Avis sur la notification d'un contrôle préalable reçue du DPD (délégué à la protection des données) du Parlement européen à propos du dossier "REMEDE"

Bruxelles, le 14 novembre 2006 (Dossiers 2006-301)

1. Procédure

Le Contrôleur européen de la protection des données (CEPD) a reçu en date du 19 juin 2006 une notification dans le sens de l'article 27.3 du règlement (CE) n° 45/2001 envoyée par le Délégué à la protection des données (DPD) du Parlement européen, concernant le dossier "REMEDE" (2006-301).

Le traitement "REMEDE" est déjà établi, de sorte que le contrôle ne peut être considéré comme étant préalable. Le traitement est donc soumis à un contrôle "a posteriori".

Le CEPD a identifié certains thèmes prioritaires et a choisi un nombre de traitements sujets au contrôle préalable a posteriori devant être notifiés. Les traitements relatifs aux données médicales figurent parmi ceux-ci.

Le CEPD a demandé le 6 juillet 2006 des informations supplémentaires concernant le traitement. Une réponse a été apportée le 28 septembre 2006. Le 8 novembre 2006, le CEPD a suspendu le délai pour rendre son avis de 7 jours afin de permettre au DPD d'apporter ses commentaires et, le cas échéant, des informations complémentaires. Des commentaires ont été apportés en date du 10 novembre 2006.

2. Examen de l'affaire

2.1. Les faits

Le traitement analysé concerne la gestion des remboursements des frais médicaux des députés européens ainsi que ceux de leur famille. Les personnes concernées sont donc les députés et les membres de leur famille (conjoint ou partenaire stable non matrimoniaux et les enfants à charge).

La base juridique du traitement REMEDE se trouve dans la Règlementation concernant les frais et indemnités des députés au Parlement européen, en son article 21, complétée de l'annexe IV.

Les données traitées sont les suivantes : le numéro de personnel, les données relatives à la santé du député - sous forme de factures relatives aux prestations médicales (nom du médecin, nature des prestations) -, à la famille du député, à son compte bancaire, les données relatives à la sécurité sociale - données de gestion liées aux demandes de remboursement des frais médicaux (numéro de demande, montant, dates début/fin de validité pour les remboursements, coefficients d'égalité, codification des prestations, récapitulatif des remboursements, tables de

Adresse postale : rue Wiertz 60 - B-1047 Bruxelles
Bureaux : rue Montoyer 63
E-mail : edps@edps.europa.eu- Site Internet www.edps.europa.eu
Tél.: 02/283 19 00 - Fax : 02-283 19 50

contrôle, etc) -. Ces données sont les données administratives nécessaires à la tarification des dépenses médicales. Elles sont partiellement collectées via la base données SIDEP qui centralise la signalétique des députés et des anciens députés.

Le traitement est partiellement manuel et partiellement automatisé. Les dossiers papier contiennent uniquement les ordonnances et les factures de soins ou de prestations médicales. Les rapports médicaux sont quant à eux transmis sous pli fermé et confidentiel aux médecins conseils de l'institution pour avis. Les rapports médicaux ne sont pas conservés par le service REMEDE.

Les données sont conservées pour une durée indéterminée en ce qui concerne les données sur support informatique de la base de données REMEDE. Les dossiers papier contiennent des pièces comptables, ils sont soumis à l'article 49 des Modalités d'exécution du règlement financier. Ce dernier fixe le délai de conservation à 5 ans au moins à compter de la décharge du Parlement européen pour l'année budgétaire à laquelle les pièces se rapportent (sauf pour les opérations non définitivement clôturée). Passé ce délai, les dossiers des anciens députés stockés aux archives sont détruits par une société agréée et leur destruction est certifiée par celle-ci. Les données des députés en activité sont conservées pendant toute la durée de leur mandat, y compris s'il est renouvelé.

Les données peuvent être transférées occasionnellement au Bureau liquidateur du RCAM afin d'obtenir l'avis d'un médecin conseil ou des avis sur les tarifications.

Le Parlement européen projette d'informer les personnes concernées par la voie d'une communication ad hoc. Cette communication ad hoc n'a pas encore été rédigée.

