Avis sur la notification d'un contrôle préalable reçu à propos du dossier "Procédures relatives à la gestion administrative des frais médicaux" de la Banque européenne d'investissement.

Bruxelles le 6 avril 2005 (Dossier 2004-305)

Procédure

Par courrier en date du 10 février 2005 une notification dans le sens de l'article 27 (3) du Règlement (CE) n° 45/2001 a été effectuée par Monsieur Jean-Philippe MINNAERT, Délégué à la Protection des données de la Banque Européenne d'Investissement.

Faits

L'équipe de la Caisse Maladie (CM ci-après) doit assurer le remboursement des frais médicaux conformément aux règles contenues dans l'annexe II des Dispositions administratives de la Banque.

L'affilié remet à la CM un bordereau récapitulatif avec indication du nombre de pièces jointes ainsi que les totaux des montants par rubrique (consultation, dentisterie, hospitalisation, lunetterie, analyses/radios, kinésithérapie). Ce bordereau doit être accompagné des originaux des mémoires d'honoraires. Chaque mémoire d'honoraires fait l'objet d'une ou plusieurs lignes de saisie à l'ordinateur. En cas d'hospitalisation, une lettre de prise en charge peut être établie. Dans ce cas les factures arriveront et seront payées directement à l'hôpital par la CM.

La saisie se compose de différentes étapes : introduction du numéro de personnel de l'agent concerné : la situation personnelle de cet agent apparaît à l'écran (nom de chaque membre de sa famille avec indication si affiliation à la CM à titre principal ou à titre complémentaire).

Chaque acte médical est saisi sous forme de code (ex. consultation : FM0107, analyses : DI0102, radios : DI0104 etc.) ; saisie de la date de la prestation et du montant y relatif. Le montant du remboursement apparaît automatiquement à l'écran.

Pour la procédure de paiement, tous les listings relatifs au paiement sont générés et imprimés par les gestionnaires caisse de maladie uniquement. Le processus se compose de plusieurs étapes :

- identification de tous les montants à payer ;
- préparation d'un listing comportant les montants du paiement – rapport d'identification - ;
- contrôle de ce listing par les gestionnaires CM. Sur la dernière page avec les totaux, signature d'un responsable RH pour « Bon à payer » ;
- transfert électronique des montants à payer au travers du système de paiement « S-Multiline » de la Banque et Caisse d'Epargne de l'Etat à Luxembourg;
- impression d'un listing des prestations en suspens ;

Adresse postale : rue Wiertz 60- B-1047 Brussels
Bureaux : rue Montoyer 63
E-mail : edps@edps.eu.int - Web site: www.edps.eu.int
Tel.: 02-283 19 00 - Fax : 02-283 19 50

- impression des extraits en double exemplaire : un exemplaire est mis sous enveloppe (pli confidentiel) automatiquement et est envoyé aux membres du personnel ou aux pensionnés, un exemplaire est classé dans le dossier CM de chaque agent avec les justificatifs correspondants. Ces dossiers sont conservés sous clef dans les bureaux de la CM pendant deux ans –année courante plus année précédente- et envoyés ensuite aux archives centrales de la Banque. La durée de conservation de ces dossiers médicaux (support papier) est de 10 ans.

Une note signée par le responsable de la division RH/Administration est adressée à la comptabilité avec indication du montant total des remboursements, des montants des avances sur bordereaux, des montants des avances sur hospitalisations et du montant du virement à la Banque et Caisse d'Epargne de l'Etat. Seront annexées à cette note copie de la page avec le bon à payer et copie du bordereau récapitulatif.

Les données sont de nature médicale et pour la plupart codifiées. Elles sont en relation avec :

- nom et prénom de l'agent
- numéro personnel de l'agent
- nature des frais : consultations, médicaments, dentisterie, hospitalisation, lunetterie, radios analyses, kinésithérapie
- date des prestations
- nom et prénom du malade (si conjoint ou enfant concernés)
- montant des frais

La conservation des données est exposée ainsi :

Les dossiers médicaux administratifs contenant le remboursement des frais médicaux avec les extraits Caisse Maladie (CM) et les justificatifs- sont conservés pendant une période totale de 10 ans (deux ans dans les bureaux de la CM –année courante plus année précédente- et envoyés ensuite aux archives centrales de la Banque). Seuls les gestionnaires CM et le personnel concerné ont accès à ces dossiers.

Les lettres de prises en charge en cas d'hospitalisation sont conservées aux archives centrales de la Banque pendant 5 ans.

- *Les listings papier des paiements CM sont conservés aux archives centrales de la Banque pendant 10 ans.*

- *Pour les données informatiques contenues dans les bases de données (encodage des frais, remboursements) les délais de conservation varient entre 3 et 4 ans selon le type de prestation.*

Un dossier médical pour chaque membre du personnel est conservé au service médical de la Commission européenne (dans ce dossier sont classés les rapports et résultats des examens concernant la visite médicale annuelle, la médecine préventive, les éventuels avis émis par le médecin-conseil pour la personne concernée).

