Avis sur les notifications d'un contrôle préalable reçues des délégués à la protection des données de certaines agences européennes concernant «*Le traitement des données relatives à la santé sur le lieu de travail*»

Bruxelles, le 11 février 2011 (Dossier 2010-0071)

1. Procédure

En date du 4 septembre 2008, le Contrôleur européen de la protection des données (CEPD) a envoyé une lettre à toutes les agences de l'UE (agences) annonçant la nouvelle procédure d'analyse de contrôle préalable ex-post concernant les procédures communes au sein des agences.

En date du 28 septembre 2009, le CEPD a envoyé ses *«Guidelines concerning the processing of health data in the workplace by Community institutions and bodies»* (Lignes directrices concernant le traitement des données relatives à la santé sur le lieu de travail par les institutions et organes communautaires) à toutes les agences de l'UE. Il a été demandé à ces agences de soumettre leurs notifications sur les données relatives à la santé, ainsi qu'une lettre d'accompagnement du Délégué à la protection des données (DPD) soulignant les aspects spécifiques en regard des lignes directrices du CEPD dans ce domaine. La date limite de soumission des notifications était le 16 novembre 2009, mais peu d'agences l'ont respectée. Le CEPD a continué à recevoir des notifications après cette date, la dernière étant datée du 20 septembre 2010.

Le CEPD a reçu des notifications d'un contrôle préalable (au sens de l'article 27, paragraphe 3, du règlement (CE) n° 45/2001) et une lettre d'accompagnement des DPD des 18 agences suivantes:

- la Fondation européenne pour la formation (**ETF**),
- le Centre européen pour la prévention et le contrôle des maladies (**ECDC**),
- l'Agence des droits fondamentaux de l'Union européenne (**FRA**),
- l'Agence exécutive pour la recherche (**REA**),
- le Centre européen pour le développement de la formation professionnelle (**CEDEFOP**),
- l'Agence exécutive du réseau transeuropéen de transport (**TEN-T EA**),
- l'Agence ferroviaire européenne (**AFE**),
- l'Agence exécutive pour la santé et les consommateurs (**AESC**),
- l'Agence communautaire de contrôle des pêches (**ACCP**),
- l'Agence exécutive du Conseil européen de la recherche (**ERCEA**),
- l'Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures (**FRONTEX**),
- l'Agence exécutive pour la compétitivité et l'innovation (**EACI**),
- l'Agence européenne pour la sécurité et la santé au travail (**EU-OSHA**),

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

- l'Agence européenne des produits chimiques (**ECHA**),
- la Fondation européenne pour l'amélioration des conditions de vie et de travail (**EUROFOUND**),
- l'Agence européenne pour l'environnement (**AEE**),
- l'Agence européenne de la sécurité aérienne **(AESA**),
- l'Agence européenne pour la sécurité maritime (**EMSA**).

Le projet d'avis a été envoyé aux 18 DPD des agences concernées pour qu'ils formulent leurs commentaires pour le 10 janvier 2011. Certains commentaires des DPD ont été reçus le 11 février 2011, un DPD d'une agence ayant sollicité une extension du délai.

2. Aspects juridiques

2.1. Contrôle préalable

Les opérations de traitement à l'examen recouvrent différentes procédures, notamment les visites médicales d'embauche, les visites médicales annuelles et les congés de maladie, et impliquent différentes catégories de personnes concernées (fonctionnaires permanents, agents temporaires, agents contractuels, experts nationaux, stagiaires, candidats pour un quelconque de ces postes et visiteurs d'agences européennes). Ces opérations de traitement sont sujettes à un contrôle préalable conformément à l'article 27, paragraphe 2, point a), du règlement (CE) n° 45/2001 («le règlement»), puisqu'elles concernent le traitement de données relatives à la santé ainsi que les données administratives et financières liées à ou en rapport avec la santé.

Le CEPD a analysé les pratiques de chacune des agences par rapport aux principes de protection des données contenus dans le règlement et a évalué si chaque agence respectait ou non les lignes directrices du CEPD. Au vu des similarités dans les procédures, ainsi que des similarités entre certaines agences en termes de pratiques de protection des données, le CEPD a décidé d'examiner toutes les notifications dans le même contexte et d'émettre un avis conjoint. Dans cet avis conjoint, le CEPD souligne toutes les pratiques des agences qui ne semblent pas se conformer aux principes du règlement ou aux lignes directrices du CEPD et fournit aux agences concernées les recommandations appropriées. L'avis conjoint propose également des exemples de bonnes pratiques. Ainsi, le CEPD note l'analyse rigoureuse des opérations et pratiques de traitement des données, menée par le **CEDEFOP** à la lumière des lignes directrices du CEPD. En outre, l'**ETF** a compilé une brochure complète énumérant les procédures en matière de gestion des dossiers personnels et médicaux.

