Avis sur une notification en vue d'un contrôle préalable adressée par le délégué à la protection des données de la Commission concernant la gestion du régime d'assurance maladie commun aux institutions des Communautés européennes (RCAM)

Bruxelles, le 10 juillet 2007 (Dossier 2004-238)

1. Procédure

Le 6 mars 2007, le contrôleur européen de la protection des données (ci-après dénommé "le CEPD") a reçu du délégué à la protection des données (DPD) de la Commission une notification en vue d'un contrôle préalable (ci-après dénommée "la notification") concernant la gestion du régime d'assurance maladie commun aux institutions des Communautés européennes (ci-après dénommé "le régime d'assurance maladie") par l'Office de gestion et de liquidation des droits individuels (ci-après dénommé "le PMO") et les remboursements effectués par ce dernier au titre du régime.

Le CEPD a demandé des informations complémentaires le 4 avril 2007, qui ont été communiquées le 25 mai 2007. Une réunion à laquelle ont participé des agents du secrétariat du CEPD et des membres du personnel du PMO a eu lieu le 4 juin 2007, afin de confirmer les informations factuelles et de préciser différents aspects du fonctionnement du régime d'assurance maladie. Le 14 juin 2007, le CEPD a transmis, pour observation, le projet d'avis au PMO. Les agents du secrétariat du CEPD et les membres du personnel du PMO se sont réunis de nouveau le 22 juin 2007. Lors de la réunion, le personnel du PMO a communiqué au CEPD ses observations sur le projet d'avis, qui ont par la suite été prises en compte dans la version papier du projet d'avis du 29 juin 2007.

2. Examen du dossier

2.1. Les faits

Présentation du régime d'assurance maladie commun: l'unité Assurance maladie & Accident du PMO (ci-après dénommé "PMO/3") est notamment responsable de la gestion du régime commun d'assurance maladie pour les fonctionnaires, agents temporaires et pensionnés des institutions de l'UE ("membres du personnel de l'UE"). Les conjoints/partenaires, enfants et personnes à charge peuvent également être couverts par l'assurance ("les assurés")[1].

[1] Dans le présent avis, nous utiliserons le terme "membres du personnel de l'UE" pour désigner les fonctionnaires, agents temporaires et pensionnés des institutions de l'UE ayant droit à la couverture des risques d'accident et de maladie professionnelle au titre des articles 72 et 28 du statut et du régime applicable aux autres agents des Communautés européennes, respectivement. Nous ferons référence aux "assurés" pour tenir compte également des conjoints/partenaires, enfants et personnes à charge assimilées. Les références s'entendront comme faites aux affiliés ou aux assurés, selon les cas.

Le régime d'assurance maladie a été établi conformément à l'article 72 du statut des fonctionnaires des Communautés européennes et à l'article 28 du régime applicable aux autres agents des Communautés européennes[2]. La notification porte sur les opérations de traitement de données relatives à la gestion du régime d'assurance maladie.

Afin de gérer le régime d'assurance maladie et les remboursements effectués dans le cadre du régime, certaines règles ont été définies pour compléter l'article 72 du statut. Les règles déterminent notamment le taux exact de remboursement, qui dépend de la nature des services, du type de maladie, des procédures de remboursement et d'autres facteurs. Conformément à ces règles, en général, les membres du personnel de l'UE affiliés au régime d'assurance maladie paient à l'avance les frais liés à l'utilisation des services médicaux et des produits pharmaceutiques. Ensuite, les membres du personnel de l'UE doivent remplir des formulaires normalisés pour demander le remboursement de leurs dépenses et les transmettent sous forme papier au bureau liquidateur au sein du PMO/3. Les formulaires doivent être accompagnés des factures originales et des prescriptions médicales. En cas d'hospitalisation, les membres du personnel de l'UE peuvent demander au bureau liquidateur d'accepter la prise en charge des frais d'hospitalisation.

Pour certains traitements, le bureau liquidateur exige une autorisation préalable avant de commencer la thérapie ou la médication. Dans de tels cas, les membres du personnel de l'UE doivent fournir au bureau liquidateur des renseignements spécifiques relatifs au traitement ainsi qu'une prescription médicale précisant notamment le diagnostic de la maladie nécessitant un traitement. Des procédures similaires s'appliquent à la reconnaissance de maladies graves, lesquelles sont remboursées à un taux plus élevé que les maladies ordinaires.

À la réception des demandes de remboursement, le personnel du bureau liquidateur scanne les documents reçus, enregistre le document scanné et toutes les informations complémentaires dans un ordinateur et traite la demande. La base de données logicielle utilisée est ASSMAL. Le bureau dresse régulièrement des listes de paiement et des ordres de paiement qui sont transférés à la DG BUDGET aux fins du paiement par l'intermédiaire du compte bancaire des affiliés.

La ***finalité d'ensemble du traitement*** des données est de gérer et de garantir le remboursement des dépenses médicales résultant de l'affiliation au régime d'assurance maladie, conformément à l'article 72 du statut et des règlements pris pour son application.

La ***responsabilité première du traitement des données*** incombe à l'unité PMO/3, comme cela a été expliqué ci-dessus. La plupart des opérations de traitement des données réalisées dans le cadre de la gestion du régime d'assurance maladie sont effectuées par le bureau liquidateur au sein du PMO/3. En outre, les médecins-conseils relevant du PMO/3 effectuent également certaines opérations de traitement de données.

Comme cela est décrit plus en détail ci-dessous, les opérations de traitement manuelles et les opération de traitement des données automatisées sont très étroitement liées. Alors que certaines opérations de traitement des données, telles que la collecte initiale des informations, sont manuelles, ces données sont ensuite invariablement introduites dans une base de données logicielle et transférées par voie électronique. Les ***opérations manuelles*** peuvent être résumées comme suit:

[2] Adopté par le Conseil le 22 mars 2004. Ces deux documents seront désignés respectivement par "statut" et "régime applicable aux autres agents" ou parfois conjointement par "statut".

- en ce qui concerne les demandes de remboursement de frais médicaux, une fois que le bureau liquidateur a reçu la demande à laquelle sont jointes les déclarations de frais, factures et prescriptions médicales, le personnel du bureau liquidateur les *scanne*. Ensuite, le personnel du bureau liquidateur évalue la nature de chaque dépense et sa tarification, sur la base des documents fournis par le membre du personnel de l'UE. Suite à cette évaluation, ces informations sont encodées afin d'être soumises à un traitement complémentaire aux fins du remboursement final des dépenses.

