LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis sur une notification en vue d'un contrôle préalable adressée par le délégué à la protection des données de la Commission concernant l'administration de l'assurance accident et maladie professionnelle

Bruxelles, le 27 juillet 2007 (Dossier 2007-157)

1. Procédure

Le 9 mars 2007, le contrôleur européen de la protection des données (ci-après dénommé "le CEPD") a reçu du délégué à la protection des données de la Commission une notification en vue d'un contrôle préalable concernant les traitements de données effectués dans le cadre de la gestion de l'assurance accident et maladie professionnelle (ci-après dénommée "la notification"). Les traitements de données effectués dans le cadre de la gestion de l'assurance accident et maladie professionnelle (ci-après dénommée "l'assurance accident et maladie professionnelle") telle qu'elle est décrite dans la notification sont réalisés par l'Office de gestion et de liquidation des droits individuels (ci-après dénommé "le PMO").

Le 17 avril 2007, le CEPD a demandé des informations complémentaires, qui lui ont été communiquées le 25 mai 2007. Le 4 juin 2007, une réunion s'est tenue entre les services du PMO et du CEPD afin de confirmer des informations factuelles et de préciser différents aspects du fonctionnement de l'assurance maladie et accident professionnel. Le 14 juin 2007, le CEPD a transmis, pour observations, au PMO son projet d'avis sur la notification en vue d'un contrôle préalable Les services du PMO et du CEPD se sont à nouveau réunis le 10 juillet 2007. Lors de la réunion, les services du PMO ont présenté leurs observations orales au CEPD sur le projet d'avis, qui ont été prises en compte dans la version papier du projet d'avis en date du 24 juillet 2007.

2. Examen du dossier

2.1 Les faits

Le régime d'assurance accident et maladie professionnelle a été instauré en application de diverses dispositions du statut des fonctionnaires et du régime applicable aux autres agents des Communautés européennes[1]. En vertu de ces dispositions, les fonctionnaires, les agents temporaires et les agents contractuels des institutions de l'UE ("les membres du personnel de l'UE")[2] sont couverts contre les accidents et les maladies professionnelles. En particulier,

[1] Les dispositions qui établissent l'assurance accident et maladie professionnelle sont l'article 73 du statut des fonctionnaires, l'article 25 de l'annexe X du statut des fonctionnaires et l'article 28 du régime applicable aux autres agents des Communautés européennes. Ces dispositions ont été développées dans la règlementation commune relative à la couverture des risques d'accident et de maladie professionnelle des fonctionnaires des Communautés européennes, entrée en vigueur en 2006. Ce point est développé au point 2.2.2.

[2] Dans certains cas, les conjoints/partenaires, les enfants et les personnes à charge peuvent également être couverts par l'assurance (les "assurés"). Dans le présent avis, nous utiliserons l'expression "membres du personnel de l'UE" pour désigner les fonctionnaires et les agents temporaires et contractuels qui bénéficient de l'assurance accident et maladie professionnelle conformément à l'article 73 et à l'article 28, visés à la note de bas de page 1. Nous emploierons le terme "assurés" pour tenir compte également des conjoints/partenaires, enfants et personnes à charge assimilées. Il sera fait mention des membres du personnel de l'UE ou des assurés, selon le cas.

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

l'assurance couvre le paiement de prestations en cas de décès, en cas d'invalidité permanente totale et en cas d'invalidité permanente partielle. Elle prévoit également un remboursement complémentaire de tous les frais médicaux qui y sont liés. Les Communautés ont conclu un contrat de réassurance avec deux compagnies d'assurance, en vertu duquel les Communautés

sont assurées contre le risque résultant de l'application de l'article 73, qui prévoit leur obligation d'assurer les membres du personnel de l'UE contre les accidents et les maladies professionnelles.

L'Unité assurance maladie et accidents, qui est l'Unité 3 du PMO (ci-après dénommée "le PMO 3"), assume notamment la responsabilité de la gestion de l'assurance accident et maladie professionnelle, afin de garantir le paiement des prestations et des frais médicaux aux membres du personnel de l'UE.

Les assurés qui ont subi un accident ou une maladie professionnelle doivent transmettre au PMO 3 la déclaration d'accident et/ou la demande de reconnaissance de maladie professionnelle, accompagnée des rapports médicaux appropriés. Un fichier de données électronique sera créé pour chaque déclaration d'accident et chaque demande de reconnaissance de maladie professionnelle. Le fichier de données sera complété progressivement. Il contiendra notamment tous les rapports médicaux complémentaires transmis par la victime, les divers rapports établis par le médecin désigné par l'autorité investie du pouvoir de nomination, ainsi que les décisions définitives prises par cette autorité en ce qui concerne la reconnaissance de l'évènement visé par les dispositions juridiques et la reconnaissance d'un éventuel pourcentage d'invalidité. Le dossier contiendra également des copies de la correspondance échangée entre les services du PMO 3 et la compagnie d'assurance, qui doit être informée de la procédure pour exécuter les divers versements.

Tandis que le PMO 3 est compétent pour la gestion du régime d'assurance, la décision définitive sur le point de savoir si la cause d'un accident doit être imputée à l'existence d'un risque professionnel ou non professionnel, de même que les décisions concernant la nature professionnelle d'une maladie, sont prises par l'autorité investie du pouvoir de nomination, sur la base des rapports établis par les médecins externes désignés par elle.

La ***finalité d'ensemble*** du traitement est d'administrer l'assurance accident et maladie professionnelle afin d'assurer le paiement des prestations et le remboursement de l'ensemble des frais médicaux qui y sont liés, auxquels les membres du personnel de l'UE ont droit.

La ***responsabilité principale*** du traitement des données incombe à l'Unité assurance maladie et accidents (PMO 3). La plupart des traitements de données effectués dans le cadre de l'administration de l'assurance accident et maladie professionnelle sont réalisés par la section 3.001 compétente pour les accidents et les maladies professionnelles. Toutefois, une
partie du traitement, principalement manuelle, est effectuée par les médecins externes désignés par l'autorité investie du pouvoir de nomination.