Un élément important dans toutes les notifications reçues est qu'à l'exception de la **FRA**, toutes les agences sous-traitent les examens médicaux et de laboratoire à un médecin-conseil ou à des prestataires externes. La plupart des agences ont recours aux services médicaux de la Commission à Bruxelles et à Luxembourg et ont conclu des ANS (accords de niveau de service) correspondants, y compris ceux qui ont recours à des prestataires médicaux externes. En outre, toutes les agences (à l'exception de la **FRA**) utilisent le questionnaire médical approuvé par le CEPD en juillet 2008 en coopération avec le collège médical interinstitutionnel dans le cadre des visites médicales d'embauche. En termes de mesures de sécurité, le CEPD note qu'aucune agence ne semble avoir adopté une politique de sécurité spécifique concernant le traitement des données relatives à la santé (voir point 2.9 sur la sécurité plus avant).

Le CEPD estime utile d'indiquer les diverses parties impliquées dans les opérations de traitement à l'examen. De cette manière, les agences pertinentes peuvent avoir une idée plus précise de la

relation entre le responsable du traitement et le sous-traitant, et de l'identité de la personne chargée de conserver les dossiers médicaux des fonctionnaires.

i) Dossiers médicaux conservés par les services médicaux de la Commission

Les agences **REA, TEN-T, AFE, ACCP, ERCEA, FRONTEX** et **EACI** ont conclu un ANS avec le service médical de la Commission à Bruxelles; l'**AESC** a conclu un ANS avec le service de la Commission à Luxembourg. Les dossiers médicaux sont conservés au sein des services médicaux de la Commission.

ii) Dossiers médicaux conservés par un centre médical externe

Les agences **ECHA, AESA, CEDEFOP, EUROFOUND, AEE**, **EU-OSHA** et **EMSA** ont également conclu un ANS avec les services médicaux de la Commission. Certaines d'entre elles, notamment **EUROFOUND, AEE, EU-OSHA** et **ECDC,** ont également conclu des contrats avec des centres médicaux externes qui conservent les dossiers médicaux des fonctionnaires des agences.

iii) Dossiers médicaux conservés par un médecin-conseil externe

Les agences **ECHA** et **AESA** ont également conclu des contrats avec des centres médicaux externes, mais les dossiers médicaux de leurs fonctionnaires sont conservés par des médecins-conseil externes qui exercent leurs activités dans les locaux des agences. Le **CEDEFOP** et l'**ETF** ont conclu des contrats avec des conseillers externes qui conservent les dossiers médicaux des fonctionnaires.

La **FRA** ne dispose d'aucun médecin-conseil ou service médical. Les fonctionnaires conservent eux-mêmes leurs dossiers médicaux.

Les agences **ECDC, AESA** et **AESC** ont indiqué dans leurs notifications que les opérations de traitement relatives aux visites médicales d'embauche et aux visites médicales annuelles impliquent non seulement des données relatives à la santé mais également des données destinées à évaluer les aspects de la personnalité des personnes concernées, notamment pour déterminer si un fonctionnaire est apte ou non à la fonction (article 27, paragraphe 2, point b)). Le CEPD précise qu'en vertu de l'article 28, alinéa e), du statut des fonctionnaires des Communautés européennes («statut»), la détermination de l'aptitude d'un individu implique une évaluation de l'aptitude physique pour l'exercice de ses fonctions, et non une évaluation de sa compétence, de son rendement ou de son comportement. Par conséquent, l'article 27, paragraphe 2, point b), ne s'applique pas dans ce contexte.

S'agissant des visites médicales d'embauche, les agences **ECDC, AESA** et **AEE** ont affirmé que le traitement relève également de l'article 27, paragraphe 2, point d), du règlement (CE) n° 45/2001, puisqu'il vise à exclure des personnes d'un contrat. Le CEPD souligne que le recrutement d'un candidat retenu est basé sur le nombre de conditions, spécifiées à l'article 28 du statut, auxquelles il satisfait. Plus particulièrement, l'article 33 du statut prévoit qu'*«avant qu'il ne soit procédé à sa nomination, le candidat retenu est soumis à l'examen médical d'un médecin-conseil de l'institution, afin de permettre à celle-ci de s'assurer qu'il remplit les conditions exigées à l'article 28, alinéa e)»*. En conséquence, une visite médicale d'embauche entend satisfaire à l'une des six conditions de nomination, précisée à l'article 28, alinéa e), du statut, à savoir que *«nul ne peut être nommé fonctionnaire…que s'il ne remplit les conditions d'aptitude physique requises pour l'exercice de ses fonctions»*, et ne vise pas à exclure une personne d'un contrat. L'opération de traitement sur les visites médicales d'embauche doit faire l'objet d'un contrôle préalable en raison des risques spécifiques présentés en vertu de l'article 27, paragraphe 2, point a), et non de l'article 27, paragraphe 2, point d), du règlement.