- Les demandes d'autorisation préalable, y compris pour les traitements dentaires, sont reçues par le bureau liquidateur, qui est l'organe chargé de la réception des formulaires et documents connexes. Parmi ces documents complémentaires figurent la prescription médicale indiquant les raisons du traitement, des informations sur le traitement (type, nombre de séances, durée probable) ainsi que des renseignements sur le diagnostic de la maladie nécessitant la prescription. Le personnel du bureau liquidateur envoie les demandes au bureau du médecin-conseil, qui introduit les informations dans ASSMAL. Le médecin-conseil *évaluera* s'il y a lieu d'accéder à la demande. Son avis sera repris dans un document word, enregistré dans la base de données ASSMAL. Si le médecin-conseil recommande d'accorder l'autorisation, le bureau liquidateur délivre une autorisation officielle qui est ensuite transmise au demandeur.
- Les demandes de prise en charge sont *reçues* et *scannées* par le bureau liquidateur qui *vérifie* a posteriori si le demandeur y a droit. Si oui, le personnel du bureau liquidateur *rédige* une lettre de prise en charge qui est envoyée directement à l'affilié au format papier. Une version électronique de la lettre est conservée dans ASSMAL.
- Les demandes pour la reconnaissance d'une maladie grave doivent être envoyées aux médecins- conseils, en joignant un rapport médical détaillé. Le personnel travaillant pour les médecins-conseils *scanne* les informations dans ASSMAL. Lors de l'analyse des documents, le médecin-conseil délivre un avis *recommandant ou non* l'autorisation à accorder. Cet avis est conservé dans ASSMAL. Le responsable du bureau liquidateur délivre une autorisation officielle, qui est ensuite transmise au demandeur. Chaque autorisation reçoit un numéro de référence.
- Les formulaires de déclaration confidentielle doivent être complétés pour déterminer si les conjoints/partenaires peuvent être couverts au titre du régime d'assurance maladie. Comme le formulaire se présente actuellement, les conjoints/partenaires sont invités à fournir des informations sur leur situation professionnelle, y compris le nom de leur employeur, et doivent également indiquer s'ils perçoivent une pension ou un revenu. En outre, ils sont invités à indiquer le montant de leurs revenus annuels, d'origine professionnelle ou provenant d'une pension, etc., et à préciser s'ils peuvent être couverts contre les risques de maladie par un régime primaire d'assurance maladie légal ou réglementaire autre que celui des C.E. Ces renseignements sont fournis par les affiliés sur papier au bureau liquidateur qui introduira certaines des informations dans ASSMAL.

Si les opérations de traitement des données ci-dessus ont une composante manuelle, toutes sont reprises dans des documents électroniques et ***automatisées.*** Il s'agit notamment des opérations suivantes:

- Archivage électronique dans la base de données ASSMAL de l'ensemble des documents ayant été scannés après réception, y compris les formulaires de demande, les copies des prescriptions établies par les médecins, les déclarations de frais originales. Cet archivage est réalisé par le personnel du bureau liquidateur (demandes de remboursement de frais médicaux) ou par le personnel travaillant avec le médecin-conseil (reconnaissance de maladies graves et demandes d'autorisation préalable).

- Encodage des dépenses et évaluations de ces dernières en fonction de la tarification; archivage ultérieur dans ASSMAL.
- Archivage électronique dans la base de données ASSMAL des recommandations/avis des médecins-conseils concernant les autorisations préalables et la reconnaissance de maladies graves.
- Élaboration des listes de paiement et des ordres de paiement correspondants qui sont ensuite transmis par voie électronique à la DG BUDGET aux fins du paiement par le biais du compte bancaire des membres du personnel de l'UE.
- Archivage électronique des documents tels que les accords sur les prises en charge, les déclarations confidentielles, les autorisations de traitement, y compris les traitements dentaires, les autorisations de reconnaissance de maladies graves.

L'accès à ASSMAL repose sur le besoin d'en connaître. Ainsi, le personnel du bureau liquidateur n'a pas accès aux états pathologiques sous-jacents introduits dans ASSMAL par les médecins-conseils. Par exemple, en ce qui concerne les recommandations/avis des médecins-conseils quant aux autorisations préalables et reconnaissances de maladies graves, les personnes autres que les médecins-conseils ne pourront voir dans ASSMAL que si la recommandation a été acceptée ou non (c'est-à-dire "oui" ou "non").

Les personnes concernées sont les suivantes: *i)* membres, fonctionnaires des institutions et agences de l'UE; *ii)* agents temporaires des institutions et agences de l'UE; *iii)* agents contractuels des institutions et agences de l'UE, *iv)* personnel à la retraite et, *v)* conjoints/partenaires reconnus, enfants, personnes assimilées à un enfant à charge.

Outre ce qui précède, parmi les autres personnes concernées dont les informations sont également traitées figurent les noms des médecins extérieurs, par exemple ceux qui délivrent les prescriptions, ainsi que ceux des médecins-conseils de la Commission.

Parmi les ***catégories de données à caractère personnel*** collectées figurent: *i)* les données relatives aux affiliés du régime d'assurance maladie: membre du personnel de l'UE, institution pour laquelle il/elle travaille, adresse administrative et adresse personnelle si la personne est à la retraite, date de naissance, type de bénéficiaire (s'il s'agit d'un agent, d'un enfant à charge ou équivalent ou d'un conjoint); *ii)* informations relatives au compte bancaire sur lequel les paiements doivent être effectués, *iii)* informations relatives au salaire; et *iv)* informations relatives à la santé des assurés (prescriptions de médecins, déclarations de frais liés à l'achat de produits pharmaceutiques, rapports médicaux, etc). Dans chaque cas, le fait qu'une catégorie particulière de données soit collectée dépendra des particularités du cas. Ainsi, les informations relatives au salaire sont utilisées uniquement aux fins de l'application de l'article 72, paragraphe 3, du statut[3].

Pour ce qui est de la conservation des données, les dossiers papiers relatifs aux états pathologiques sous-jacents des personnes couvertes (tels que les documents fournis à l'appui d'une maladie grave) sont conservés pendant toute la durée de vie de l'affilié plus cinq ans. Ils sont conservés pendant deux ans dans les bureaux du PMO/3, après quoi ils sont conservés dans les archives centrales de la Commission, compte tenu de l'espace limité disponible dans les locaux du PMO/3. Les dossiers papiers ayant trait aux demandes de remboursement de frais médicaux sont détruits après un délai total de 7 ans.

[3] L'article 72, paragraphe 3, établit que si le montant des frais non remboursés pour une période de douze mois dépasse la moitié du traitement mensuel de base du fonctionnaire ou de la pension versée, un remboursement spécial est accordé par l'autorité investie du pouvoir de nomination, compte tenu de la situation de famille de l'intéressé, sur la base de la réglementation prévue au paragraphe 1.

Comme cela été expliqué ci-dessus, outre les formulaires papier, tous les dossiers électroniques, y compris les demandes de remboursement de frais médicaux, sont conservés dans la base de données ASSMAL, qui est hébergée au Luxembourg. Les informations contenues dans ASSMAL sont conservées pendant la durée de vie de l'affilié plus cinq ans.

