les seuls à pouvoir être destinataires de ces données. En l'espèce, l'article 10.3 qui indique que "*Le paragraphe 1 ("le traitement des données relatives à la santé ou ... sont interdits") ne s'applique pas lorsque le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé et que le traitement de ces données est effectué par un praticien de la santé soumis au secret professionnel ou par une autre personne également soumise à une obligation de secret équivalente"* du règlement est bien respecté.

Pour la même raison, il est nécessaire de souligner que les personnes qui gèrent les dossiers administratifs, et qui ne sont pas elles-mêmes des praticiens de la santé, doivent être soumises à "l'obligation de secret équivalente". Ceci est évidement applicable à l'ensemble du personnel de la société GMC amené à traiter des dossiers de remboursement de soins médicaux. Le Contrôleur européen de la protection des données se félicite que la BEI ait prévu une clause spécifique de confidentialité à respecter par le personnel de GMC et notamment par l'instauration d'une annexe spécifique au contrat qui doit être signée par chaque membre du personnel de GMC amené à traiter les dossiers de remboursement de soins de la BEI.

3.4. Responsable du traitement et sous-traitant

Conformément à l'article 2.d, du règlement, le responsable du traitement est "l'institution ou organe communautaire, la direction générale, l'unité ou toute autre entité organisationnelle qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel". Le responsable du traitement est chargé de veiller à ce que les obligations prévues par le règlement soient remplies (information de la personne concernée, garantie des droits de la personne concernée, choix du sous-traitant, notification au délégué à la protection des données…). Le sous-traitant est "la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement" (article 2.e).

Conformément au règlement (CE) 45/2001, dans le cas d'espèce, la BEI est dans le cadre de la sous-traitance partielle de la Caisse Maladie le responsable du traitement.

Le contractant (GMC) pour le traitement des remboursements de soins médicaux est considéré comme sous-traitant lorsqu'il accomplit les tâches telles que prévues au contrat le liant à la BEI.

Le rôle du sous-traitant, en tant que tel, est d'aider la BEI à permettre le remboursement des soins médicaux du personnel de la BEI qui aurait fait ce choix. L'article 2.e du règlement est donc bien applicable.

Dès lors, la mention " *(...) Ces données sont destinées à GMC Services et à GMC Gestion en tant que responsables du traitement, et à la Banque européenne d'investissement, uniquement aux fins de gestion de votre garantie et sont traités en conformité avec la loi française n° 78-17 transposant la Directive (CE) 95/46 du 24 octobre 1995 (...)*" inscrite au bas du formulaire est erronée. GMC services et GMC Gestion sont des sous-traitants agissant pour le compte de BEI, sur la base d'un contrat conclu le 8 avril 2008[3].

Le CEPD recommande que cette mention soit rectifiée dans le cadre du formulaire de remboursement des soins à retourner par la personne concernée à GMC Services.

3.5. Qualité des données

Les données doivent être "*adéquates, pertinentes et non excessives*" (article 4.1.c du Règlement (CE) 45/2001). Les données traitées, décrites au début de cette opinion, doivent être considérées comme remplissant ces qualifications par rapport au traitement. Le CEPD estime que l'article 4.1.c. du règlement (CE) 45/2001 est respecté.

Par ailleurs les données doivent être *traitées loyalement et licitement* (article 4.1.a du Règlement (CE) 45/2001). La licéité a déjà fait l'objet d'une analyse (voir supra, point 3.2). Quant à la loyauté, dans le cadre d'un sujet aussi sensible, elle doit faire l'objet de beaucoup d'attention. Elle est liée aux informations qui doivent être transmises à la personne concernée (voir supra, point 3.9).

Enfin les données doivent être "*exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables sont prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées*" (article 4.1d du Règlement). Le système lui même contribue par ailleurs à garantir que les données sont exactes et mises à jour puisque la personne concernée fournit elle-même les données soumises au traitement. Par ailleurs, les droits d'accès et de rectification sont à la disposition de la personne concernée ce qui concourt à garantir la mise à jour des données et à rendre le dossier le plus complet possible. Ils représentent la deuxième possibilité d'assurer la qualité des données. Concernant ces deux droits d'accès et de rectification, voir point 3.8 ci-après.

3.6. Conservation des données

L'article 4.1.e du Règlement (CE) 45/2001 pose le principe que les données doivent être "*conservées sous une forme permettant l'identification des personnes concernées pendant une*

3 "*We refer to the above contract governing the assignment which your staff is due to undertake* ***on behalf of the Bank's*** *SG-JU-RH-RH/ADM Department under the health project*".

durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement".

La société GMC applique à cet égard la même durée de conservation des données que la BEI dans le cadre du même traitement[4], les recommandations sur ce point sont applicables de façon identique. L'architecture de sauvegarde du système permet une conservation sécurisée des données.

Néanmoins les applications du traitement reposent sur les logiciels (9 au total) qui sont des applications de gestion, des applications à des fins statistiques etc. Ces dernières applications doivent respecter les conditions de l'article 4.1.e du règlement 45/2001 ("*L'institution ou l'organe communautaire prévoit, pour les données à caractère personnel qui doivent être conservées au-delà de la période précitée à des fins historiques, statistiques ou scientifiques, soit qu'elles ne seront conservées que sous une forme qui les rend anonymes, soit, si cela est impossible, qu'elles ne seront stockées qu'à condition que l'identité de la personne concernée soit cryptée. Les données ne doivent en tout cas pas être utilisées à des fins autres qu'historiques, statistiques ou scientifiques*"). Le CEPD recommande donc que ces données fassent l'objet soit d'une anonymisation soit d'un encryptage.