En vertu de l'article 27, paragraphe 4, du règlement (CE) n° 45/2001, le CEPD doit rendre son

avis dans les deux mois qui suivent la réception de la notification. La dernière notification ayant été soumise au CEPD le 20 septembre 2010, le CEPD considère cette date comme étant la date de réception de toutes les notifications. Après l'expiration du délai, il a sollicité des réponses à ses questions et des informations complémentaires auprès des DPD. Le 6 décembre 2010, le CEPD a envoyé un courrier électronique à tous les DPD concernés les informant qu'en raison de la complexité du dossier, et conformément à l'article 27, paragraphe 4, du règlement (CE) n° 45/2001, il avait décidé de prolonger le délai d'un mois supplémentaire, jusqu'au 9 janvier 2010. (Étant donné que cette date tombe un dimanche, le projet d'avis a été envoyé aux DPD le 10 janvier 2011.) La période de contrôle préalable a été suspendue pendant 18 jours (en tenant compte uniquement de la période de suspension de la dernière notification reçue), pendant un mois en raison de la complexité du dossier et pendant 15 jours pour permettre aux DPD de formuler des commentaires. Par conséquent, le présent avis doit être rendu le 11 février 2011 au plus tard. Le CEPD enverra également à chaque agence une lettre individuelle soulignant la nécessité d'informer le CEPD des mesures prises en réponse aux recommandations de cet avis dans un délai de 3 mois.

2.2. Licéité du traitement

La licéité du traitement des données personnelles doit être examinée à la lumière de l'article 5 du règlement. Les opérations de traitement à l'examen relèvent de l'article 5, point a), en vertu duquel le traitement n'est légitime que s'il *«est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités ou relevant de l'exercice légitime de l'autorité publique dont est investi l'institution ou l'organe communautaire».*

L'article 5, point a), comporte donc deux aspects, le premier étant de déterminer s'il existe une base juridique spécifique justifiant le traitement et le second étant de vérifier si le traitement en question est nécessaire à l'exécution de la mission effectuée dans l'intérêt public.

Base juridique dans le Traité ou dans d'autres instruments juridiques
La base juridique justifiant la visite médicale d'embauche se trouve aux articles 28 et 33 du statut et aux articles 12, alinéa d), 13, alinéa 2), et 83, alinéa 2), du régime applicable aux autres agents des Communautés européennes (RAA).

S'agissant des visites médicales annuelles, la base juridique est l'article 59, alinéa 6, du statut et l'article 16, alinéa 1, l'article 59 et l'article 91 du RAA.

L'article 59, alinéa 1, du statut constitue la base juridique pour le traitement des données relatives à la santé dans le cadre d'un contrôle médical durant un congé pour maladie ou accident.

Dans les notifications ou déclarations de confidentialité, les agences **TEN-T EA** et **AEE** ne semblent pas avoir indiqué la base juridique spécifique pour le traitement des données à caractère personnel en rapport avec les visites médicales d'embauche, les visites médicales annuelles ou les congés de maladie. Le CEPD recommande, comme expliqué clairement dans les lignes directrices, que les dispositions spécifiques soient clairement visibles par toutes les personnes concernées au travers des déclarations de confidentialité (voir plus avant la section «Information des personnes concernées», point 2.8).

EUROFOUND a indiqué l'article 59, alinéa 6), du statut comme étant la base juridique des visites médicales annuelles. **EUROFOUND** devrait également ajouter la base juridique des visites médicales annuelles pour les agents temporaires et contractuels, conformément aux dispositions du RAA. En outre, le CEPD recommande que la base juridique de la visite médicale d'embauche,

applicable aux candidats fonctionnaires potentiels, soit également indiquée dans la notification et la déclaration de confidentialité (voir le point 2.8 plus avant sur la déclaration de confidentialité).

Comme il a été souligné dans les lignes directrices, le traitement ultérieur des données médicales collectées conformément aux dispositions du statut ne peut être considéré comme licite qu'à condition qu'il soit basé sur le consentement éclairé et volontaire de la personne concernée, ou si le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée. La personne concernée devrait avoir la possibilité de refuser et/ou de retirer son consentement en ce qui concerne le traitement ultérieur de ses données médicales à des fins de suivi médical. Dans le cas présent, le consentement n'est valable que s'il est basé sur l'information que chaque agence se doit de fournir à ses fonctionnaires conformément aux articles 11 et 12 du règlement (CE) n°45/2001 (voir point 2.8 «Information des personnes concernées»).

Traitement nécessaire à l'exécution d'une mission effectuée dans l'intérêt public
En considérant si les opérations de traitement à l'examen satisfont à la deuxième condition de l'article 5 du règlement (CE) n° 45/2001, le CEPD note que les visites médicales d'embauche et les visites médicales annuelles spécifiques sont nécessaires à la gestion et au contrôle de l'aptitude physique et des congés de maladie des fonctionnaires des agences. De plus, les visites médicales annuelles peuvent être considérées comme nécessaires et par conséquent licites à d'autres fins, notamment dans le cadre de l'établissement d'un régime d'assurance maladie (articles 72 et 73 du statut). Ces opérations de traitement relèvent donc de l'exécution d'une mission des agences dans l'intérêt public conformément à l'article 5, point a), du règlement (CE) n° 45/2001.

Dans tous les cas, toutes les agences doivent veiller à ce que le fonctionnaire concerné soit:

- informé de l'issue de la visite médicale annuelle par le médecin examinateur,
- invité à recevoir des informations complémentaires/précisions du médecin, s'il le souhaite,
- autorisé à passer cette visite médicale annuelle auprès d'un autre praticien de son choix et être remboursé de la même manière que si l'examen avait été pratiqué au centre médical de l'agence.