Le responsable du traitement des données, le PMO/3, peut ***transférer des données à caractère personnel*** aux destinataires ci-après, qui sont tous des institutions ou organes communautaires: *i)* la DG BUDGET qui effectue le paiement des montants dus par le biais du compte bancaire du membre du personnel de l'UE; *ii)* PMO Rémunérations qui recouvre sur les salaires des montants qui ont été avancés dans le cadre des hospitalisations et *iii)* le médecin-conseil, le comité de gestion et l'unité ADMIN.B.2 dans le cadre des deux procédures ci-après, en particulier:

i) le conseil médical peut être consulté par le comité de gestion ou le bureau central sur toute question de nature médicale qui se poserait dans le cadre du régime d'assurance maladie. Dans le cadre d'une consultation, des données à caractère personnel peuvent être transmises au conseil médical par le PMO/3[4].

ii) lorsqu'une décision prise par le PMO/3 au sujet du régime d'assurance maladie donne lieu à une plainte, une réclamation peut être introduite et en vertu de l'article 90, paragraphe 2, du statut. Dans ces conditions, conformément à l'article 16 de la réglementation commune relative à la couverture des risques de maladie des fonctionnaires des Communautés européennes ("réglementation commune relative à la couverture des risques de maladie", décrite plus en détail à la section 2.2.2 ci-dessous), l'autorité investie du pouvoir de nomination doit demander l'avis du comité de gestion avant de prendre une décision sur une réclamation. Cet avis, qui n'est pas contraignant, est transmis simultanément à l'autorité et à l'intéressé. Dans de tels cas, le comité de gestion recevra du PMO/3 la réclamation ainsi que les informations médicales sous-jacentes. Ces informations pourront être complétées par les informations fournies par le médecin-conseil. Étant donné que la DG ADMIN B 2 est responsable de la gestion des recours introduits sur la base de l'article 90, paragraphe 2, du Statut, elle peut également recevoir des informations directement de l'affilié.

Pour ce qui est du ***droit à l'information***, la notification mentionne une déclaration de confidentialité visant à fournir des renseignements aux affiliés du régime d'assurance maladie. La déclaration de confidentialité est disponible sur le site intranet de la Commission, dans la section "Assurance maladie et accidents": http://intracomm.cec.eu-admin.net/pers_admin/sick_insur/index_fr.html.

La déclaration de confidentialité contient notamment des informations sur l'identité du responsable du traitement, les finalités du traitement et l'existence d'un droit d'accès. Elle indique également les durées de conservation des données et les références à la base légale

---

[4] Le rôle du ***conseil médical*** est prévu par l'article 22 de la réglementation commune relative à la couverture des risques de maladie. L'article 22, paragraphe 2, prévoit notamment que "le conseil médical peut être consulté par le comité de gestion ou le bureau central sur toute question de nature médicale qui se poserait dans le cadre du présent régime. Il se réunit à la demande du comité de gestion ou du bureau central ou à la demande d'un des médecins-conseils des bureaux liquidateurs et émet son avis dans le délai qui lui est indiqué". Le conseil médical est composé d'un médecin-conseil par institution et des médecins-conseils de chaque bureau liquidateur. Le rôle du ***comité de gestion*** est prévu par l'article 18 de la réglementation relative à la couverture des risques de maladie, qui définit les membres du comité et leurs fonctions. Le comité est notamment chargé d'émettre son avis sur toute question relevant, directement ou indirectement, de l'application des dispositions statutaires en matière de couverture des risques de maladie; il est également chargé d'émettre son avis sur le niveau des contributions et prestations prévues, notamment en cas de variation sensible des coûts des soins médicaux.

applicable. Le ***droit d'accès*** et les procédures pour l'exercer sont reconnus dans la déclaration de confidentialité. Celle-ci ne contient aucune référence au ***droit de rectification***.

Des mesures de sécurité sont mises en œuvre.

2.2. Aspects juridiques

2.2.1. Contrôle préalable

Le présent avis sur la notification en vue d'un contrôle préalable porte sur la gestion du régime d'assurance maladie réalisée par le PMO, conformément à l'article 72 du statut et à l'article 28 du régime applicable aux autres agents des Communautés européennes. En conséquence, l'avis évaluera dans quelle mesure les opérations de traitement des données décrites ci-dessus effectuées par le PMO/3 sont conformes au règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (ci-après dénommé "règlement (CE) n° 45/2001" ou "le règlement").

Conformément à ce qui précède, le présent avis ne traitera pas des opérations de traitement de données réalisées par le PMO/3 dans le cadre de la gestion de l'assurance contre les risques de maladie professionnelle et les risques d'accident, conformément à l'article 73 du statut. Celle-ci fera l'objet d'un avis distinct actuellement analysé séparément par le CEPD . En outre, le présent avis n'évaluera pas les opérations de traitement des données qui peuvent être réalisées par les autres organes/institutions susceptibles de recevoir des informations collectées initialement par le PMO/3 dans le cadre de la gestion du régime d'assurance maladie et pour lesquelles ces organes peuvent être responsables du traitement. Par exemple, c'est le cas du traitement réalisé par la DG ADMIN B 2 dans le cadre de la gestion des recours introduits sur la base de l'article 90 du statut ou par le comité de gestion dans le cadre de ses attributions.

Applicabilité du règlement. Le règlement (CE) n° 45/2001 s'applique au *"traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier*" et au traitement "*par toutes les institutions et tous les organes communautaires, dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire.*"[5]. Pour les raisons indiquées ci-dessus, tous les éléments qui déclenchent l'application du règlement sont réunis:

Tout d'abord, la gestion du régime d'assurance maladie implique la collecte et le traitement ultérieur de *données à caractère personnel* tel que définies à l'article 2, point a), du règlement (CE) n° 45/2001. En effet, comme indiqué dans la notification, les données à caractère personnel des affiliés qui exercent leurs droits dans le cadre du régime d'assurance maladie sont collectées et traitées ultérieurement. Il s'agit notamment d'informations liées à la santé des membres du personnel de l'UE telles que des prescriptions de médecins, des déclarations de frais liés à l'achat de produits pharmaceutiques, des informations relatives aux traitements médicaux, etc.

Ensuite, comme le décrit la notification, les données à caractère personnel collectées subissent des opérations de *"traitement automatisé"*, telles que définies à l'article 2, point b), du règlement (CE) n° 45/2001 ainsi que des opérations de traitement manuel. En effet, les

[5] Voir l'article 3 du règlement (CE) n° 45/2001.

informations à caractère personnel sont tout d'abord collectées au format papier directement auprès des membres du personnel de l'UE. Dans la plupart des cas, les informations sont scannées et conservées dans une base de données.

Enfin, le traitement est effectué par une institution communautaire, en l'espèce le PMO/3, qui fait partie de la Commission européenne, dans le cadre du droit communautaire (Article 3, paragraphe 1, du règlement (CE) n° 45/2001). C'est pourquoi l'ensemble des éléments qui déclenchent l'application du règlement sont réunis dans la gestion du régime d'assurance maladie.

Motif de procéder à un contrôle préalable. L'article 27, paragraphe 1, du règlement (CE) n° 45/2001 soumet au contrôle préalable du contrôleur européen de la protection des données *"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, paragraphe 2, du règlement fournit une liste des traitements susceptibles de présenter de tels risques. Cette liste comprend notamment, au paragraphe a), les traitements de données relatives à la santé. Les données collectées en liaison avec la gestion du régime d'assurance maladie constituent des données relatives à la santé. C'est pourquoi les opérations de traitement doivent faire l'objet d'un contrôle préalable par le CEPD.

Contrôle préalable ex-post. Puisque le contrôle préalable vise à traiter des situations susceptibles de présenter des risques particuliers, le CEPD devrait rendre son avis avant le début de l'opération de traitement. En l'espèce, toutefois, les opérations de traitement ont déjà été mises en place. Il ne s'agit pas d'une difficulté insurmontable dans la mesure où toutes les recommandations formulées par le CEPD seront pleinement prises en compte et les opérations de traitement seront ajustées en conséquence.