Comme cela est précisé ci-après, les traitements manuels et automatisés des données qui sont effectués dans le cadre de l'administration du régime d'assurance, sont étroitement liés. Alors que certains traitements de données comme la collecte initiale d'informations sont réalisés manuellement et sur papier, ces informations sont toujours introduites dans une base de données informatique. Les traitements manuels et électroniques peuvent être résumés comme suit:

- La Section accidents et maladies professionnelles (PMO 3.001) *reçoit* deux types de documents concernant le régime d'assurance: *i)* une déclaration d'accident, qui est une déclaration normalisée devant être accompagnée de documents médicaux (tels que des rapports d'examen

aux rayons X ou des rapports d'hospitalisation) et, *ii)* une demande écrite de reconnaissance d'une maladie professionnelle devant être accompagnée d'un rapport médical.

- Dès la réception de ces informations, ces documents sont *scannés*. Les informations fournies à l'appui de chaque déclaration, y compris le rapport médical relatif à la maladie professionnelle et le certificat médical sont également scannés. Le document scanné est introduit dans une base de données informatique dénommée "ASSMAL".
- Les services de la Section accidents et maladies professionnelles (PMO 3.001) *notifient* à la compagnie d'assurance chaque déclaration d'accident et de maladie professionnelle.
- Les services de la Section accidents et maladies professionnelles (PMO 3.001) *transmettent* les exemplaires originaux sur papier de toutes les informations au médecin externe désigné par l'autorité investie du pouvoir de nomination en vue de leur examen.
- La personne concernée *reçoit une notification* et est invitée à passer un examen pratiqué par le médecin externe désigné par l'autorité investie du pouvoir de nomination.
- Le médecin externe *établit*, après consultation de la personne concernée, *un rapport* qui sera transmis au PMO 3.001 pour être joint à son dossier.
- Si le dossier concerne une maladie professionnelle, les services de la Section accidents et maladies professionnelles (PMO 3.001) effectuent une enquête administrative pour définir la nature de la maladie et pour déterminer si elle résulte de la profession de l'assuré. L'intervention de l'OIDC[3] sera sollicitée dans certains cas, en particulier pour déterminer si la maladie est liée à un harcèlement ou en résulte. À l'issue de l'enquête, les services de la Section accidents et maladies professionnelles (PMO 3.001) établiront un rapport sur l'enquête administrative qui sera introduit dans ASSMAL.
- Enfin, l'autorité investie du pouvoir de nomination prendra une décision définitive qui sera communiqué au membre de personnel[4].

Une fois que les services de la Section accidents et maladies professionnelles (PMO 3.001) ont introduit les informations dans ASSMAL, l'accès à celles-ci est accordé sur la base du principe du besoin d'en connaître.

Les ***catégories de personnes concernées*** dont les données sont collectées dans le cadre de l'assurance accident et maladie professionnelle sont: *i)* les membres et fonctionnaires des institutions et agences de l'UE; *ii)* le personnel temporaire et contractuel des institutions et agences de l'UE[5].

En outre, parmi les autres personnes concernées dont les informations sont aussi traitées figurent les médecins externes, par exemple ceux qui signent les déclarations d'accident, ainsi que ceux désignés par l'autorité investie du pouvoir de nomination dans le cadre de leurs fonctions.

Parmi les ***catégories de données à caractère personnel*** collectées figurent **:** *(i)* les données destinées à identifier les membres du personnel de l'UE: numéro de matricule, institution pour laquelle la personne travaille, adresse professionnelle et adresse privée en cas de départ à la retraite, date de naissance, type de bénéficiaire (membre du personnel, enfant à charge et équivalent ou conjoint); *(ii)* les informations relatives au compte bancaire sur lequel les paiements doivent être effectués, *(iii)* les informations relatives au salaire; et *(iv)* les informations relatives à la santé des assurés (type d'accident, type de maladie professionnelle, rapports médicaux, traitements proposés, etc.).

---

[3] L'OIDC est l'Office d'investigation et de discipline créé par la décision C(2004) 1588 de la Commission du 28 avril 2004. Il a notamment pour fonction d'effectuer des enquêtes administratives au titre des articles 24, 73 et 90 du statut des fonctionnaires.

[4] Les traitements de données peuvent varier en fonction des circonstances. Par exemple, comme le prévoit la règlementation commune relative à la couverture des risques d'accident et de maladie professionnelle des fonctionnaires des Communautés européennes, entrée en vigueur en 2006, les assurés peuvent demander que la commission médicale soit consultée. À l'évidence, cette consultation implique la transmission des informations à cette commission en vue de l'examen de la question.

[5] En outre, dans certains cas, les données des conjoints ou partenaires non matrimoniaux, des enfants et des personnes à charge des fonctionnaires et des agents temporaires ou contractuels des institutions de l'UE affectés dans les pays tiers sont également susceptibles d'être traitées.

En ce qui concerne ***la conservation des données***, les dossiers sur support papier sont conservés dans les archives de la Section accidents et maladies professionnelles et dans les archives de la Commission pendant une durée de cinq ans après le décès de l'assuré. Les fichiers électroniques sont conservés dans la base de données informatique ASSMAL qui est hébergée à Luxembourg pendant la même durée.

Le responsable du traitement (PMO 3) peut ***transférer des données à caractère personnel*** recueillies dans le cadre de l'administration de l'assurance accident et maladie professionnelle aux types suivants de destinataires:

- à des ***institutions communautaires***, à savoir: *i)* à la DG BUDGET qui versera les montants liés aux frais médicaux par l'intermédiaire du compte bancaire des membres du personnel[6]. *ii)* à l'OIDC dans le cadre d'affaires de harcèlement; en outre, *iii)* des données peuvent être transférées à la DG ADM B2 (l'Unité Recours), dans le cadre de recours engagés au titre de l'article 90, paragraphes 1 et 2, du statut des fonctionnaires. La réponse à la question de savoir si une catégorie particulière de données sera transférée dépend du destinataire. Par exemple, les seules informations qui sont transférées à l'OIDC sont le nom de la personne concernée et la demande d'ouverture d'un dossier. Aucune information relative à la santé n'est transférée à l'OIDC;

- à d'***autres destinataires que les institutions et organes communautaires,*** à savoir: *i)* à deux compagnies d'assurance établies en Belgique et régies par le droit belge. Les données transférées comprennent les données d'identification, la date de naissance, l'adresse privée et l'adresse professionnelle, les données relatives aux accidents ou aux maladies professionnelles, le type de lésion et les informations bancaires. Les paiements aux membres du personnel de l'UE ayant subi un accident ou une maladie professionnelle seront directement effectués par la compagnie d'assurance, à l'exception des remboursements de frais médicaux[7]; *(ii)* à des médecins externes désignés par l'autorité investie de pouvoir de nomination.