2.3. Traitement portant sur des catégories particulières de données

Dans le cadre des procédures de sélection et de recrutement, le traitement de certaines données relevant des *«catégories particulières de données»* au sens de l'article 10 du règlement (CE) n° 45/2001 est interdit, excepté pour les motifs énoncés au même article 10, paragraphes 2 à 5.

Certaines des agences prétendent qu'elles ne reçoivent pas des données médicales au sens strict du terme, et que par conséquent les opérations de traitement ne devraient pas être soumises à un contrôle préalable. Plus particulièrement, les agences **EU-OSHA, REA, TEN-T** et **AESC** affirment qu'elles ne traitent que les certificats d'aptitude, les données administratives relatives aux congés de maladie, les certificats médicaux, les visites médicales annuelles et l'acquisition de matériel médical pour les activités professionnelles quotidiennes de certains fonctionnaires.

Comme l'a expliqué le CEPD dans ses lignes directrices, la notion de données relatives à la santé fait essentiellement référence à deux formes de données, à savoir les données médicales et les documents administratifs comportant des données à caractère personnel portant sur l'état de santé d'un individu. Plusieurs agences collectent et traitent, par exemple, des notes administratives certifiant l'aptitude médicale au travail, des factures indiquant qu'un individu a subi une visite médicale annuelle ou reçu un vaccin, des requêtes pour un examen médical de suivi, ou tout simplement des informations envoyées au département RH à des fins administratives indiquant qu'un individu est en congé de maladie. Ces données ont trait à l'état de santé d'un individu et peuvent permettre l'identification d'une maladie ou d'un handicap dont souffre une personne

concernée. Bien que le type de maladie exact ne soit pas précisé sur le certificat médical, la personne concernée peut être identifiée comme ayant été absente pour une maladie de courte ou de longue durée avec traitement médical ou pour un congé de maladie spécial de nature médicale.

En conséquence, même si aucune donnée médicale stricto sensu n'est traitée, les opérations de traitement à l'examen sont liées à la santé, et relèvent donc de l'article 27, paragraphe 2, point a), du règlement, et sont de ce fait soumises à un contrôle préalable.

Le CEPD recommande par conséquent de rappeler à l'ensemble du personnel RH des agences **ETF, ECDC, FRA, REA, CEDEFOP, TEN-T, AESC, ECHA, EU-OSHA, EACI, EUROFOUND, AEE, AESA** et **EMSA,** qui sont responsables de la collecte des certificats d'aptitude et de toute autre information liée à l'état de santé de leurs fonctionnaires, de les traiter dans le respect des principes du secret médical. Le CEPD invite ces agences à préparer des déclarations de confidentialité à faire signer par les fonctionnaires compétents, précisant qu'ils sont soumis à une obligation de secret professionnel équivalente à celle des praticiens de la santé, conformément à l'article 10, paragraphe 3, du règlement (CE) n° 45/2001. (Cette question doit être reliée à l'article 7, paragraphe 3, du règlement, voir point 2.6 du présent avis pour plus de détails.)

Le CEPD prend note de la déclaration de confidentialité préparée par le **CEDEFOP** et recommande qu'une phrase soit ajoutée dans la déclaration, à savoir *«Je suis soumis à une obligation de secret professionnel équivalente à celle des praticiens de la santé conformément à l'article 10, paragraphe 3, du règlement (CE) n° 45/2001»*. Cette phrase supplémentaire se réfère spécifiquement aux données relatives à la santé traitées, et souligne leur caractère sensible.

2.4. Qualité des données

Adéquation, pertinence et proportionnalité: En vertu de 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 semble que les données relatives à la santé collectées par les agences à l'examen, et les données médicales collectées et traitées par les prestataires externes de certaines de ces mêmes agences soient en principe adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées, conformément à l'article 4, paragraphe 1, point c), du règlement.

Néanmoins, le CEPD attire l'attention sur le principe de proportionnalité, en particulier en ce qui concerne les agences **ECHA, AESA, CEDEFOP, EUROFOUND, AEE, EU-OSHA, EMSA, ECDC** et **ETF**. Ces agences ne sont pas exclusivement liées aux services médicaux de la Commission et traitent des données médicales dans le cadre des visites médicales d'embauche et des visites médicales annuelles au travers de leurs prestataires externes. Elles doivent par conséquent garantir l'interdiction de la collecte de données à d'autres fins que la détermination de l'aptitude physique à la fonction, la détermination des droits aux avantages sociaux en matière d'invalidité ou de décès ou la protection de la santé des membres du personnel. Le CEPD recommande par conséquent que les agences *«entreprennent une réévaluation précise des questions contenues dans le questionnaire pour la visite médicale d'embauche et la visite médicale annuelle à la lumière des principes d'adéquation, de pertinence et de proportionnalité, afin de juger l'aptitude à la fonction»*[1].

[1] Voir l'avis du CEPD rendu le 14 juillet 2007 sur le traitement des données médicales par les services médicaux du PE à Bruxelles et Strasbourg (Dossier 2004-205).