Notification et date à laquelle l'avis du CEPD est attendu. La notification a été reçue le 6 mars 2007. Conformément à l'article 27, paragraphe 4, du règlement (CE) n° 45/2001, le délai de deux mois au cours duquel le CEPD doit rendre son avis a été suspendu pendant une durée totale de 66 jours. L'avis doit par conséquent être adopté au plus tard le 11 juillet 2007.

2.2.2. Licéité du traitement

Le traitement de données à caractère personnel ne peut être effectué que si des fondements juridiques peuvent être trouvés dans l'article 5 du règlement (CE) n° 45/2001. Comme cela est souligné dans la notification, les fondements justifiant l'opération de traitement s'appuient sur l'article 5, point a), conformément auquel le traitement de données ne peut être effectué que si 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".*

Afin de déterminer si les opérations de traitement sont conformes à l'article 5, point a), du règlement (CE) n° 45/2001, deux éléments doivent être pris en compte: tout d'abord, si le traité ou d'autres actes législatifs prévoient une mission dans l'intérêt public, et ensuite si les opérations de traitement effectuées par le PMO/3 sont bien nécessaires à l'exécution de cette mission.

Base juridique. Afin de déterminer les fondements juridiques qui, dans le traité ou d'autres actes législatifs, rendent légitimes les opérations de traitement effectuées dans le cadre de la gestion du régime d'assurance maladie, le CEPD prend note de l'article 72 du statut.

Conformément à ce qui est illustré ci-dessus, cet article définit la couverture des fonctionnaires de l'UE au titre de l'assurance maladie.

En particulier, l'article 72 du statut prévoit que "*dans la limite de 80% des frais exposés, et sur la base d'une réglementation établie d'un commun accord par les institutions des Communautés après avis du comité du statut, le fonctionnaire, son conjoint {....}, ses enfants et les autres personnes à sa charge au sens de l'article 2 de l'annexe VII, sont couverts contre les risques de maladie*". L'article 72 prévoit en outre que "*ce taux est relevé à 85% pour les prestations suivantes: consultations et visites, interventions chirurgicales, hospitalisation, produits pharmaceutiques, radiologie, analyses, examen de laboratoire et prothèses sur prescription médicale à l'exception des prothèses dentaires. Il est porté à 100 % en cas de tuberculose, poliomyélite, cancer, maladie mentale et autres maladies reconnues de gravité comparable par l'autorité investie du pouvoir de nomination, ainsi que pour les examens de dépistage et en cas d'accouchement. Toutefois, les remboursements prévus à 100 % ne s'appliquent pas en cas de maladie professionnelle ou d'accident ayant entraîné l'application de l'article 73."* Le CEPD note également que conformément à l'article 72 ci-dessus, le 16 juin 2004, les institutions ont adopté la réglementation commune relative à la couverture des risques de maladie des fonctionnaires des Communautés européennes. Cette réglementation définit notamment les règles procédurales visant à garantir le remboursement des frais, et les règles relatives au choix du médecin et de l'établissement de soins.

La législation ci-dessus, qui concerne les fonctionnaires des institutions de l'UE, est complétée par l'article 28 du régime applicable aux autres agents. L'article 28 prévoit notamment que "*les articles 72 et 73 du statut concernant les régimes de couverture des risques de maladie et d'accident sont applicables par analogie à l'agent temporaire pendant la période de ses fonctions, pendant ses congés de maladie et pendant les périodes de congé sans rémunération prévues à l'article 11 ainsi qu'à l'article 17 …*; *l'article 72 du statut concernant le régime de couverture des risques de maladie est applicable par analogie à l'agent titulaire d'une allocation d'invalidité ainsi qu'au titulaire d'une pension de survie. L'article 72 est également applicable à l'agent visé à l'article 39 paragraphe 2 et titulaire d'une pension d'ancienneté.".*

Lors de l'analyse du cadre juridique ci-dessus, le CEPD estime que le traitement des données réalisé en liaison avec la gestion du régime d'assurance maladie est effectué sur la base i) du statut (Article 72), ii) du régime applicable aux autres agents (Article 28) et iii) de la réglementation commune relative à la couverture des risques de maladies. Ces instruments juridiques prévoient que les fonctionnaires et autres agents bénéficient de la couverture des risques de maladies dans certaines conditions. Afin de mettre en oeuvre cette obligation, les institutions mettent en place un régime d'assurance maladie dont la gestion implique le traitement de données à caractère personnel. En conclusion, le régime d'assurance maladie est fondé juridiquement sur les instruments juridiques ci-dessus.

Test de nécessité. Conformément à l'article 5, point a), du règlement (CE) n° 45/2001, le traitement de données doit être "*nécessaire à l'exécution d'une mission*" comme indiqué ci-dessus. Par conséquent, il y a lieu d'évaluer si le traitement des données effectué dans le cadre du régime d'assurance maladie est "*nécessaire"* à l'exécution d'une mission, en l'espèce, à la gestion du régime d'assurance maladie.

Comme indiqué ci-dessus, en vertu du statut, les fonctionnaires et autres agents ont droit à bénéficier d'une assurance contre les risques de maladie, dans les conditions définies par cette législation. Les institutions sont dans l'obligation de fournir cette couverture aux fonctionnaires et autres agents de l'UE. Pour mettre en œuvre cette obligation, les institutions

sont tenues de mettre en place un régime d'assurance maladie. Pour qu'un tel régime fonctionne et soit géré de manière appropriée, il est nécessaire que les gestionnaires du régime traitent des données à caractère personnel. Cela est dû au fait que la bonne gestion du système nécessite notamment de veiller à ce que les personnes couvertes par le régime soient remboursées. À cet effet, il est nécessaire d'identifier les affiliés au régime. En outre, pour garantir que ces affiliés soient remboursés conformément à la réglementation, le régime doit collecter les informations relatives aux maladies/traitements des assurés. Seule la collecte de ces informations permettra la gestion du régime, en vérifiant si les affiliés sont couverts ou non pour certains risques/produits et le cas échéant dans quelle mesure. En conclusion, le CEPD estime que le traitement de données réalisé dans le cadre du régime d'assurance maladie peut être considéré comme nécessaire à la bonne gestion du régime.

2.2.3. Traitement portant sur des catégories particulières de données

Le traitement des données à caractère personnel relatives à la santé est interdit, à moins que des motifs puissent être trouvés à l'article 10, paragraphes 2 et 3, du règlement. L'article 10, paragraphe 2, point b), du règlement établit que l'interdiction ne s'applique pas lorsque le traitement est *"nécessaire afin de respecter les obligations et les droits spécifiques du responsable du traitement en matière de 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*".

Conformément aux explications ci-dessus relatives à la base juridique, la justification du traitement des données à caractère personnel dans le cadre du régime d'assurance maladie, y compris les données relatives à la santé, peut être trouvée dans le statut. Le traitement est effectué en application de l'obligation qu'a l'employeur de fournir une assurance contre le risque de maladie. C'est pourquoi le traitement relève de l'article 10, paragraphe 2, point b), et n'est pas interdit.

Étant donné qu'il s'agit d'une exception à une interdiction générale, l'article 10, paragraphe 2, point b), doit être interprété de manière stricte. L'article 10, paragraphe 2, point b), prévoit notamment, pour que l'exception s'applique, que le traitement doit être "*nécessaire*" afin de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail. Ainsi, le traitement de données sensibles est autorisé uniquement dans la mesure où il est pertinent et nécessaire pour assurer le régime d'assurance maladie. La question de la nécessité est abordée ci-dessous plus en détail, lors de l'examen de l'article 4, paragraphe 1, point d), du règlement, qui porte sur la qualité des données.