En ce qui concerne le ***droit d'information,*** la notification en vue d'un contrôle préalable a été accompagnée d'une déclaration de confidentialité qui devrait être disponible sur le site intranet de la Commission. Toutefois, les services du CEPD ont eu des difficultés à trouver cette déclaration sur le site intranet et n'y sont parvenus qu'après avoir obtenu des explications complémentaires du PMO concernant son emplacement. La déclaration de confidentialité contient des informations sur les points suivants : l'identité du responsable du traitement, les types de données et les finalités du traitement, les destinataires des données, l'existence d'un droit d'accès et de rectification et les conditions d'exercice du droit d'accès. La déclaration de confidentialité mentionne également la base juridique, les délais de conservation des données et le droit d'avoir recours au contrôleur européen de la protection des données.

Le ***droit d'accès*** et les procédures permettant de l'exercer sont reconnus dans la déclaration de confidentialité. Le ***droit de rectification*** est reconnu.

Des ***mesures de sécurité*** ont été mises en oeuvre.

2.2. Aspects juridiques

2.2.1. Contrôle préalable

Motifs du contrôle préalable: Le 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 "le règlement (CE) n° 45/2001" ou simplement "le règlement") 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 […] dans un fichier*", ainsi qu'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*"[8].

[6] La DG BUDGET obtiendra ultérieurement le remboursement de ces montants des compagnies d'assurance.
[7] Voir note de bas de page 6.
[8] Aux termes de l'article 3, paragraphe 2, du règlement (CE) n° 45/2001.

Pour les raisons exposées ci-après, le traitement de données réalisé dans le cadre de la gestion de l'assurance accident et maladie professionnel réunit tous les éléments qui déclenchent l'applicabilité du règlement.

Premièrement, le CEPD note que la gestion de l'assurance nécessite la collecte et le traitement ultérieur de *données à caractère personnel*, telles qu'elles sont définies à l'article 2, point a), du règlement (CE) n° 45/2001. En effet, comme le précise la notification, les données à caractère personnel des assurés seront recueillies et traitées ultérieurement. Elles comprennent des informations relatives à la santé des assurés, telles que des rapports de médecins précisant la nature de lésions, les conséquences d'un accident, des informations relatives à des traitements médicaux, le nom d'une maladie professionnelle, etc.

Deuxièmement, comme le précise la notification, les données à caractère personnel qui sont recueillies sont soumises à des opérations de "*traitement automatisé*", telles que définies à l'article 2, point b), du règlement (CE) n° 45/2001, ainsi qu'à des opérations de traitement manuel. En effet, les informations à caractère personnel sont d'abord recueillies sur support 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 informatique, qui est utilisée par le PMO 3.001 pour assurer la gestion du régime d'assurance. D'autres traitements de données de suivi seront effectués en fonction des types de demande des membres du personnel de l'UE (à savoir, déclarations de maladies professionnelles ou d'accidents et demandes ultérieures de remboursement).

Enfin, le CEPD confirme que le traitement est réalisé par une institution communautaire, en l'occurrence l'Unité assurance maladie et accidents de l'Office de gestion et de liquidation des droits individuels, qui fait partie de la Commission européenne, dans le cadre du droit communautaire (article 3, paragraphe 1, du règlement (CE) n° 45/2001). Il ne fait donc aucun doute que la gestion de l'assurance accident et maladie professionnelle réunit tous les éléments qui déclenchent l'applicabilité du règlement.

Les opérations de traitement de données relèvent-elles de l'article 27 du règlement ?
L'article 27, paragraphe 1, du règlement (CE) n° 45/2001 soumet au contrôle préalable du CEPD "*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 contient une liste des traitements susceptibles de présenter de tels risques. Dans cette liste figurent, au point a), les traitements de données relatives à la santé. Les données recueillies dans le cadre de la gestion du régime d'assurance portent à l'évidence sur la santé des personnes et constituent donc des données relatives à la santé. Par conséquent, les traitements doivent faire l'objet d'un contrôle préalable du CEPD.

Contrôle préalable effectué a posteriori: Étant donné que le contrôle préalable vise à faire face à des situations susceptibles de présenter certains risques, l'avis du CEPD devrait être rendu avant le début du traitement concerné. Or en l'espèce, les traitements ont déjà été effectués. Cela ne devrait cependant pas poser de problème sérieux dans la mesures où d'éventuelles recommandations du CEPD peuvent encore être adoptées si nécessaires.

Notification et date prévue pour l'avis du CEPD: La notification a été reçue le 9 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 78 jours. Par conséquent, le CEPD doit rendre son avis au plus tard le 27 juillet 2007.

2.2.2 Licéité du traitement

Le traitement de données à caractère personnel ne peut être effectué que sur la base des fondements juridiques visés à l'article 5 du règlement (CE) n° 45/2001. Comme cela est souligné dans la notification, le traitement est justifié sur le fondement de l'article 5, point a), selon lequel le traitement des 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 traitements sont conformes à l'article 5, point a) du règlement (CE) n° 45/2001, il convient de répondre aux deux questions suivantes. Premièrement, le traité ou d'autres

actes législatifs prévoient-ils les traitements effectués par le PMO 3? Deuxièmement, les traitements sont-ils nécessaires à l'exécution d'une mission?

Existence de fondements pertinents dans le traité ou d'autres actes législatifs. Pour établir l'existence, dans le traité ou d'autres actes législatifs, de fondements juridiques qui légitiment les traitements réalisés dans le cadre de la gestion de l'assurance accident et maladie professionnelle, le CEPD prend note de l'article 73 du statut des fonctionnaires. Comme il est précisé ci-après, cet article énonce le droit des fonctionnaires de l'UE à l'assurance accident et maladie professionnelle, dans les conditions fixées par une réglementation établie d'un commun accord.