Aspects légaux

1. contrôle préalable

La notification reçue par e-mail le 10 février 2005 représente un traitement de données à caractère personnel ("toute information concernant une personne identifiée ou identifiable" - article 2.a) et tombe dès lors 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".

La 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.

La notification du Délégué à la protection des données de la Banque Européenne d'Investissement a été reçue le 10 février 2005 par e-mail. Le Contrôleur européen de la protection des données rendra donc son avis pour le 10 avril 2005 au plus tard, tel que prévu à l'article 27.4 du Règlement.

2. base légale et licéité du traitement

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 ainsi que le Règlement du régime de pension du personnel.

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.

L'analyse de la base légale par rapport au Règlement (CE) 45/2001 s'accompagne de l'analyse de la 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 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.

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.

De la même façon, l'article 10.2.b (*le traitement des données relatives à la santé est interdit ... 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 ..."*) s'applique en l'espèce. 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.

Enfin, dans le cas présent, certaines données relatives notamment à la CM sont communiquées - sous pli confidentiel - au médecin conseil ou au médecin dentiste-conseil. En raison de la nature même des données, relatives à la santé, l'article 10.3 relatif aux catégories particulières de données du Règlement (CE) 45/2001 indiquant : "*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"* est d'application en l'espèce. En raison de leur fonction, le médecin conseil ou le médecin dentiste-conseil de la Commission (qui supplée l'absence de médecin au sein 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 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".

Le Contrôleur européen de la protection des données recommande que le personnel, dont il est fait mention ci-dessus, soit informé qu'il est soumis à l'obligation de secret.

3. collecte et transfert des données

L'utilisation du numéro personnel de l'agent permet de dire que certaines données sont extraites des bases de données du personnel. Le traitement analysé n'implique pas un changement général de la finalité prévue pour les bases de données relatives au personnel et n'est pas non plus incompatible avec cette finalité. Ceci implique que l'article 6.1 du Règlement (CE) 45/2001 n'est pas d'application en l'espèce et que l'article 4.1.b du Règlement est respecté.

La Banque européenne d'investissement utilise le numéro de personnel. L'utilisation d'un identifiant n'est, en soi, qu'un moyen -légitime, en l'espèce- de faciliter le travail du responsable du traitement des données à caractère personnel; toutefois, cette utilisation peut avoir des conséquences importantes. C'est d'ailleurs ce qui a poussé le législateur européen à encadrer l'utilisation de numéros identifiants par l'article 10§6 du Règlement, qui prévoit l'intervention du contrôleur européen. En l'espèce, l'utilisation du numéro de personnel peut avoir pour conséquence de permettre l'interconnexion de données traitées dans des contextes différents. Il ne s'agit pas ici d'établir les conditions dans lesquelles la Banque européenne d'investissement peut traiter le numéro personnel, mais de souligner l'attention qui doit être portée à ce point du Règlement. En l'espèce, l'utilisation du Numéro Personnel par la Banque européenne d'investissement est raisonnable car l'utilisation de ce numéro est un moyen de faciliter le travail du traitement.

Le traitement doit être aussi examiné à la lumière de l'article 7.1 du Règlement (CE) 45/2001. Le traitement au regard de l'article 7.1 concerne les transferts de données à caractère personnel entre institutions ou organes communautaires ou en leur sein "*si nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire*".

Nous sommes dans le cas d'un transfert au sein d'une même institution (Caisse Maladie, Ressources humaines, transferts bancaires, personnel concerné, Comptabilité, Archives centrales). Nous sommes aussi en présence d'un transfert entre Institutions puisque le dossier médical de chaque membre du personnel est conservé par le Service médical de la Commission européenne. En effet, il n'y a pas de service médical à la Banque européenne d'investissement, les visites médicales d'embauche, les visites médicales annuelles et les visites médicales d'expertise sont faites par le Service Médical de la Commission.

Il faut donc s'assurer que les conditions de l'article 7.1. soient respectées, ce qui est le cas puisque les données collectées sont nécessaires à la réalisation du traitement et que par ailleurs les données sont "*nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire*". En l'occurrence, cette mission relève de la compétence de la Commission européenne et l'article 7.1 est donc bien respecté.

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

Au-delà de la réalisation de la finalité (remboursement des soins par la Caisse Maladie), la conservation est faite sur le long terme :

- 10 ans pour les dossiers médicaux administratifs contenant le remboursement des frais médicaux ainsi que pour les listings papier des paiements CM;
- 5 ans pour les lettres de prise en charge en cas d'hospitalisation,
- entre 3 et 4 ans pour les données informatiques contenues dans les bases de données.