L'interdiction énoncée à l'article 10, paragraphe 3, ne s'applique pas non plus au traitement des données relatives à la santé effectué par les médecins-conseils, par exemple dans le cadre de l'autorisation préalable ou de la reconnaissance de maladie grave: *"Le paragraphe 1 ne s'applique pas lorsque* [...] *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"*. La même exception s'applique au personnel travaillant pour le PMO/3, y compris le bureau liquidateur, conformément à l'article 20 de la réglementation commune relative à la couverture des risques de maladie: "*Les agents affectés aux bureaux liquidateurs et au bureau central sont astreints au secret médical quant aux frais et/ou pièces dont ils ont connaissance à l'occasion de l'exercice de leurs fonctions* [...]*"*.

À cet égard, le CEPD recommande que le PMO/3 sensibilise son personnel non médical à l'application du secret médical. Cela revêt une importance capitale pour le personnel non médical étant donné que, contrairement aux médecins, ils sont uniquement liés par les règles

relatives au secret médical au titre de l'article 20, paragraphe 4, de la réglementation commune relative à la couverture des risques de maladie, et non du fait de leur titre professionnel. Cela signifie qu'ils ne sont pas soumis à une autorité externe d'autorégulation en matière d'éthique professionnelle, telle qu'un ordre des médecins national. La réglementation commune relative à la couverture des risques de maladie ne prévoit pas non plus un ensemble détaillé de règles relatives au secret médical semblable à ce qui existe au niveau national. Plus important encore peut-être, les médecins ont reçu une formation exhaustive sur les questions relatives à l'éthique médicale, y compris le secret médical. Il y a une différence énorme entre, d'une part, la connaissance du secret médical et l'engagement à cet égard d'un médecin qui a prêté le serment d'Hippocrate et, d'autre part, le personnel comptable et administratif qui n'a jamais reçu de formation officielle sur les questions liées au secret médical et qui est soumis uniquement aux exigences du secret médical en vertu d'un article de la réglementation commune relative à la couverture des risques de maladie qu'il a peut-être uniquement survolée de manière superficielle.

Pour ces motifs, le CEPD recommande que l'ensemble du personnel du PMO/3 et le reste du personnel non médical ayant accès aux données médicales reçoivent une formation appropriée et complète sur les questions de secret médical. Ils devraient également être tenus de déclarer par écrit qu'il ont reçu une formation et s'engagent à respecter leurs obligations en matière de confidentialité.

2.2.4. Qualité des données

Adéquation, pertinence et proportionnalité. Conformément à l'article 4, paragraphe 1, point c), du règlement (CE) n° 45/2001, 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 s'agit là du principe de la qualité des données.

Certaines des informations demandées aux affiliés du régime d'assurance maladie doivent être fournies par le biais de formulaires normalisés à remplir et à accompagner de prescriptions et/ou de rapports médicaux. Cela s'applique par exemple aux demandes de remboursement, aux déclarations d'accidents et aux demandes d'autorisation préalable. Le CEPD n'a relevé dans les formulaires aucune demande d'informations qui serait de prime abord non pertinente ou excessive, à l'exception de ce qui est examiné ci-dessous (déclaration confidentielle).

Néanmoins, compte tenu du fait que les informations médicales sensibles seront contenues essentiellement dans les rapports médicaux et les prescriptions, le fait de savoir si les informations fournies sont excessives ou non dépendra de chaque cas d'espèce. Afin de garantir que les informations fournies dans ces rapports/prescriptions demeurent adéquates, pertinentes et non excessives, il peut être judicieux de fournir des lignes directrices relatives au contenu de ces rapports/prescriptions. Ces lignes directrices pourraient ainsi énumérer les points nécessaires pour que le PMO/3 puisse répondre, effectuer un paiement ou autoriser un traitement donné. Ces lignes directrices constitueraient des indications pour les médecins leur précisant quelles informations sont nécessaires dans le cadre du régime d'assurance maladie. Cela pourrait contribuer à la communication d'informations adéquates et pertinentes. En outre, si des informations non pertinentes sont néanmoins fournies à l'appui d'une demande particulière, le PMO/3 et le bureau des médecins-conseils devraient donner pour instruction à leur personnel de ne pas introduire ces informations dans ASSMAL.

Le CEPD se félicite de la pratique suivie dans le cadre de la demande pour reconnaissance de maladie grave. Dans ce type de procédure, les affiliés du régime d'assurance maladie sont

invités à envoyer des rapports médicaux au format papier aux *médecins-conseils* et non à d'autres membres du personnel du PMO/3. Le CEPD estime qu'une procédure similaire devrait être suivie en ce qui concerne les rapports médicaux qui accompagnent les demandes d'autorisation préalable. Afin de garantir que ces informations sont adressées au médecin-conseil et que les données parviennent bien à leurs destinataires, et par conséquent ne subissent pas un traitement qui irait à l'encontre du principe de la qualité des données, les affiliés devraient être tenus de fournir les renseignements sous pli fermé portant la mention "confidentiel", "à ouvrir uniquement par le destinataire" ou équivalente. Cela est particulièrement important en ce qui concerne les rapports médicaux qui accompagnent les demandes d'autorisation préalable et de reconnaissance de maladie grave. Les affiliés devraient être informés qu'il est important de suivre cette pratique lorsqu'ils envoient des informations au PMO/3 et au médecin-conseil. Le CEPD estime que le site web et la déclaration de confidentialité devraient être modifiés afin d'inviter les membres du personnel de l'UE à suivre ces lignes directrices lorsqu'ils envoient des informations médicales. En outre, si le bureau liquidateur reçoit des informations destinées au médecin-conseil, et qui ne sont pas marquées comme telles, celles-ci devraient être transmises à nouveau sous pli fermé.

Outre ce qui précède, afin de garantir que l'accès aux rapports médicaux soit strictement limité au médecin-conseil, le PMO/3 devrait s'assurer que les droits d'accès à ASSMAL sont définis sur la base du besoin d'en connaître et définir des procédures strictes pour éviter les accès non autorisés.

Formulaire de déclaration confidentielle. Le CEPD estime que les informations contenues dans le formulaire de déclaration confidentielle sont pertinentes et adéquates afin de déterminer si les conjoints/partenaires peuvent être couverts par le régime d'assurance maladie de l'UE. Néanmoins, compte tenu du fait qu'une telle couverture n'est pas obligatoire - autrement dit c'est aux partenaires/conjoints qu'il revient d'accepter ou de refuser la couverture découlant du régime d'assurance maladie - ils ne devraient être tenus de fournir aucune information dans les cas où aucune couverture n'est demandée (par exemple, le partenaire/conjoint ne souhaite bénéficier d'aucune couverture). Par conséquent, les CEPD recommande de modifier le formulaire pour préciser que ces informations sont nécessaires uniquement si les partenaires/conjoints souhaitent bénéficier de leur couverture éventuelle au titre du régime d'assurance maladie. À l'inverse, si les partenaires/conjoints souhaitent bénéficier de cette couverture, ils doivent compléter le formulaire. Étant donné que le formulaire est complété et signé non pas par le conjoint/partenaire mais par le membre du personnel de l'UE, la question peut se poser de savoir s'il s'agit d'une collecte licite de ces informations. Le CEPD estime qu'en communiquant ces informations dans le formulaire, les membres du personnel de l'UE doivent avoir précédemment informé leurs conjoints/partenaires et en avoir obtenu le consentement. Pour garantir que c'est bien le cas, le CEPD recommande de modifier le formulaire pour préciser qu'il est entendu pour le PMO/3 que le partenaire/conjoint est informé des finalités du traitement des informations le concernant et a consenti à leur transfert et à leur traitement ultérieur par le PMO/3.