1) Visite médicale d'embauche

Le CEPD note que le questionnaire médical utilisé par l'agence ***ECHA*** exige la photo des personnes concernées qui sont invitées à passer des visites médicales d'embauche. Le CEPD n'estime pas ces informations pertinentes aux fins du traitement, qui consiste à déterminer si le candidat retenu est apte ou non à la fonction.

2) Visite médicale réalisée par un médecin généraliste

Lorsque les fonctionnaires veulent passer une visite médicale préventive chez un praticien de leur choix, les agences **ETF**, **FRONTEX, EACI, EU-OSHA, ECHA, EUROFOUND, AEE, AESA** et **EMSA** doivent établir une politique en vertu de laquelle le médecin privé de la personne concernée s'engage à ne pas communiquer les résultats au médecin de l'agence ou au service médical de la Commission, sans le consentement éclairé et volontaire de la personne concernée. Le praticien doit uniquement envoyer une déclaration aux agences RH confirmant que les visites ont bien eu lieu et, si nécessaire, mentionner spécifiquement le fait que la personne concernée requiert des aménagements particuliers.

L'agence **CEDEFOP** a précisé que les visites médicales annuelles ne sont pas essentiellement préventives, mais qu'elles entendent vérifier que le fonctionnaire présente l'aptitude physique nécessaire à l'exercice de la fonction ou si des aménagements sont nécessaires sur le lieu de travail. L'agence considère donc que tous les résultats médicaux doivent être communiqués au médecin-conseil externe du **CEDEFOP,** puisqu'il est le seul à pouvoir certifier l'aptitude physique à la fonction dans l'environnement de travail prévu et dans le cadre de la médecine du travail. Le CEPD souligne que du point de vue de la protection des données, les personnes concernées doivent être libres de décider si leurs résultats médicaux doivent être communiqués au médecin de l'agence par leur médecin traitant. Une déclaration confirmant que le fonctionnaire présente l'aptitude physique nécessaire devrait être suffisante pour l'agence. Néanmoins, le CEPD considère que dans certains cas problématiques, lorsque l'état de santé d'un fonctionnaire peut poser un risque pour ses collègues ou pour ses propres performances professionnelles, ces résultats spécifiques pourraient être envoyés au médecin de l'agence à condition que la personne concernée ait été informée avant le transfert de ces données médicales.

Exactitude: L'article 4, paragraphe 1, point d), du règlement dispose que les données à caractère personnel doivent être *«exactes et, si nécessaire, mises à jour»*. En outre, *«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»*.

Ce principe doit être appliqué aussi bien aux dossiers médicaux qu'aux dossiers personnels.

Les agences **ETF, ECDC, REA, CEDEFOP, AFE, AESC, ACCP, ERCEA, FRONTEX, EACI, EU-OSHA, ECHA, EUROFOUND, AEE, AESA** et **EMSA** doivent veiller à ce que les certificats d'aptitude d'embauche et les rapports des visites médicales préventives annuelles soient conservés dans les dossiers personnels. Les dossiers doivent être complétés avec des documents mis à jour attestant de l'état de santé de l'individu lorsque nécessaire, notamment dans le cas d'une visite médicale annuelle. Les notes internes doivent être adressées comme il se doit au personnel RH compétent.

Les agences **ETF, ECHA** et **AESA** doivent veiller au respect du principe de qualité en ajoutant, par exemple, une clause dans le contrat conclu avec les médecins-conseil externes et les centres

médicaux. Les agences **ECDC**[2]**, EU-OSHA, EUROFOUND, AEE** et **EMSA** sont invitées à en faire de même avec leurs services médicaux externes respectifs. Cette clause doit énumérer les méthodes spécifiques qui peuvent garantir que les données médicales des personnes concernées restent **exactes, complètes** et **mises à jour,** par exemple:

- le consentement et la signature des personnes concernées pour les informations relatives à des contacts avec leur médecin traitant ou spécialiste peuvent aider à assurer l'exhaustivité des données médicales contenues dans le rapport médical;
- les personnes concernées peuvent signer les rapports de leurs visites médicales de façon à vérifier l'exactitude de leurs données administratives;
- les personnes concernées peuvent soumettre d'autres avis médicaux aux médecins-conseil et aux services médicaux des agences susmentionnées afin de garantir l'exhaustivité de leur dossier médical;
- le médecin-conseil doit veiller à ce qu'aucun commentaire ou annotation ne soit ajouté à un quelconque formulaire médical par un tiers quelconque.

Dans les cas où les services médicaux de la Commission[3] réalisent une partie ou l'ensemble des visites médicales pour certains des fonctionnaires des agences, et que leurs dossiers médicaux sont conservés dans les services médicaux de la Commission, ces agences, plus particulièrement la **REA,** la **TEN-T,** l'**AFE,** l'**AESC,** la **ACCP,** l'**ERCEA, FRONTEX,** l'**EACI** et l'**EMSA,** doivent veiller à ce que les personnes concernées soient conscientes des pratiques susmentionnées concernant l'exactitude de leur dossier médical.