Les dossiers papier des députés sont conservés dans des armoires fermées à clef des gestionnaires de REMEDE. Les dossiers papier des anciens députés sont stockés dans des armoires fermées à clef appartenant au service de l'Unité Droits sociaux et dépenses particulières. Les fichiers électroniques se trouvent dans le serveur central de la DIT via une connexion réservée aux agents du Service pensions et assurances des députés. Les membres du Service de vérification ex-ante - de la Direction A et de la DG Finances - y ont également accès. Chaque membre du Service dispose d'un mot de passe personnel pour accéder à la base de données. Différents niveaux d'accès sont prévus pour le personnel gestionnaire. La base de données est journalisée; les accès à la base de données et les opérations sont contrôlées. Un backup - une sauvegarde - est effectué par la DIT quotidiennement.

2.2. Les aspects légaux

2.2.1. Contrôle préalable

La notification reçue par le CEPD le 19 juin 2006 représente un traitement de données à caractère personnel au sens du règlement (CE) 45/2001 - toute information concernant une personne identifiée ou identifiable - article 2.a). Le traitement de données est effectué par une institution communautaire et est mis en œuvre pour l'exercice d'activités relevant du champ d'application du droit communautaire (article 3.1). Il implique la collecte, l'enregistrement, l'organisation, la conservation, l'extraction, la consultation, etc., des données à caractère personnel (article 2.b) du règlement (CE) 45/2001) relative à la gestion des remboursements des soins de santé des députés européens et de leur famille. Ces activités sont constitutives d'un traitement partiellement automatisé et partiellement manuel. Lorsque le traitement est manuel, les données traitées sont contenue dans un fichier, dans ce cas-ci les dossiers papier

des députés (article 3.2). Dès lors, le traitement tombe sous le champ d'application du règlement (CE) 45/2001.

L'article 27.1. du règlement (CE) 45/2001 soumet au contrôle préalable du CEPD tous "les traitements susceptibles 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".

L'article 27.2. du règlement contient une liste des traitements susceptibles de présenter de tels risques. Le traitement REMEDE doit être soumis au contrôle préalable du CEPD car il contient des données relatives à la santé, comme le prévoit l'article 27.2.a).

En principe, le contrôle effectué par le CEPD est préalable à la mise en place du traitement. Dans ce cas, en raison de la nomination du CEPD, qui est postérieure à la mise en place du système, le contrôle devient par la force des choses "a posteriori". Ceci n'enlève rien à la mise en place des recommandations présentées par le CEPD.

La notification du Délégué à la protection des données du Parlement européen a été reçue le 19 juin 2006. Le CEPD aurait du donc rendre son avis pour le 20 août 2006 au plus tard, tel que prévu à l'article 27.4 du règlement. Une demande d'information supplémentaire a suspendu le délai dans lequel il faut rendre l'avis de 84 jours. Par e-mail en date du 8 novembre, la procédure a été suspendue pendant 7 jours afin de permettre au DPD d'apporter ses commentaires et, le cas échéant, des informations complémentaires. Les commentaires ont été reçus le 10 novembre 2006, l'avis devra donc être rendu pour le 14 novembre 2006 (20 août + 86 jours de suspension).

2.2.2. Licéité du traitement

Conformément au règlement (article 5.a)), la licéité du traitement est liée à l'exécution d'une mission effectuée dans l'intérêt public sur la base d'actes législatifs adoptés sur la base des traités instituant les Communautés européennes ou relevant de l'exercice légitime de l'autorité publique dont est investie l'institution communautaire. Le paragraphe 27 du préambule du règlement mentionne que "le traitement de données à caractère personnel effectué pour l'exécution de missions d'intérêt public par des institutions et organes communautaires comprend le traitement de données à caractère personnel nécessaires pour la gestion et le fonctionnement de ces institutions et organes". Dans le présent dossier, le Parlement européen traite des données à caractère personnel à propos du traitement "REMEDE", afin d'accomplir sa mission : veiller à la bonne gestion des remboursements des frais médicaux des députés et de leur famille. La licéité du traitement se fonde aussi sur l'article 5.b du règlement car le remboursement des frais de santé représente une obligation légale. Ceci posé, la licéité du traitement proposé est donc respecté.

Le Parlement européen est donc légitime à organiser le système de remboursement des prestations médicales. La base juridique spécifique du traitement se fonde sur l'article 21 et l'annexe IV de la Règlementation concernant les frais et indemnités des députés au Parlement européen. Cet article établit les conditions de remboursement des frais médicaux. Dans le cas qui nous occupe, la base juridique a toute son importance car les données traitées sont sensibles par leur nature. Le traitement porte sur une catégorie particulière de données (voir ci-dessous le point 2.2.3).