En particulier, l'article 73, paragraphe 1, du statut des fonctionnaires prévoit que "*Dans les conditions fixées par une réglementation établie d'un commun accord des institutions des Communautés, après avis du comité du statut, le fonctionnaire est couvert, dès le jour de son entrée en service, contre les risques de maladie professionnelle et les risques d'accident.[…]*
Les risques non couverts sont précisés dans cette réglementation." L'article 25 de l'annexe X du statut des fonctionnaires prévoit que "*Le conjoint, les enfants et les autres personnes à charge du fonctionnaire sont couverts par une assurance couvrant les accidents pouvant survenir hors de la Communauté dans les pays figurant sur une liste arrêtée à cet effet par l'autorité investie du pouvoir de nomination*".

L'article 73, paragraphe 2, prévoit les prestations garanties aux membres du personnel de l'UE en cas de décès, d'invalidité permanente totale ou d'invalidité permanente partielle. L'article 73 prévoit également que certaines prestations et certains produits[9] seront néanmoins couverts au titre du même régime, lorsque le montant versé en application de l'article 72 ne couvre pas entièrement les frais exposés. L'article 72 concerne le régime d'assurance maladie qui a fait l'objet d'un contrôle préalable du CEPD[10]. En outre, le CEPD fait observer que conformément à l'article 73 susmentionné, les institutions ont arrêté, le 13 décembre 2005, la réglementation commune relative à la couverture des risques d'accident et de maladie professionnelle des fonctionnaires des Communautés européennes. Cette réglementation est entrée en vigueur en janvier 2006. Elle définit notamment les accidents, les maladies professionnelles, les cas d'exclusion de la couverture, les prestations et les procédures de remboursement des fais.

La législation mentionnée ci-dessus, qui concerne les fonctionnaires en activité des institutions de l'UE, est complétée par l'article 28 du régime applicable *aux autres agents* des Communautés européennes, qui s'applique aux agents temporaires. Cet article 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…*".

En outre, l'article 85 bis du statut des fonctionnaires prévoit que "*lorsque la cause du décès, d'un accident ou d'une maladie dont est victime une personne visée au présent statut est imputable à un tiers, les Communautés sont, dans la limite des obligations statutaires leur incombant consécutivement à l'événement dommageable, subrogées de plein droit à la victime ou à ses ayants droit dans leurs droits et actions contre le tiers responsable.*"

---

[9] Les frais médicaux, pharmaceutiques, d'hospitalisation, chirurgicaux, de prothèse, de radiographie, de massage, d'orthopédie, de clinique et de transport, ainsi que tous les frais similaires nécessités par l'accident ou la maladie professionnelle.

[10] Avis du CEPD du 10 juillet 2007 sur une notification en vue d'un contrôle préalable concernant la gestion le régime d'assurance maladie (Dossier 2004-238).

Après analyse du cadre juridique susmentionné, le CEDP estime que le traitement de données réalisé dans le cadre de la gestion du régime d'assurance est manifestement effectué sur la base du statut des fonctionnaires (article 73), du régime applicable aux autres agents des Communautés européennes (article 28) et de la règlementation commune relative à la couverture des risques d'accident et de maladie professionnelle des fonctionnaires des communautés européennes, entrée en vigueur en 2006.
Ces actes législatifs prévoient que les fonctionnaires de l'UE en activité et les autres agents bénéficient de la couverture des risques d'accident et de maladie professionnelle dans certaines conditions. Afin de mettre en œuvre cette obligation, les institutions ont instauré un régime d'assurance dont la gestion implique le traitement de données à caractère personnel. L'assurance accident et maladie professionnelle a manifestement pour base juridique les actes législatifs mentionnés ci-dessus.

Critère 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 de données qui est effectué dans le cadre de l'assurance est "*nécessaire"* à l'exécution d'une mission, en l'occurrence, à la gestion du régime d'assurance.

Comme indiqué ci-dessus, dans le cadre du statut des fonctionnaires, les membres du personnel de l'UE en activité bénéficient d'une assurance contre les risques d'accident et de maladie professionnelle, dans les conditions fixées par cette règlementation. Les institutions ont l'obligation de fournir cette couverture aux membres du personnel de l'UE en activité. Afin d'exécuter cette obligation, qui lie les institutions, il est logique que ces dernières instaurent un régime d'assurance accident et maladie professionnelle. Pour qu'un régime d'assurance fonctionne correctement et soit bien administré, il est nécessaire que les gestionnaires du régime procèdent à des traitements de données à caractère personnel, car la bonne gestion du régime nécessite notamment de veiller à ce que les personnes couvertes par le régime (et non d'autres) soient dûment remboursées. À cet effet, il est nécessaire d'identifier les assurés. En outre, pour veiller à ce que les membres du personnel soient remboursés conformément aux règles, les gestionnaires du régime doivent recueillir des informations sur les maladies professionnelles ou les accidents concernés. Seule la collecte de ces informations permettra de gérer le régime, notamment de déterminer si des personnes bénéficient d'une couverture et dans l'affirmative, les pourcentages de cette couverture. En conclusion, le CEPD estime que le traitement de données effectué dans le cadre du régime d'assurance accident et maladie professionnelle est indispensable à la bonne gestion de ce régime.

2.2.3. Traitement portant sur des catégories particulières de données

Le traitement de données à caractère personnel relatives à la santé est interdit, à moins qu'il ne puisse être justifié par des motifs visés à l'article 10, paragraphes 2 et 3, du règlement. L'article 10, paragraphe 2, point b), du règlement prévoit 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, le traitement des données à caractère personnel dans le cadre du régime d'assurance, y compris des données relatives à la santé, trouve sa justification dans le statut des fonctionnaires et dans le régime applicable aux autres agents des Communautés européennes. Dès lors, ce traitement est réalisé en raison de l'obligation incombant à l'employeur de fournir une assurance accident et maladie professionnelle. Par conséquent, le traitement relève manifestement de l'article 10, paragraphe 2, point b), et n'est donc pas interdit.