La **FRA** devrait prendre en considération les recommandations susmentionnées au cas où l'agence conclurait un contrat avec un sous-traitant pour réaliser toutes les visites médicales.

En cas de congé de maladie, lorsque des données administratives relatives à la santé sont collectées de manière électronique, l'**ETF,** l'**ECDC,** la **FRA,** la **REA,** l'**AFE,** l'**AESC,** la **ACCP, FRONTEX,** l'**EU-OSHA,** l'**EACI**, l'**AEE, EUROFOUND** et l'**EMSA** doivent veiller à ce qu'un relevé des accès soit en place pour garantir la traçabilité des actions des utilisateurs (voir la section sur la sécurité, point 2.10).

2.5. Conservation des données

L'article 4, paragraphe 1, point e), du règlement n° 45/2001 pose le principe que les données doivent être *«conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement»*.

Le CEPD souhaiterait clarifier, comme souligné dans les lignes directrices, qu'en règle générale, le délai maximum de conservation des données médicales sera de 30 ans à compter du dernier ajout d'un document médical au dossier. Le délai de conservation devra être évalué et déterminé à la lumière de l'article 4, paragraphe 1, point e), du règlement. Comme le recommande le CEPD dans sa lettre au Comité des chefs d'administration du 26 février 2007[4]**,** la nature des documents médicaux doit être examinée à la lumière des règles applicables afin de déterminer quels délais de

---

[2] Le CEPD a pris note de la lettre du DPD de l'**ECDC** du 29 janvier 2010 mentionnant que l'agence avait demandé au sous-traitant d'adopter la recommandation du CEPD concernant la signature des rapports de laboratoire par les personnes concernées.

[3] Il convient de rappeler que les activités du service médical de la Commission à Bruxelles et à Luxembourg étaient soumises à un contrôle préalable par le CEPD. L'avis a été émis le 10 septembre 2007 (Dossier 2004-232).

[4] Voir http://www.CEPD.europa.eu/CEPDWEB/CEPD/Supervision/Adminmeasures.

conservation seraient les plus adaptés à chaque type de document. Il est par conséquent nécessaire d'examiner dans quelle mesure et à quelle fin il est nécessaire de conserver plusieurs documents médicaux pendant et après la période d'emploi d'un fonctionnaire. Il est important de noter que le 11 octobre 2010, le Conseil des chefs d'administration a soumis une consultation au CEPD au titre de l'article 28, paragraphe 1, du règlement concernant les délais de conservation spécifiques pour divers documents médicaux. Après diverses réunions entre le CEPD et le CPAS, le sous-comité pertinent du Comité, le CEPD émettra sa décision sur la consultation en tenant compte de la lettre du CEPD du 26 février 2007 et de ses avis de contrôle préalable.

À cet égard, et afin d'éviter toute confusion, l'**EACI** devrait ajouter à sa déclaration de confidentialité que les données médicales sont conservées pour une durée maximale de 30 ans *«à compter du dernier ajout d'un document médical au dossier, à la lumière de l'article 4, paragraphe 1, point e), du règlement»*. L'**EACI** devrait également adopter des délais de conservation des données spécifiques pour les congés de maladie et les candidats non recrutés, conformément aux lignes directrices du CEPD.

Le CEPD note que l'**ECDC** conserve des certificats d'aptitude («certificats de santé») aussi bien des candidats recrutés que non recrutés pour une durée maximale de trente ans.
En outre, **EUROFOUND** a déclaré qu'une *«copie du certificat d'embauche est conservée dans le dossier personnel de façon permanente. L'original est conservé dans le dossier médical. Le dossier médical, en tant que partie intégrante du dossier personnel d'un fonctionnaire, est conservé de façon permanente»*.
L'**ECHA** a indiqué dans sa notification que *«les dossiers médicaux des membres du personnel sont conservés pour une durée de 10 ans à compter de la cessation de la relation de travail»*.
L'**AESA** a également affirmé dans sa notification que *«les résultats sont ajoutés au dossier médical, qui est conservé pour une durée de 10 ans à compter de la cessation de la relation de travail»*.
Le CEPD tient à souligner que les données qui doivent être conservées dans les dossiers médicaux par les sous-traitants des agences sont les résultats de laboratoire des visites médicales d'embauche et de toute autre visite médicale que la personne concernée souhaiterait subir. D'après l'évaluation susmentionnée, les dossiers médicaux doivent être conservés pour une durée maximale de 30 ans après le départ du fonctionnaire. Les certificats d'aptitude attestant de l'aptitude ou non du fonctionnaire doivent être conservés dans le dossier personnel. D'après les lignes directrices du CEPD en matière de recrutement de personnel[5], le CEPD recommande que les dossiers personnels ou individuels soient conservés pour une durée de 10 ans à compter de la fin du service ou du dernier versement d'une pension.
En conséquence, les délais de conservation de données adoptées par l'**ECDC** et **EUROFOUND** sont excessifs aux fins pour lesquelles les données sont collectées et les délais de conservation des données indiqués par l'**ECHA** et l'**AESA** ne sont pas conformes aux politiques susmentionnées. Le CEPD invite les quatre agences à réévaluer les données conservées dans les dossiers médicaux et personnels et à établir des délais de conservation des données appropriés, tel qu'expliqué ci-dessus.
En outre, à la lumière des lignes directrices du CEPD, l'**ECDC** et l'**ECHA** doivent adopter un délai de conservation des données des candidats non recrutés, tenant compte des délais prévus pour la contestation des données ou le réexamen éventuel de la décision négative. En outre, le CEPD recommande que l'**ECDC** et l'**ECHA** adoptent des délais de conservation de données spécifiques pour les données sur les congés de maladie.