2.2.3. Traitement portant sur des catégories particulières de données

Le traitement des données relatives à la santé est interdit (article 10.1) à moins qu'il ne soit justifié par des motifs visés à l'article 10.2 et/ou 10.3.

L'article 10.3 du règlement (CE) 45/2001 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. C'est le cas en l'espèce.

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 une "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 une obligation de secret professionnel équivalente à celle des praticiens de la santé. Le CEPD accueille favorablement le fait que les examens médicaux soient transmis au médecin conseil du Parlement européen sous pli confidentiel.

2.2.4. Qualité des données

Conformément à l'article 4.1.c) du règlement, les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement. Il va de soi que les données médicales d'un dossier varieront selon les cas. Il convient de garantir que le principe de la qualité des données sera respecté. Ces garanties pourraient revêtir la forme d'une recommandation générale qui serait adressée aux personnes traitant les dossiers, leur demandant d'assurer le respect de l'article 4.1.c).

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 point 2.2.2). 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 ci-dessous point 2.2.10).

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 4.1.d) du règlement). Le système lui-même doit garantir l'exactitude des données. La mise à jour des données est effectuée par le responsable du traitement qui collecte des données raisonnablement exactes et les droits d'accès et de rectification doivent pouvoir être exercés par les députés, afin de rendre le dossier le plus complet possible. Concernant les droits d'accès et de rectification des personnes concernées, voir point 2.2.9.

2.2.5. Conservation des données

Le principe général du règlement veut que les données à caractère personnel ne puissent être conservées sous une forme permettant l'identification des personnes concernées que 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 (article 4.1.e) du règlement). Les dossiers électroniques n'ont pas pour l'instant de limite de conservation. Le CEPD estime qu'un délai de conservation proportionnel aux finalités pour lesquelles les données ont été collectées doit être établi.

En ce qui concerne les dossiers papier, ils répondent aux exigences fixées par les Modalités d'exécution du règlement financier. Le CEPD estime que ce délai de conservation est raisonnable au regard des finalités pour lesquelles les données ont été collectées.

En ce qui concerne le back up - sauvegarde - journalier effectué par la DIT, le CEPD rappelle que la conservation de ces données ne peut intervenir que dans le but de rétablir la stabilité du système afin d'assurer la continuité du traitement en cas d'incident. La durée de conservation doit être proportionnelle à cette finalité.

Si les données sont conservées à des fins historiques, statistiques ou scientifiques (article 4.1.b) comme il est envisagé dans la notification, les données devront être rendues anonymes.

2.2.6. Changement de finalité / Usage compatible

L'utilisation du numéro personnel du député, permet de dire que certaines données sont extraites des bases de données du personnel (dans ce cas-ci, la base de données SIDEP). Le traitement analysé n'implique pas un changement général de la finalité prévue pour les bases de données relatives aux députés 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.

Concernant le back up, le CEPD recommande que les personnes de la DIT ayant accès au back up - sauvegarde - du système REMEDE soient informées que la restauration des données (qui sont liées aux députés eux-mêmes) de back up collectées dans le but de rétablir la stabilité du système afin d'assurer la continuité du traitement en cas d'incident ne peut être utilisée pour aucune autre finalité, à l'exception de la prévention, la recherche, la détection et la poursuite d'infractions pénales graves comme prévu par l'article 6.2 du règlement.

2.2.7. Transfert des données

Le traitement doit être aussi examiné à la lumière de l'article 7.1 du règlement (CE) 45/2001. L'article 7.1 du règlement dispose que les données à caractère personnel ne peuvent faire l'objet de transferts entre institutions ou organes communautaires ou en leur sein que si elles sont 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 (médecin-conseil, DG Finances). Nous sommes aussi en présence d'un transfert entre institutions puisque les données personnelles peuvent, occasionnellement, être transférées au Bureau Liquidateur du Régime Commun d'Assurance Maladie (RCAM).

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 des différents services du Parlement européen et du Bureau Liquidateur du RCAM. Concernant ces transferts, rappelons que seules les données pertinentes doivent être transférées. Ce

transfert est donc bien licite dans la mesure où la finalité est couverte par les compétences des destinataires. L'article 7.1 semble donc bien respecté.