Comme il s'agit d'une exception à une interdiction générale, l'article 10, paragraphe 2, point b), doit faire l'objet d'une interprétation restrictive. En particulier, dans la mesure où l'article 10, paragraphe 2, point b), prévoit que, pour que l'exception s'applique, le traitement doit être

"*nécessaire*" afin de respecter les obligations et les droits spécifiques en matière de droit du travail. Ainsi, le traitement de données sensibles ne peut être autorisé que dans la mesure où il est pertinent et nécessaire afin de fournir l'assurance accident et maladie professionnelle. La question de la nécessité est abordée ci-dessous plus en détail lors de l'examen de l'application de l'article 4, paragraphe 1, point d), du règlement, qui porte sur la qualité de données.

Outre l'application de l'article 10, paragraphe 2, point b), le traitement des données relatives à la santé effectué par les médecins serait également exempté de l'interdiction en application de l'article 10, paragraphe 3, qui dispose: "*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 peut s'appliquer au personnel travaillant pour le PMO 3.001, en application de l'article 24 de la règlementation commune relative à la couverture des risques d'accident et de maladie professionnelle des fonctionnaires des Communautés européennes, entrée en vigueur en 2006, lequel énonce: "*Les agents affectés à la gestion de la présente règlementation sont astreints au secret médical quant aux pièces et/ou frais dont ils ont connaissance à l'occasion de l'exercice de leurs fonctions. Ils restent soumis à cette obligation après avoir cessé leurs fonctions au titre de la présente règlementation.*" À cet égard, le CEPD recommande que le PMO 3.001 sensibilise son personnel non médical à l'application du secret médical. Cela est essentiel pour les membres du personnel non médical, étant donné que, contrairement aux médecins diplômés, ils ne sont tenus au respect des règles du secret médical qu'en vertu de l'article 24 de la règlementation commune relative à la couverture des risques d'accident et de maladie professionnelle des fonctionnaires des Communautés européennes, entrée en vigueur en 2006, et non en vertu de leurs titres professionnels. Cela signifie qu'ils ne sont pas soumis à une autorité externe d'autorégulation en matière de déontologie professionnelle, telle qu'un conseil national de l'ordre des médecins. La règlementation commune relative à la couverture des risques d'accident et de maladie professionnelle des fonctionnaires des Communautés européennes, entrée en vigueur en 2006, ne prévoit pas non plus un corps élaboré de règles relatives au secret médical semblable à celui existant au niveau national. Et, point peut-être même plus important, les médecins ont reçu une formation complète sur les questions ayant trait à la déontologie médicale, y compris le secret médical. Il y a un monde de différence entre la connaissance du secret médical et l'engagement de le respecter, entre, d'une part, un médecin qui a prononcé le serment d'Hippocrate, et d'autre part, un membre du personnel comptable et administratif, qui n'a jamais reçu, à proprement parler, de formation sur les questions ayant trait au secret médical et qui n'est soumis à des prescriptions relatives au secret médical qu'en vertu d'un article de la règlementation commune relative à la couverture des risques d'accident et demaladie professionnelle des fonctionnaires, entrée en vigueur en 2006, qu'il n'a peut-être que lue en diagonale.

Pour ces motifs, le CEPD recommande que l'ensemble du personnel du PMO 3.001 et les autres membres du personnel non médical ayant accès aux données médicales reçoivent une formation appropriée et complète sur les questions ayant trait au secret médical. Ils devraient également être tenus de certifier par écrit qu'ils ont reçu une telle formation et qu'ils s'engagent à respecter leurs obligations 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 assurées doivent être fournies par le biais de formulaires normalisés à remplir et à accompagner de prescriptions et/ou de rapports médicaux. C'est, par exemple, le cas des déclarations d'accident. Le CEPD n'a relevé dans ce formulaire aucune demande d'information qui serait, en principe, non pertinente ou excessive.

Toutefois, les rapports médicaux contiendront un grand nombre de données. Dans ce cas, le caractère excessif des informations fournies dépendra de chaque cas particulier. Afin de veiller à ce que ces rapports ne contiennent pas d'informations non pertinentes, non adéquates et excessives, il peut être judicieux de prévoir des lignes directrices relatives au contenu de ces rapports et de ce qui

doit être précisément transmis au PMO 3.001 par les membres du personnel de l'UE et les assurés. Par exemple, la liste des éléments ou informations à communiquer au PMO 3 pourrait être décrite dans les formulaires concernés. Les lignes directrices permettraient d'orienter les médecins au sujet des informations pertinentes pour le régime, et contribueraient ainsi à la communication d'informations adéquates et pertinentes. Par ailleurs, les lignes directrices s'appliqueraient également aux assurés, auxquels elles permettraient de connaître les informations qui sont nécessaires et celles qui ne le sont pas. Par exemple, on pourrait établir un formulaire de déclaration de maladie professionnelle énumérant notamment les informations devant nécessairement figurer dans le rapport à joindre, décrivant la nature de la maladie. En outre, si des informations non pertinentes sont cependant communiquées à l'appui d'une demande particulière, le PMO 3 devrait donner à son personnel l'instruction de ne pas les introduire dans ASSMAL. Le CEPD estime par ailleurs que le caractère proportionné du traitement des données serait renforcé si les membres du régime devaient transmettre les informations sous pli fermé portant la mention "confidentiel" ou "à n'ouvrir que par le destinataire" ou une mention similaire. Ce point est particulièrement important en ce qui concerne les rapports médicaux qui sont joints à l'appui des demandes de reconnaissance de maladies professionnelles et des déclarations d'accident. Les personnes devraient être informées de l'importance que revêt le respect de cette pratique. Le CEPD estime que le site internet et la déclaration de confidentialité devraient être modifiés pour demander aux membres du personnel de l'UE de suivre ces lignes directrices lorsqu'ils transmettent des informations médicales. En outre, la transmission de ces informations du PMO 3 aux médecins désignés par l'autorité investie du pouvoir de nomination devrait également être effectuée sous pli fermé.
Par ailleurs, afin de garantir que l'accès aux rapports médicaux justificatifs est strictement limité, le PMO 3 devrait s'assurer que les droits d'accès à ASSMAL sont créés sur la base du principe du besoin d'en connaître et définir des procédures strictes permettant d'éviter les accès non autorisés.