D'après la notification de la **FRA**, l'agence conserve les certificats d'aptitude dans les dossiers

[5] Orientations concernant les opérations de traitement des données en matière de recrutement de personnel, 10 octobre 2008.

personnels des candidats recrutés pour une période indéterminée, aussi longtemps que le dossier personnel existe. Le CEPD estime que cette période est excessive et inutile au sens de l'article 4, paragraphe 1, point e), du règlement. Comme souligné précédemment, le CEPD recommande que la **FRA** conserve les dossiers personnels pour une durée maximale de 10 ans à compter de la fin du service ou du dernier versement d'une pension.

L'**AESC** doit suivre les mêmes recommandations pour le délai de conservation des certificats d'aptitude liés aux visites médicales d'embauche, conservés dans le dossier personnel, et définir un délai de conservation des données pour les candidats non recrutés, tel que recommandé dans les lignes directrices du CEPD.

Dans le cas de l'**ETF**, le CEPD recommande que l'agence adopte également des délais de conservation spécifiques pour les données relatives aux congés de maladie, les données relatives aux visites médicales annuelles et les données relatives aux candidats non recrutés, conformément aux lignes directrices du CEPD.

Le CEPD invite l'agence **REA**, au moment d'établir sa propre liste de conservation spécifique, à ne pas considérer uniquement la «Liste commune de conservation des dossiers au niveau de la Commission européenne», mais également les recommandations formulées par le CEPD dans ses lignes directrices; la **REA** devrait notamment adopter des délais de conservation pour les données relatives à la santé aussi bien pour les candidats recrutés que pour les candidats non recrutés (certificats d'aptitude et certificats médicaux), les congés de maladie et si nécessaire, les visites médicales spécifiques. Dès que cette liste sera adoptée, il conviendra d'en informer le CEPD.

L'agence **TEN-T EA** a communiqué au CEPD les délais de conservation pour les données relatives aux congés de maladie et aux candidats non recrutés, qui sont jugés raisonnables. Le CEPD recommande que ces délais de conservation soient indiqués aussi bien dans la notification que dans la déclaration de confidentialité.

L'agence **FRONTEX** doit établir un délai de conservation pour les données relatives à la santé des candidats non recrutés conformément aux lignes directrices du CEPD.

Les agences **AFE** et **EU-OSHA** doivent établir un délai de conservation pour les données relatives aux congés de maladie conformément à l'article 59, paragraphe 4, du statut et aux lignes directrices du CEPD.

L'**AEE** n'a pas indiqué un quelconque délai de conservation dans la notification pour:

- les certificats d'aptitude dans les dossiers personnels,
- les données relatives aux congés de maladie,
- les visites médicales spécifiques et
- les données des candidats non recrutés.

Le CEPD recommande que l'**AEE** adopte des délais de conservation spécifiques pour ces données et qu'elle veille à ce que le prestataire médical externe de l'agence conserve les données médicales de ses fonctionnaires pour un délai maximal de 30 ans à compter de l'ajout du dernier document médical au dossier du fonctionnaire, à la lumière de l'article 4, paragraphe 1, point e), du règlement.

L'agence **AFE** a indiqué dans la notification que *«les données sur les congés de maladie sont traitées à des fins statistiques de manière anonyme, par conséquent le règlement (CE) n°45/2001 n'est pas applicable»*. Afin d'éviter toute confusion, le CEPD attire l'attention sur l'article 4, paragraphe 1, point e), du règlement qui stipule explicitement que *«(…) les*

données à caractère personnel qui doivent être conservées au-delà de la période précitée à des fins historiques, statistiques ou scientifiques (…)ne seront conservées que sous une forme qui les rend anonymes (…) Les données ne doivent en tout cas pas être utilisées à des fins autres qu'historiques, statistiques ou scientifiques». En vertu de cette disposition, l'**AFE** est tenue de s'assurer que les données sont rendues anonymes si elles sont utilisées à des fins statistiques. Ce n'est qu'au travers de cette manipulation que le règlement n'est plus applicable. Le CEPD demande en conséquence à l'agence **AFE** de fournir des preuves de la méthode utilisée pour garantir l'anonymat des données utilisées à des fins statistiques.

2.6. Transfert de données

Le traitement au regard de l'article 7, paragraphe 1, concerne les transferts de données à caractère personnel entre institutions ou organes communautaires ou en leur sein *«si nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire»*.