2.2.8. Traitement incluant le numéro de personnel ou le numéro identifiant

Le Parlement européen 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.

Il ne s'agit pas ici d'établir les conditions dans lesquelles le Parlement européen 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 le Parlement européen est raisonnable car l'utilisation de ce numéro est un moyen de faciliter le travail du traitement, en particulier son archivage.

2.2.9. Droit d'accès et de rectification

En application de l'article 13 du règlement, la personne concernée a notamment le droit d'obtenir, sans contrainte, du responsable du traitement, la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données. L'article 14 stipule que la personne concernée a le droit d'obtenir du responsable du traitement la rectification sans délai de données inexactes ou incomplètes.

Le CEPD estime que les droits d'accès et de rectification ainsi que ceux de verrouillage et d'effacement (articles 15 et 16 du règlement) doivent être accordés à la personne concernée pour les dossiers papier et électroniques.

2.2.10. Information des personnes concernées

Les articles 11 et 12 portent sur les informations à fournir à la personne concernée afin de garantir un traitement transparent des données à caractère personnel. L'article 11 prévoit que, lorsque les données sont collectées auprès de la personne concernée, les informations doivent être fournies au moment de la collecte. Lorsque les données n'ont pas été collectées auprès de la personne concernée, les informations doivent être fournies dès l'enregistrement des données ou lors de leur première communication, sauf si la personne concernée en dispose déjà (article 12).

En l'espèce, les informations peuvent être collectées auprès de l'intéressé en ce qui concerne ses données liées aux frais médicaux par exemple. Elles peuvent également être collectées auprès d'un tiers, dans le cas de ces données d'identification via d'autres bases de données (SIDEP) ou via le médecin conseil. En l'espèce, les articles 11 et 12 s'appliquent.

Le CEPD note qu'il n'existe aucun mode d'information des personnes concernées à ce jour. Le CEPD demande qu'une information complète à la personne concernée soit mise en place. Cette information devra contenir toutes les mentions des articles 11 et 12 du règlement (CE) 45/2001.

2.2.11. Sécurité

Des mesures techniques et organisationnelles ont été prises afin d'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. Après une analyse attentive par le CEPD des mesures de sécurités adoptées, le CEPD considère que ces mesures sont adéquates à la lumière de l'article 22 du règlement (CE) 45/2001.

Conclusion

Certains éléments du traitement proposé ne tiennent pas compte des dispositions du règlement (CE) 45/2001. De manière à assurer le respect du règlement (CE) 45/2001, le CEPD recommande que les remarques qui précèdent soient prises en compte, en particulier que:

- Le personnel en charge du traitement soit informé qu'il est soumis à une obligation de secret professionnel équivalente à celle des praticiens de la santé.

- Une recommandation générale demandant d'assurer le respect de l'article 4.1.c). soit adressée aux personnes traitant les dossiers.

- Un délai de conservation proportionnel aux finalités pour lesquelles les données ont été collectées soit établi pour les dossiers électroniques.

- La durée de conservation des donnée de back up soit proportionnelle à la finalité pour laquelle elles ont été collectée - rétablir la stabilité du système afin d'assurer la continuité du traitement en cas d'incident -.

- Si les données sont conservées à des fins historiques, statistiques ou scientifiques (article 4.1.b) comme envisagé dans la notification, qu'elles soient rendues anonymes.

- Que les personnes de la DIT ayant accès au back up - sauvegarde - du système REMEDE soient informées que la restauration des données (qui sont liées aux députés eux-mêmes) de back up collectées dans le but de rétablir la stabilité du système afin d'assurer la continuité du traitement en cas d'incident ne peut être utilisée pour aucune autre finalité, à l'exception de la prévention, la recherche, la détection et la poursuite d'infractions pénales graves comme prévu par l'article 6.2 du règlement.

- Les droits d'accès et de rectification ainsi que ceux de verrouillage et d'effacement soient accordés à la personne concernée pour les dossiers papier et électroniques.

- Une information complète à la personne concernée soit mise en place. Cette information devra contenir toutes les mentions des articles 11 et 12 du règlement (CE) 45/2001.

Fait à Bruxelles, le 14 novembre 2006

Peter HUSTINX
Le Contrôleur