Loyauté et licéité. L'article 4, paragraphe 1, point a), du règlement exige que les données soient traitées loyalement et licitement. La question de la licéité a été analysée ci-dessus (voir section 2.2.2). La question de la loyauté est étroitement liée à celle des informations qui sont communiquées aux personnes concernées, question qui est traitée plus en détail dans la section 2.2.7.

Exactitude. Conformément à l'article 4, paragraphe 1, point d), du règlement, les données à caractère personnel 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". En l'espèce, les données comprennent les rapports médicaux, les prescriptions, les reçus de frais médicaux, etc. Étant donné la nature de la plupart de ces données, il n'est pas facile d'en prouver l'exactitude. Toutefois, le CEPD souligne que le PMO/3 doit néanmoins prendre toutes les mesures raisonnables pour garantir que les données soient à jour et pertinentes. Sur ce point, voir également la section 2.2.8.

2.2.5. Conservation des données

Conformément à l'article 4, paragraphe 1, point e), du règlement (CE) n° 45/2001, les données à caractère personnel 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.

Le CEPD remarque certaines incohérences entre les informations fournies dans la notification et celles contenues dans la déclaration de confidentialité en ce qui concerne la durée de conservation des données.

Le CEPD croit comprendre que le PMO/3 conserve les documents liés aux états pathologiques sous-jacents des assurés (documents fournis à l'appui d'une maladie grave et rapports accompagnant les autorisations préalables) au format papier pendant la durée de vie du membre du personnel de l'UE plus cinq ans et détruit les demandes de remboursement de frais médicaux et les factures correspondantes après un délai de 7 ans.

Le CEPD estime que la durée de conservation de sept ans est raisonnable puisqu'il s'agit de la durée approximative pendant laquelle les pièces justificatives doivent être conservées au titre du règlement financier. En effet, l'article 49 du règlement financier, tel que modifié en 2007, établit que *"les systèmes et procédures de gestion concernant la conservation des pièces justificatives originales prévoient: d) la conservation de ces pièces pendant une période de cinq ans au moins à compter de la date d'octroi de la décharge par le Parlement européen pour l'année budgétaire à laquelle ces pièces se rapportent. Les pièces relatives à des opérations non définitivement clôturées sont conservées au-delà de la période prévue au premier alinéa, point d), et jusqu'à la fin de l'année suivant celle de la clôture desdites opérations"*[6]. Le CEPD souhaiterait toutefois appeler l'attention du PMO/3 sur le dernier alinéa de l'article 49 du règlement financier selon lequel *"les données à caractère personnel contenues dans les pièces justificatives sont supprimées si possible lorsqu'elles ne sont pas nécessaires aux fins de la décharge budgétaire, du contrôle et de l'audit"* et invite le PMO/3 à déterminer si ce cas permet la suppression des données à caractère personnel figurant parmi les pièces justificatives à des stades antérieurs.

Le CEPD est préoccupé par la pratique consistant à conserver certaines informations cinq ans après la date du décès du membre du personnel de l'UE concerné. En règle générale, en ce qui concerne la conservation des données médicales, le CEPD considère que 30 ans est le délai maximal absolu pendant lequel les données devraient être conservées dans ce contexte. Le CEPD invite le PMO/3 à évaluer dans quelle mesure et à quelles fins les données qu'il détient au sujet des membres du personnel de l'UE doivent être conservées pendant la durée de vie de

[6] Règlement (CE, Euratom) n° 478/2007 de la Commission du 23 avril 2007 modifiant le règlement (CE, Euratom) n° 2342/2002 établissant les modalités d'exécution du règlement (CE, Euratom) no 1605/2002 du Conseil portant règlement financier applicable au budget général des Communautés européennes, JO L 111 du 28.4.2007.

l'affilié plus cinq ans. À ce titre, le CEPD appelle l'attention du PMO sur ses recommandations publiées le 26 février 2007 dans l'affaire 2006-532 en réponse à la consultation du Collège des chefs d'administration et concernant la proposition du Collège de conserver l'ensemble des documents médicaux au sein des institutions communautaires pendant une période uniforme de 30 ans[7]. Dans ses recommandations, le CEPD a invité le Collège des chefs d'Administration à réévaluer son initiative et à examiner au cas par cas, quels délais de conservation sont nécessaires pour les différents types de documents médicaux, en tenant compte du fait que l'article 4, paragraphe 3, du règlement prévoit que les données doivent être conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées.

La déclaration de confidentialité ne fait référence qu'à la durée de stockage des informations conservées sur papier, mais reste muette quant au stockage électronique. Pourtant, l'ensemble des données traitées par le PMO/3, même les données conservées sur papier qui sont détruites après sept ans, sont également conservées sous forme électronique dans ASSMAL et sont conservées jusqu'à 5 ans après le décès de l'affilié. Le CEPD estime que les données conservées dans ASSMAL devraient être soumise aux mêmes délais de conservation que les données conservées au format papier. Les raisons qui justifient la conservation des données pendant une certaine durée sont les mêmes pour le papier et les formats électroniques. C'est pourquoi les règles de conservation devraient être harmonisées.

Conformément à ce qui précède, pour ce qui est des données papier et des données conservées au format électronique, un système devrait être élaboré qui permettrait de détruire les informations au bout d'un certain délai. Ce principe devrait être pris en compte notamment dans le cadre des prochaines évolutions du nouveau ASSMAL.

Par ailleurs, le CEPD estime que la déclaration de confidentialité devrait être complétée pour décrire la durée de conservation des données conservées dans ASSMAL. Cela permettrait non seulement de fournir des renseignements sur la conservation mais, conformément à ce qui est décrit ci-dessous, cela préciserait également que les informations sont conservées sous forme électronique et au format papier.

2.2.6. Transferts de données

Les articles 7, 8 et 9 du règlement (CE) n° 45/2001 établissent certaines obligations qui s'appliquent lorsque les responsables du traitement transfèrent des données à caractère personnel à des tiers. Les règles diffèrent selon que le transfert est effectué i) à des institutions ou organes communautaires (conformément à l'article 7), ii) à des destinataires relevant de la directive 95/46/CE (conformément à l'article 8), iii) ou à d'autres types de destinataires (conformément à l'article 9).

Selon la notification, le transfert des informations est limité i) à la DG BUDGET pour qu'elle exécute le paiement des sommes dues par l'intermédiaire du compte bancaire du membre du personnel de l'UE , ii) au PMO Rémunérations pour qu'il recouvre sur les salaires les montants ayant été avancés dans le cadre de l'hospitalisation, et iii) au conseil médical, au comité de gestion et à l'unité ADMIN.B.2 dans le cadre des recours.