3.7. Transfert des données

Se pose ici la question de comment considérer les transferts entre GMC et la BEI. Le transfert peut s'effectuer à deux occasions :

1. lors du transfert de statistiques comptables et dans ce cas si les données sont anonymisées, il n'y a plus de transfert de données personnelles;
2. à l'occasion de la demande d'avis aux médecins-conseils. Lorsque pour les dossiers traités par GMC l'avis d'un des médecins-conseils est nécessaire, GMC adressera le dossier directement au médecin-conseil sous plis strictement confidentiels, sans transiter par la caisse de maladie.

Sur ce point, ce traitement doit être examiné à la lumière de l'article 8 ("*transferts de données à caractère personnel à des destinataires autres que les institutions et organes communautaires et relevant de la directive 95/46/CE*"), GMC agissant pour le compte de la BEI. Dans le cas d'espèce, ces transferts sont couverts par l'article 8.a dans le sens où "*le destinataire démontre que les données sont nécessaires à l'exécution d'une mission effectuée dans l'intérêt public ou relevant de l'exercice de l'autorité publique*", comme sous-traitant des données. Actuellement, le contractant est soumis aux obligations prévues par la directive 95/46/CE.

3.8. Droit d'accès et de rectification

L'article 13 du règlement (CE) 45/2001 dispose du droit d'accès - et de ses modalités - à la demande de la personne concernée par le traitement. L'article 14 du règlement (CE) 45/2001 établit un droit de rectification pour la personne concernée. De la même façon que la personne concernée dispose du droit d'accès, cette dernière peut aussi modifier directement ou faire modifier les données personnelles si nécessaire.

Pour mémoire, les droits des personnes concernées sont garantis par le sous-traitant directement qui mentionne expressément ces deux possibilités dans le cadre même de son formulaire de remboursement. Par ailleurs, pour les affiliés qui optent pour GMC, la

[4] Voir avis 2004-305 du 6 avril 2005 sur le site web du CEPD.

réglementation reste la même, ils auront la possibilité de suivre l'évolution de leur dossier et les modalités à suivre sur le site Web de GMC par le biais d'un username et d'un mot de passe personnalisé.

Les dispositions des articles 13 et 14 du règlement sont donc respectées.

3.9. Information des personnes concernées

Il est indiqué dans la notification que les personnes concernées, en l'occurrence le personnel de la Banque européenne d'investissement, sont informées par le biais des dispositions administratives, de la page Ressources Humaines d'Intranet et les notes de services. Les séances d'informations ont été organisées pour informer les membres du personnel. La division RH publiera sur intranet une liste des questions/réponses qui reviennent régulièrement.

Les dispositions de l'article 11 sur l'information de la personne concernée sont applicables en l'espèce et sont respectées dans la mesure où les recommandations effectuées par le CEPD dans le cadre du dossier 2004-305[5] ont été mises en œuvre par la BEI. L'information fournie quant à elle par GMC dans le cadre de son formulaire de remboursement[6] reprend également les informations nécessaires pour la personne concernée.

3.10. Traitement de données à caractère personnel pour le compte du responsable du traitement

Lorsqu'une opération de traitement est effectuée pour le compte d'un responsable du traitement, l'article 23 du règlement stipule que celui-ci choisit un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation prévues par le règlement. La réalisation de traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que le sous-traitant n'agit que sur instruction du responsable du traitement et que les obligations de confidentialité et de sécurité concernant le traitement des données à caractère personnel incombent également au sous-traitant.

En l'occurrence, la BEI a accompli son obligation puisque les termes de référence du cadre de l'appel d'offres spécifient l'obligation pour le contractant d'assurer la confidentialité des données personnelles traitées par le contractant aux fins exclusives de l'exécution du contrat-cadre, en conformité avec les dispositions du règlement (CE) n° 45/2001. Cette obligation est reprise dans le contrat.

L'article 23.2.b du règlement 45/2001, relatif au traitement de données à caractère personnel pour le compte du responsable du traitement, doit être également mentionné. Le sous-traitant a explicitement fait référence aux aspects relatifs à la confidentialité et aux mesures de sécurité qui sont repris aux articles 16 et 17.3 de la directive 95/46/CE. Le sous-traitant fait explicitement référence à la loi française 78-17 transposant la Directive 95/46/CE.

3.11. Sécurité

Conformément à l'article 22 du règlement (CE) 45/2001 relatif à la sécurité des traitements, *"le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à caractère personnel à protéger".*

[5] Voir note en bas de page n° 1.
[6] Voir note en bas de page n°2.

Au regard de l'ensemble des mesures de sécurité et des autres mesures organisationnelles et techniques prises, tant par le responsable du traitement que par le sous-traitant et tout particulièrement telles que présentées à l'annexe 2 du contrat, afin d'assurer une sécurité maximale au traitement, le CEPD estime que celles-ci peuvent être considérées comme adéquates au sens de l'article 22 du règlement (CE) 45/2001.

Conclusion

Le traitement proposé ne paraît pas entraîner de violations des dispositions du Règlement (CE) 45/2001 pour autant qu'il soit tenu compte des observations faites ci-dessus. Cela implique, en particulier, que la Caisse maladie de la Banque européenne d'investissement transmette au sous-traitant la mise en place des recommandations suivantes :

- que la mention "*responsables du traitement"* soit rectifiée dans le cadre du formulaire de remboursement des soins à retourner par la personne concernée à GMC Services.
- que les données susceptibles de faire l'objet de statistiques soient anonymisées ou encryptées.

Fait à Bruxelles, le 16 septembre 2008

(signé)

Joaquín BAYO DELGADO
Contrôleur européen adjoint de la protection des données