Enfin, l'adéquation, la pertinence et la proportionnalité devraient également être évaluées en ce qui concerne les informations qui sont transférées aux compagnies d'assurance. Selon la notification, les données transférées comprennent les données d'identification, la date de naissance, l'adresse privée et l'adresse professionnelle, les données relatives aux accidents et aux maladies professionnelles,ainsi que le type de lésion ou de maladie professionnelle, et les informations bancaires. Le transfert de ces informations semble nécessaire pour permettre aux compagnies d'assurance d'exécuter leurs obligations au titre du contrat de réassurance. La compagnie aura notamment besoin des données d'identification pour établir l'identité de la personne concernée et déterminer si elle est couverte par la police d'assurance. Elle aura besoin d'informations relatives à l'accident ou à la maladie professionnelle pour vérifier les évènements en cause et évaluer les barèmes correspondants. Le CEPD estime que les informations fournies aux compagnies d'assurance sont adéquates et proportionnées aux fins du traitement effectué par ces compagnies.

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

Exactitude.- Conformément à l'article 4, paragraphe 1, point c), du règlement, les données à caractère personnel doivent être "*exactes et, si nécessaire, mises à jour*" et "*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 justificatifs de frais médicaux, etc. Compte tenu de 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 veiller à ce qu'elles soient à jour et pertinentes.

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 conserves 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.

En ce qui concerne la question de la conservation des informations sur support papier, le CEPD déduit de la déclaration de confidentialité et de la notification que le PMO 3 conserve ces informations sur support papier du vivant du membre du personnel de l'UE et pendant une durée de 5 ans après son décès. Le CEPD est informé que la raison justifiant une si longue durée de conservation des informations est qu'elle permet aux membres du personnel de l'UE ou à leurs ayants droit de rouvrir le dossier à la suite de l'aggravation d'une maladie professionnelle ou de lésions provoquées par un accident. Par exemple, elle permettrait à un membre du personnel de l'UE de demander des prestations supplémentaires. En règle générale, en ce qui concerne la conservation des données médicales, le CEPD estime que la durée de 30 ans constitue la durée maximale absolue pendant laquelle les données devraient être conservées, sous réserve de certaines exceptions particulières. Toutefois, dans les recommandations qu'il a publiées le 26 février 2007 dans le dossier 2006-532 en réponse à la consultation du Collège des chefs d'administration concernant l'application de l'article 73 du statut des fonctionnaires, le CEPD a reconnu la nécessité de conserver les données relatives à la santé pendant des périodes plus longues. En l'espèce, le CEPD estime que les avantages résultant de la conservation des donnés du vivant du membre du personnel et pendant 5 ans après son décès peuvent l'emporter sur la menace pesant sur la confidentialité et la protection des données. En effet, il apparaît que la nécessité de s'assurer que les membres du personnel peuvent rouvrir un dossier et réajuster leurs droits en fonction de leur dernier état de santé justifie la conservation des informations aussi longtemps que les membres du personnel ou leurs descendants peuvent exercer ce droit. La possibilité de rouvrir un dossier est expressément prévue à l'article 21 de la règlementation commune relative à la couverture des risques d'accident et de maladie professionnelle des fonctionnaires des Communautés européennes, entrée en vigueur en 2006. Toutefois, le CEPD souligne la nécessité de veiller pendant toute la durée de conservation à ce que des mesures techniques et organisationnelles appropriées soient mises en œuvre afin de d'éviter la divulgation illicite ou non désirée des informations.

Enfin, le CEPD constate que la déclaration de confidentialité ne mentionne que la durée de conservation des informations sur support papier, mais n'aborde pas la question de la conservation électronique des données. Le CEPD estime que la déclaration de confidentialité devrait être complétée pour décrire le stockage et la durée de conservation des données dans ASSMAL. Cela permettrait non seulement de fournir des renseignements sur la conservation, mais, conformément à ce qui est décrit ci-après, cela préciserait également que les informations ne sont pas seulement conservées sur support papier, ce qui constitue une information importante.

2.2.6 Transferts de données

Les articles 7, 8 et 9 du règlement (CE) n° 45/2001 énoncent 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 à des institutions ou organes communautaires

(conformément à l'article 7), à des destinataires relevant de la directive 95/46/CE[11] (conformément à l'article 8), ou à d'autres destinataires (conformément à l'article 9). Les faits exposés dans la notification indiquent que les informations recueillies sont transférés à deux catégories de destinataires:

i) Institutions et organes communautaires: Les informations sont en particulier transférées *i*) au PMO Rémunérations et à la DG BUDGET afin de calculer les rémunérations et de verser les montants dus par l'intermédiaire du compte bancaire du membre du personnel de l'UE concerné, *ii)* à l'OIDC dans le cadre d'affaires de harcèlement. En outre, *iii)* des données peuvent être transférées à la DG ADM B2 dans le cadre de recours au titre de l'article 90 du statut des fonctionnaires. Tous ces destinataires étant des institutions ou des organes communautaires, l'article 7 du règlement s'applique.

ii) Destinataires autres que les institutions et organes communautaires: Ces destinatires sont:
i) les deux compagnies d'assurance établies en Belgique et régies par le droit belge. Les données transférées aux compagnies d'assurance comprennent les données d'identification, la date de naissance, l'adresse privée et l'adresse professionnelle, les données relatives aux accidents ou aux maladies professionnelles, le type de lésion et les informations bancaires;
ii) les médecins externes désignés par l'autorité investie du pouvoir de nomination. Ces destinataires étant soumis à la directive 95/46/CE, l'article 8 du règlement s'applique.

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

Le CEPD estime que les transferts d'informations à la DG BUDGET et au PMO Rémunérations aux fins susmentionnées sont conformes à ces exigences. Dans les deux cas, les destinataires sont compétents pour exécuter la mission pour laquelle les données sont transférées, c'est à dire pour déterminer les rémunérations et effectuer le paiement des montants dus par l'intermédiaire du compte bancaire du membre du personnel de l'UE. De même, dans les deux cas, les transferts de données seront nécessaires pour que les destinataires exécutent leurs missions. Cela se vérifie tant que les données transmises à la DG BUDGET et au PMO Rémunérations sont limitées aux données nécessaires à l'exécution de leurs missions. Dans les deux cas, les informations à transférer seront limitées aux données d'identification du membre du personnel, aux informations bancaires, et aux informations relatives aux rémunérations. Aucune donnée relative à la santé ne devrait être transférée au PMO et à la DG BUDGET dans la mesure où ces informations ne sont pas nécessaires à l'exécution de leurs missions.