Le délai de 10 ans concernant la rétention des dossiers médicaux administratifs et des listings papier des paiements CM est mentionné dans le manuel des procédures du Département des Ressources Humaines, manuel qui est inséré sur le site intranet de la BEI. Il en est de même pour le délai de 5 ans concernant les lettres de prise en charge, ce qui ne paraît pas irraisonnable.

Les délais de 3 et 4 ans n'ont pas de base stricto sensu, mais les délais sont réduits par rapport au délai de 10 ans déjà utilisé, ce qui est raisonnable au regard de l'article 4.1.e.

La perspective que les données soient conservées pour des raisons historiques, statistiques ou scientifiques est exclue dans la notification.

La conservation des données sur le long terme devrait néanmoins être accompagnée de garanties appropriées. Le Contrôleur européen recommande la mise en oeuvre de garanties appropriées pour l'utilisation de ces données après la fin des remboursements des soins.

5. 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 dispositions de l'article 11 sur l'information de la personne concernée sont applicables en l'espèce. Les dispositions mentionnées aux points a) (identité du responsable du traitement), b) (finalités du traitement), c) (destinataires ou catégories de destinataires des données) et d) (caractère obligatoire ou facultatif de la réponse aux questions ainsi que les conséquences éventuelles d'un défaut de réponse) sont bien respectées.

Néanmoins, à aucun moment n'est indiqué dans la notification ou dans son annexe (modalités de remboursement des soins par la Caisse maladie) les possibilités suivantes : paragraphe e) ("*l'existence d'un droit d'accès aux données le concernant et de rectification de ces données*") et le paragraphe f) de ce même article qui fait part des informations non obligatoires (*base juridique du traitement, délais de conservation des données, droit de saisir à tout moment le contrôleur européen de la protection des données*). Ces éléments, en tout cas obligatoirement le point e), doivent être indiquées à la personne devant être informée.

Au regard de ces différentes considérations, le Contrôleur européen de la protection des données souhaite que les informations obligatoires à mentionner (*l'existence d'un droit d'accès aux données le concernant et de rectification de ces données)* le soient, ainsi que les informations mentionnées au point f de l'article 11 du Règlement et ce à tous les niveaux d'information (dispositions administratives, page Ressources Humaines intranet, notes de services ...) ainsi que tout autre moyen approprié.

6. Droits d'accès

L'article 13 du Règlement (CE) 45/2001 dispose du droit à l'information - et de ses modalités - à la demande de la personne concernée par le traitement. Dans la notification aucune mention n'est faite à la possibilité d'accès par un membre du personnel à son dossier.

Le Contrôleur européen de la protection des données demande que les dispositions de l'article 13 soient garanties.

7. 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.

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. 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 5).

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). Il ne semble mentionné aucune règle sur la possibilité accordée au personnel de mises à jour.

Le Contrôleur européen de la protection des données demande que le personnel soit garanti de pouvoir rectifier ses données personnelles.

8. Sécurité

Conformément à l'article 22 du Règlement (CE) 45/2001 relatif à la sécurité des traitements, *"le responsable du traitement met en oeuvre 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".*

L'ensemble des mesures de sécurité présenté dans la notification et dans l'information reçue plus tard semble relativement adéquat au traitement de données sensibles.

Enfin, dans la notification il est indiqué que le nombre de personnes ayant accès au dossier est très limité. Le service comptable qui paie les prestations n'a pas accès aux données médicales. Il est nécessaire de bien établir l'accès aux dossiers aux personnes autorisées en faisant la part des choses entre les données strictement médicales et les données liées aux remboursements des soins.

Le Contrôleur européen de la protection des données demande que ces deux requêtes ci-dessus exposées soient expressément mises en place ou/et garanties.

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 :

- informe le personnel gérant les dossiers de leur obligation de secret professionnel.
- accompagne la conservation des données au long terme de garanties appropriées. Le Contrôleur européen recommande la mise en oeuvre de garanties appropriées pour l'utilisation de ces données après la fin des remboursements des soins.
- mentionne les informations obligatoires (*l'existence d'un droit d'accès aux données le concernant et de rectification de ces données*), ainsi que les informations relatives à la base juridique du traitement et le droit de saisir le Contrôleur européen à la protection des données, par le biais des dispositions administratives, page Ressources Humaines Intranet, notes administratives ainsi que tout autre moyen approprié.

- garantisse les droits d'accès tels que prévu à l'article 13 du Règlement.

- garantisse le droit de rectification de chacun des données personnelles mentionnées dans leurs dossiers.

- garantisse l'accès aux dossiers par les personnes autorisées en faisant la part des choses entre les données strictement médicales et les données liées aux remboursements des soins.

Bruxelles, le 6 avril 2005

Peter HUSTINX
Contrôleur européen de la protection des données

Note de suivi 6 novembre 2006

En date du 27 octobre 2006, la BEI a pris en compte l'ensemble des recommandations figurant dans la conclusion de cet avis.

Le Contrôleur européen de la protection des données