[7] Disponible à l'adresse: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/07-02-26_conservation_documents_medicaux_FR.pdf

Tous les transferts sont effectués entre institutions ou organes communautaires ou en leur sein, aussi l'article 7 du règlement s'applique-t-il. Aucun transfert de données n'est effectué à des destinataires relevant de la directive 95/46 ou à d'autres types de destinataires; c'est pourquoi les articles 8 et 9 du règlement ne s'appliquent pas.

L'article 7 du règlement (CE) n° 45/2001 prévoient que les données à caractère personnel ne peuvent faire l'objet de transferts "*que si elles sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire"*. Afin de respecter cette disposition, lorsqu'il transfère des données à caractère personnel, le PMO/3 doit s'assurer que *i)* le destinataire a les compétences appropriées et *ii)* le transfert est nécessaire.

Le CEPD estime que les transferts d'informations à la DG BUDGET et au PMO Rémunérations avec les finalités énoncées ci-dessus remplissent ces conditions. Dans les deux cas, les destinataires ont la compétence pour exécuter la mission pour laquelle les données sont transférées, à savoir exécuter le paiement des sommes dues via le compte bancaire du membre du personnel de l'UE et recouvrir sur les salaires des montants qui ont été avancés dans le cadre des hospitalisations. En outre, dans les deux cas, les transferts de données sont nécessaires pour que les destinataires exécutent leur mission, sous réserve que les données adressées à la DG BUDGET et au PMO Rémunérations soient limitées à ce qui est strictement nécessaire pour l'exécution de leur mission. Dans les deux cas, le type d'informations à transférer devrait être limité aux informations d'identification du membre du personnel de l'UE, aux informations relatives à son compte bancaire et à son salaire. Aucune donnée relative à la santé ne devrait être transférée au PMO et à la DG BUDGET étant donné que ces informations ne sont pas nécessaires à l'exécution de leur mission.

Les transferts de données à caractère personnel peuvent également avoir lieu à destination du comité de gestion, du conseil médical et de la DG ADM B 3 dans le cadre de la procédure de recours prévue par l'article 90, paragraphe 2, du statut. Le transfert des informations au comité de gestion est prévu à l'article 16 de la réglementation commune relative à la couverture des risques de maladie, qui établit que l'autorité investie du pouvoir de nomination ou, selon le cas, le conseil d'administration doit demander l'avis du comité de gestion avant de prendre une décision sur une réclamation. Il prévoit en outre que le comité de gestion peut demander un avis extérieur. Dans ces conditions, le comité de gestion peut également consulter le conseil médical.

Afin de prendre une décision, le comité de gestion et le conseil médical doivent disposer d'une description complète des faits. À ce sujet, le CEPD estime que les dispositions de l'article 7 sont respectées dans la mesure où les destinataires des informations ont besoin de les recevoir afin d'exécuter la mission pour laquelle ils sont compétents. Néanmoins, le CEPD se demande si le comité de gestion doit avoir accès aux informations d'identification afin d'accomplir sa mission. La transmission des informations d'identification à des personnes qui ne sont pas médecins ne semble pas nécessaire pour rendre un avis sur les questions procédurales et administratives. En outre, la transmission d'informations sensibles, par exemple le fait qu'un membre du personnel de l'UE souffre d'un cancer ou d'une maladie mentale, peut dissuader d'introduire un recours dans le cas de réclamations légitimes. Le CEPD est conscient du fait qu'en ignorant l'identité du patient, en théorie, les membres du comité de gestion peuvent ne pas repérer des conflits d'intérêts potentiels (par exemple, si la question examinée concerne un membre de la famille de l'un des membres du comité de gestion). En revanche, dans de tels cas, le membre du comité de gestion pourrait bien identifier le patient même sans disposer d'informations d'identification.

À la lumière du raisonnement décrit ci-dessus, le CEPD suggère que le PMO/3 supprime les informations d'identification relatives au plaignant avant de demander au comité de gestion

son avis en vertu de l'article 16 de la réglementation commune relative à la couverture des risques de maladie.

2.2.7. Droit d'accès et de rectification

Conformément à l'article 13 du règlement (CE) n° 45/2001, La personne concernée a le droit d'obtenir, sans contrainte, à tout moment dans un délai de trois mois à partir de la réception de la demande d'information et gratuitement, 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.

La déclaration de confidentialité confirme que le PMO/3 peut fournir les informations à caractère personnel. Elle établit en outre les dispositions à cet égard. Le CEPD se félicite que le PMO/3 autorise l'accès au dossier des membres du personnel de l'UE sans restrictions spécifiques. Le CEPD rappelle que l'accès ne saurait être limité aux "cas justifiés" et doit être autorisé pour n'importe quelle raison ou sans raison particulière. Les affiliés ne sauraient être tenus de préciser l'objet de leur demande. En outre, afin de garantir que les demandes d'accès seront traitées promptement et sans contrainte, il peut être s'avérer utile de fixer des délais raisonnables.

Le CEPD appelle l'attention du PMO/3 sur les conclusions 221/04 du 19 février 2004 du Collège des chefs d'administration, qui visent à harmoniser certains aspects des conditions d'accès dans toutes les institutions communautaires. Ce document souligne qu'il y a lieu de fournir un accès aussi large que possible aux informations médicales. Le document prévoit notamment d'autoriser l'accès aux rapports psychiatriques ou psychologiques, même si dans de tels cas l'accès peut être accordé de manière indirecte, par l'intermédiaire d'un médecin désigné par la personne concernée. À cet égard, le CEPD souhaite insister sur le fait que la règle générale demeure l'accès direct, dans tous les cas, qu'il s'agisse de la santé mentale ou physique. Cependant, en vertu de l'article 20, paragraphe 1, point c) du règlement (CE) n° 45/2001, l'accès aux données de nature psychologique ou psychiatrique peut être fourni de manière indirecte, si une évaluation réalisée au cas par cas révèle qu'un accès indirect est nécessaire pour garantir la protection de la personne concernée, compte tenu des circonstances en jeu[8].

L'article 14 du règlement prévoit que la personne concernée a le droit d'obtenir la rectification de données à caractère personnel inexactes ou incomplètes. Cela signifie que l'affilié devrait être en mesure de demander que les avis d'un autre médecin-conseil ou une décision d'un tribunal soient ajoutés dans son dossier afin de garantir que les dossiers sont exacts et complets. Le CEPD prie instamment le PMO de mettre en place les procédures appropriées pour permettre aux affiliés d'exercer leur droit de rectification.

2.2.8. Information de la personne concernée

Conformément aux articles 11 et 12 du règlement (CE) n° 45/2001, ceux qui collectent les données à caractère personnel sont tenus d'informer les individus que les données les concernant sont collectées et traitées. Les personnes concernées ont en outre le droit d'être informées, notamment, des finalités du traitement, des destinataires des données et des droits spécifiques dont les individus, ou personnes concernées, peuvent se prévaloir.

---

8 L'article 20 paragraphe 1, point c), du règlement (CE) n° 45/2001 est libellé comme suit: "*Les institutions et organes communautaires peuvent limiter l'application de l'article 4, paragraphe 1, de l'article 11, de l'article 12, paragraphe 1, des articles 13 à 17 et de l'article 37, paragraphe 1, pour autant qu'une telle limitation constitue une mesure nécessaire pour: c) garantir la protection de la personne concernée ou des droits et libertés d'autrui.*"

Afin de garantir le respect des dispositions de ces articles, le CEPD a été informé de l'existence d'une déclaration de confidentialité mise à la disposition des membres du personnel de l'UE par le biais du site intranet de la commission dans la section consacrée à l'assurance maladie.