Le CEPD a également analysé les transferts de données effectués à l'OIDC et reconnaît qu'il possède les compétences pour exécuter les missions pour lesquelles les données lui sont transférées. Le CEPD fait observer qu'il a rendu un avis sur le traitement de données effectué par l'OIDC en 2005[i].

Application de l'article 8 du règlement (CE) n° 45/2001. L'article 8 prévoit que les données à caractère personnel ne sont transférées à des destinataires relevant de la législation nationale adoptée en application de la directive 95/46/CE que si *a)* le destinataire démontre que les données

[11] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

sont nécessaires à l'exécution d'une mission effectuée dans l'intérêt public ou relevant de l'exercice de l'autorité publique, ou *b)* le destinataire démontre la nécessité de leur transfert et s'il n'existe aucune raison de penser que ce transfert pourrait porter atteinte aux intérêts légitimes de la personne concernée.

Comme indiqué ci-dessus, les données sont transférées aux compagnies d'assurance, qui peuvent être considérées comme agissant à la fois en qualité de sous-traitants et en qualité de responsables du traitement. Lorsqu'elles agissent en qualité de sous-traitants, les compagnies d'assurance traitent les informations reçues conformément à la demande du responsable du traitement, le PMO 3, en vue des finalités précisées par ce dernier. La formulation du contrat d'assurance conclu entre la Commission et les compagnies d'assurance reflète partiellement et indirectement leur rôle de sous-traitant, par exemple en définissant précisément les procédures des compagnies d'assurance concernant chaque demande relative à un accident ou à une maladie professionnelle. Cependant, le CEPD observe que le contrat susmentionné a été signé avant le règlement (CE) n° 45/2001 et qu'il ne mentionne pas expressément la protection des données et le rôle de sous-traitant. Le PMO a toutefois indiqué au CEPD qu'un nouveau contrat en cours d'élaboration prévoyait de nouvelles dispositions particulières relatives à la protection des données. Le CEPD estime qu'il serait approprié d'introduire de telles dispositions.

Outre son rôle de sous-traitant, la compagnie d'assurance agit également en qualité de responsable du traitement, rôle qui est également prévu dans le contrat et dans les modalités pratiques convenues entre les compagnies et la Commission[12]. Dans le cadre de ce rôle, le CEPD estime que l'article 8, point b), est respecté car il est nécessaire que la compagnie d'assurance détienne les informations et car il n'est pas porté atteinte aux intérêts légitimes de la personne concernée. En effet, le CEPD estime que le transfert des informations aux compagnies d'assurance est une mesure nécessaire pour réduire autant que possible l'incidence financière des maladies professionnelles au sein des institutions de l'UE. Il est conforme à l'intérêt public que soit conclu un accord avec une compagnie d'assurance afin de garantir, dans les cas concernés, que la charge financière de la maladie professionnelle d'un membre du personnel de l'UE sera couverte par la compagnie d'assurance. Comme il est indiqué précédemment au point 2.2.4., la compagnie aura notamment besoin des données d'identification, notamment pour établir l'identité de la personne concernée et pour déterminer si elle est couverte par la police d'assurance. Elle aura besoin d'informations relatives à l'accident ou à la maladie professionnelle pour vérifier les évènements en cause et évaluer les barèmes correspondants. Les principes généraux du droit des contrats, tels qu'ils résultent de la pratique européenne, incluent le droit de la compagnie d'assurance d'obtenir suffisamment d'informations sur la maladie professionnelle pour exercer tous les droits et toutes les actions dont elle dispose.

En ce qui concerne les médecins externes désignés par l'autorité investie du pouvoir de nomination, ils jouent le rôle de sous-traitants dans la mesure où ils traitent les informations pour le compte du responsable du traitement, le PMO, en vue des finalités indiquées par celui-ci. Les accords contractuels conclus entre les médecins externes et le PMO confirment implicitement ce rôle, à divers égards. Il serait opportun que le contrat soit plus explicite et par exemple qu'il contienne une clause similaire à celle proposée pour le nouveau contrat avec les compagnies d'assurance.

2.2.7 Droit d'accès et de rectification

Le droit d'accès est le droit de la personne concernée d'être informée de toute donnée la concernant qui est traitée par le responsable du traitement. Conformément à l'article 13 du règlement (CE) n° 45/2001, la personne concernée a 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

[12] Telles que le paiement direct de prestations aux personnes ayant subi un accident ou une maladie professionnelle.

de toute information disponible sur l'origine de ces données. Ces informations peuvent donc être obtenues directement par la personne concernée (ce qu'on appelle "l'accès direct") ou, dans certaines circonstances, par une autorité publique (ce qu'on appelle "l'accès indirect", qui est généralement exercé par une autorité chargée de la protection des données, soit le CEPD dans le cas présent).

La déclaration de confidentialité confirme que le PMO 3 reconnaît l'existence d'un droit d'accès aux informations à caractère personnel et d'un droit de rectification. Elle fixe en outre les modalités qui s'y rapportent. Le CEPD note avec satisfaction que le PMO 3 autorise l'accès aux dossiers des assurés sans aucune restriction particulière. Le CEPD rappelle que l'accès ne saurait être limité aux "cas justifiés" et doit être autorisé pour n'importe quel motif, voire sans qu'aucun motif ne soit avancé. Les assurés ne sauraient être tenus de préciser à quelle fin ils sollicitent l'accès à ces données. En outre, afin de garantir que les demandes d'accès seront traitées en temps utile et sans contrainte, il peut s'avérer utile de fixer des délais raisonnables.

Le CEPD attire l'attention du PMO 3 sur les conclusions 221/04 du Collège des Chefs d'administration en date du 19 février 2004, qui visent à harmoniser certains aspect des conditions d'accès dans l'ensemble des institutions communautaires. Ce document souligne qu'il y a lieu d'accorder un accès aussi large que possible aux données relatives à la santé. Il prévoit notamment d'autoriser l'accès aux données de nature psychologique ou psychiatrique, 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 accordé 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[13].

2.2.8 Information de la personne concernée

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

La notification a été accompagnée d'une déclaration de confidentialité, qui devrait être mise à la disposition des membres du personnel de l'UE par l'intermédiaire du site intranet de la Commission, dans la partie consacrée aux maladies professionnelles et aux accidents. Cette déclaration servirait donc à assurer le respect des articles susmentionnés. Le CEPD a accédé au site intranet pour vérifier si les personnes qui téléchargent les formulaires à compléter peuvent accéder facilement à la déclaration de confidentialité, mais il n'est pas parvenu à la trouver. Le PMO 3 a informé le CEPD que la déclaration de confidentialité relative au traitement des données concerné est fournie avec la déclaration de confidentialité concernant un autre traitement de données, à savoir celui du régime d'assurance maladie. Ce point a été confirmé.

[13] 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."

Le CEPD estime que la déclaration de confidentialité relative au régime d'assurance devrait figurer à un autre endroit que la déclaration de confidentialité concernant le régime d'assurance maladie. En particulier, le CEPD estime que la déclaration devrait figurer sur la page internet consacrée à l'assurance accident et maladie professionnelle, intitulée "*Que faire en cas d'accident ?*", qui est disponible à l'adresse: http://intracomm.cec.eu-admin.net/pers_admin/sick_insur/accident/index_fr.html.

Cela permettrait de trouver facilement la déclaration de confidentialité. Par ailleurs, cela permettrait d'éviter la confusion actuelle entre deux déclarations de confidentialité concernant deux traitements de données différents. Lors de la mise en ligne de la déclaration, le CEPD suggère de créer un lien permettant d'y accéder sur les pages à partir desquelles les formulaires peuvent être téléchargés. Ce lien permettra d'accéder directement à la déclaration de confidentialité à partir de la page internet que le membre du personnel doit consulter pour télécharger le formulaire. L'adresse URL de la page sur laquelle la déclaration de confidentialité est disponible devrait également être imprimée sur le formulaire de déclaration des accidents.

Le CEPD a vérifié le contenu des informations figurant dans la déclaration de confidentialité afin de contrôler s'il était conforme aux prescriptions des articles 11 et 12 du règlement (CE) n° 45/2001.

Le CEPD observe que la déclaration de confidentialité contient des informations relatives à l'identité du responsable du traitement, aux finalités du traitement, à la manière dont les données sont traitées, aux conditions d'exercice du droit d'accès, aux délais de conservation des données, ainsi qu'à la base juridique des opérations de traitement auxquelless sont destinées les données. 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 de ces articles, notamment:

i) le CEPD constate qu'il n'est pas mentionné que les données font l'objet d'un traitement automatisé. Il estime que pour assurer un traitement loyal des informations, la déclaration de confidentialité devrait indiquer que la plupart, voire la totalité, des informations fournies au PMO 3 sont introduites dans une base de données électronique. Cette indication est d'autant plus nécessaire que les membres du personnel sont invités à adresser les informations sur support papier et que, dés lors, rien n'indique aux assurés que les informations qu'ils transmettent sont conservées sous forme électronique;
ii) pour garantir une transparence totale et un traitement loyal, il serait judicieux d'ajouter l'adresse d'un correspondant (celle du responsable du traitement ou d'une personne de son unité) auquel les assurés pourraient adresser des questions relatives à la déclaration de confidentialité;
iii) la partie relative aux transferts de données devrait être complétée pour indiquer que les données peuvent être transférées à l'OIDC à des fins d'enquête en cas de harcèlement;
iv) comme indiqué ci-dessus, les informations relatives aux délais de conservation des données ne concernent que les informations sur support papier. La mention des délais applicables aux informations conservées dans ASSMAL devrait être ajoutée.

3. Conclusion

Rien ne permet de conclure à un manquement aux dispositions du règlement (CE) n° 45/2001, sous réserve que les observations formulées dans le présent avis soient pleinement prises en compte. Le PMO 3 doit en particulier:

- sensibiliser les membres de son personnel à l'application du secret médical par chacun d'eux et non seulement les médecins. À cet égard, il conviendrait de prévoir une formation, ainsi que la signature d'une déclaration de confidentialité spécifique;

- afin de veiller à ce que des informations non pertinentes, non adéquates et excessives ne soient pas fournies dans les rapports médicaux, il devrait exister des lignes directrices relatives au contenu de ces rapports;
- donner aux membres du personnel de l'UE l'instruction d'adresser les rapports médicaux joints à l'appui des demandes de reconnaissance de maladies professionnelles sous pli fermé portant la mention "confidentiel" et/ou "à n'ouvrir que par le destinataire". Ces instructions devraient figurer sur le site internet consacré à l'assurance accident et maladie professionnelle;
- s'assurer que l'accès aux rapports médicaux figurant dans ASSMAL est accordé à un nombre limité de personnes sur la base du principe du besoin d'en connaître;
- inclure des dispositions explicites concernant la protection des données dans les accords contractuels avec les compagnies d'assurance et les médecins externes désignés par l'autorité investie du pouvoir de nomination;
- mettre en ligne la déclaration de confidentialité sur la page internet appropriée, créer un lien permettant d'accéder à la déclaration de confidentialité sur la page internet à partir de laquelle les formulaires peuvent être téléchargés et faire figurer un lien d'accès à la déclaration sur les formulaires;
- modifier la déclaration de confidentialité conformément aux recommandations formulées dans le présent avis;
- mentionner les délais d'exercice du droit d'accès;
- conserver les fichiers-journaux afin de tenir la liste des accès (et de détecter les accès non autorisés) à ASSMAL.

Fait à Bruxelles, le 27 juillet 2007

Joaquín BAYO DELGADO
Contrôleur européen adjoint de la protection des données

[i] Avis du CEPD sur la notification d'un contrôle préalable reçu à propos du dossier "Enquêtes administratives et procédures disciplinaires internes de la Commission européenne, 20 avril 2007 (Dossier 2004-187). Cet avis à disponible à l'adresse suivante:
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2005/05-04-20_Commission_IDOC_FR.pdf