Le CEPD a consulté le site intranet afin de vérifier si la déclaration de confidentialité est facilement accessible pour les personnes qui consultent le site pour y télécharger les formulaires dans lesquels des informations doivent être fournies. Les déclarations de confidentialité sont disponibles dans la première section où figure une introduction au régime d'assurance maladie. Même si le CEPD juge approprié de faire figurer une déclaration de confidentialité dans cette section, cela ne suffit peut-être pas. Les individus qui téléchargent les formulaires dans lesquelles les informations doivent être fournies ne consultent pas nécessairement la première page et par conséquent manquent la page web sur laquelle figure la déclaration de confidentialité. C'est pourquoi le CEPD suggère de faire figurer un lien vers la déclaration de confidentialité sur les pages où figurent les formulaires à télécharger. Cela permettra un accès direct à la déclaration de confidentialité à partir de la page web sur laquelle doit aller le membre du personnel de l'UE pour télécharger le formulaire. D'autre part, le fait d'insérer dans les formulaires eux-mêmes l'adresse URL de la déclaration de confidentialité contribuerait également au respect du principe d'information et de la transparence.

Le CEPD a également passé en revue le contenu des informations fournies dans la déclaration de confidentialité afin de vérifier si celui-ci satisfait aux exigences des articles 11 et 12 du règlement (CE) n° 45/2001.

La déclaration de confidentialité contient des informations sur l'identité du responsable du traitement, la finalité du traitement et la manière dont les données sont traitées, les conditions d'exercice du droit d'accès, la durée de conservation des données et la base légale régissant les opérations de traitement. Le CEPD estime que la déclaration de confidentialité contient la plupart des informations requises au titre des articles 11 et 12 du règlement, néanmoins il considère que plusieurs modifications contribueraient à garantir le strict respect des articles 11 et 12, notamment:

i) il n'est fait nulle part référence au fait que les données subissent un traitement automatique. Le CEPD estime que pour assurer un traitement loyal des données, la déclaration de confidentialité devrait mentionner que les informations fournies au PMO sont introduites dans une base de données électronique. Cela est nécessaire compte tenu du fait que les membres du personnel de l'UE sont invités à adresser les informations au format papier, et que rien n'indique donc aux affiliés que les informations qu'ils envoient sont conservées sous forme électronique;

ii) pour garantir une transparence totale et un traitement loyal, il serait judicieux d'ajouter l'adresse d'une personne de contact (celle du responsable du traitement ou quelqu'un de son unité) à laquelle les membres du personnel de l'UE pourraient envoyer des questions relatives à la déclaration de confidentialité;

iii) il n'est nulle part fait référence au droit de rectification et à la procédure permettant de l'exercer; ce droit devrait être ajouté dans la déclaration de confidentialité.

iv) comme indiqué ci-dessus, les informations relatives au délai de conservation des données ne concernent que les informations sur papier. Les références aux délais s'appliquant aux informations contenues dans ASSMAL devraient être ajoutées.

2.2.9. Mesures de sécurité

Conformément aux articles 22 et 23 du règlement (CE) n° 45/2001, le responsable du traitement et le sous-traitant doivent mettre 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. Ces mesures de sécurité doivent notamment empêcher toute diffusion ou tout accès non autorisés, toute destruction accidentelle ou illicite, toute perte accidentelle ou toute altération, ainsi que toute autre forme de traitement illicite.

Le CEPD estime que les mesures de sécurité adoptées par le PMO/3 sont appropriées à la lumière de l'article 22 du règlement. Conformément à ce qui est décrit à la section 2.2.4, le CEPD estime que le fait d'utiliser des plis fermés portant la mention "confidentiel", "à ouvrir uniquement par le destinataire" ou une mention équivalente aux fins de la transmission des données médicales serait une bonne pratique et une mesure appropriée pour garantir la confidentialité des informations. En outre, le CEPD estime qu'il serait également utile de conserver les fichiers-journaux de manière à tenir la liste des accès (et détecter les accès non autorisés) à ASSMAL.

3. 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 pour le PMO/3 de:

- sensibiliser son personnel non médical au secret médical, notamment par le biais d'une formation et la signature d'une déclaration de confidentialité spécifique,
- afin de garantir que les informations fournies dans les rapports médicaux soient adéquates, pertinentes et non excessives, prévoir des lignes directrices relatives au contenu de ces rapports,
- donner pour instruction aux membres du personnel de l'UE d'adresser les rapports médicaux étayant les demandes d'autorisation préalable aux médecins-conseils, comme c'est actuellement le cas pour les demandes pour la reconnaissance de maladies graves,
- donner pour instruction aux membres du personnel de l'UE d'adresser les rapports médicaux étayant les demandes pour la reconnaissance de maladie grave et les demandes d'autorisation préalable sous pli fermé portant la mention "confidentiel", et/ou "à ouvrir uniquement par le destinataire". Ces instructions devraient figurer sur le site web de l'assurance maladie,
- modifier le formulaire de déclaration confidentielle conformément à ce qui est suggéré dans le présent avis,
- s'assurer que l'accès aux rapports médicaux figurant dans ASSMAL est limité aux médecins-conseils,
- réévaluer le délai de conservation nécessaire pour les données relatives aux états pathologiques. Un délai de 30 ans devrait être le maximum absolu, temps pour les données papier que pour les données conservées au format électronique,
- s'assurer que les durées de conservation des informations stockées dans les bases de données électroniques sont les mêmes que celles des informations sur papier,
- dans le cadre des efforts actuellement mis en œuvre pour mettre au point une nouvelle version de ASSMAL, tenir compte du fait que le système devrait être élaboré de façon à permettre la suppression des informations dans les délais fixés ci-dessus,

- garantir qu'aucune donnée relative à la santé n'est transférée à PMO Rémunérations et à la DG BUDGET puisque ces informations ne sont pas nécessaires à l'exécution de leur mission,

- limiter le transfert des informations au comité de gestion dans le cadre des recours introduits en vertu de l'article 90 du statut. En particulier, le CEPD recommande de supprimer les informations d'identification étant donné qu'elles ne sont pas nécessaires pour que le comité rende ses rapports,
- faire figurer un lien vers la déclaration de confidentialité sur la page web où se trouvent les formulaires à télécharger et insérer un lien vers la déclaration dans les formulaires eux-mêmes,
- modifier la politique de confidentialité conformément aux recommandations du présent avis,
- fixer des délais raisonnables pour le traitement des demandes émanant des personnes concernées exerçant leur droit d'accès et prévoir une procédure permettant d'exercer le droit de rectification,
- veiller à ce que les rapports médicaux qui contiennent des informations confidentielles soient toujours transmis sous pli fermé portant la mention "confidentiel" ou "à ouvrir uniquement par la personne concernée",
- conserver les fichiers-journaux afin de tenir la liste des accès (et détecter les accès non motorisés) à ASSMAL.

Fait à Bruxelles, le 10 juillet 2007

Peter HUSTINX
Contrôleur européen de la protection des données