Communication interne des données au sein de l'agence:

i) Factures médicales
Le CEPD salue les politiques spécifiques adoptées par l'**ECDC** en vertu desquelles le responsable du traitement communique au département financier/comptable de l'agence uniquement le coût total à payer au prestataire médical externe. Une déclaration de confidentialité est également signée par le responsable du département en charge de la comptabilité de l'agence.

La **FRA** doit veiller à ce que le document de remboursement (Annexe 2 de la notification) soit complété par le médecin de la personne concernée, qui communique ensuite uniquement le montant total à rembourser au bureau de la caisse d'assurance maladie de l'agence.

Les agences **ETF, FRONTEX, EU-OSHA, AEE** et **AESA** n'ont fourni aucune information concernant l'existence d'une procédure spécifique pour le transfert éventuel des données relatives à la santé au département du budget administratif de l'agence en cas de demande de remboursement. Le CEPD insiste pour que les agences précitées établissent une procédure en vertu de laquelle toutes les factures médicales sont d'abord envoyées au service médical de l'agence, qui se charge de les valider et qui ne communique ensuite que le montant total à rembourser au département du budget.

La **REA**, l'**AFE** et **FRONTEX** doivent établir une procédure en vertu de laquelle le service médical de la Commission valide toutes les factures médicales et complète ensuite un document indiquant le montant total à rembourser. Ce document doit être transféré directement au département financier compétent des agences et ce uniquement par le service médical de la Commission.

S'agissant de la position du **CEDEFOP**, le CEPD rappelle que l'objectif des lignes directrices est d'harmoniser les bonnes pratiques et d'assurer une cohérence parmi toutes les agences. Le CEPD invite donc le **CEDEFOP** à reconsidérer la politique relative aux factures médicales et à adopter les recommandations formulées dans les lignes directrices.

ii) Transferts à d'autres institutions
En outre, dans le contexte des transferts à d'autres institutions, les agences doivent veiller à ce que les destinataires des dossiers médicaux soient des personnes autorisées à accéder aux données relatives à la santé et tenues au secret professionnel.

Ceci doit être le cas pour les agences **FRA**, **REA**, **TEN-T**, **AFE, AESC**, **ACCP**, **ERCEA**, **FRONTEX**, **EACI, EU-OSHA, ECHA, AEE** et **AESA** lorsqu'elles doivent transférer des certificats d'aptitude des fonctionnaires, ou d'autres documents relatifs à leur santé, à une autre institution.

iii) Conformité avec l'article 7, paragraphe 3, du règlement (CE) n° 45/2001
L'article 7, paragraphe 3, du règlement dispose que *«le destinataire traite les données à caractère personnel uniquement aux fins qui ont motivé leur transmission»*. D'après les notifications, les agences **ETF, ECDC[6], FRA, REA, TEN-T, AFE AESC, ACCP, ERCEA, FRONTEX, ECHA, EU-OSHA, EACI, EUROFOUND, AEE**, **AESA** et **EMSA** n'ont produit aucun document ou autre référence attestant du respect du principe énoncé à l'article 7, paragraphe 3. Le CEPD recommande par exemple qu'une note interne soit préparée par chaque agence ou qu'une déclaration soit signée par les destinataires potentiels, rappelant explicitement leur obligation de ne pas utiliser les données reçues à des fins autres que celles qui ont motivé leur transmission.

Le CEPD recommande que les deux points précités ii) et iii) soient mis en œuvre conjointement avec la recommandation au point 2.3. Ceci implique que les agences concernées préparent des notes internes ou des déclarations à faire signer par les fonctionnaires concernant l'article 10, paragraphe 3, et l'article 7, paragraphe 3, du règlement (CE) n° 45/2001.

Transfert externe

i) Transfert à la lumière de l'article 8 du règlement
L'article 8 du règlement (CE) n° 45/2001 énonce les conditions en vertu desquelles les données à caractère personnel peuvent être transférées à des destinataires relevant de la législation nationale adoptée en application de la directive 95/46/CE.

Les notifications des agences **ETF, ECDC, FRA, REA, TEN-T, AFE, AESC, ACCP, ERCEA, FRONTEX, EACI, EU-OSHA, ECHA, EUROFOUND, AESA** et **EMSA** ne fournissent aucune information concernant un transfert éventuel à des destinataires relevant de la directive. Bien qu'ils soient rares, ces transferts ne peuvent être exclus. Lorsque les agences doivent transférer des données relatives à la santé, par exemple aux autorités nationales dans le cadre d'une enquête menée par une autorité nationale, la nécessité de ce transfert doit être démontrée conformément à l'article 8, point a), du règlement. En outre, le CEPD souligne que la coopération avec les autorités nationales doit également respecter les exigences et mécanismes imposés par les règlements nationaux en matière de secret médical. Dans tous les cas, il est primordial de ne transférer que des données exactes, pertinentes et non excessives.

ii) Transfert à la lumière de l'article 9 du règlement
L'article 9 du règlement (CE) n° 45/2001 dispose que les données à caractère personnel peuvent être transférées à des destinataires qui ne sont pas soumis à la législation nationale adoptée en application de la directive 95/46/CE, pour autant qu'un niveau de protection adéquat soit assuré dans le pays ou l'organisation tiers. Le caractère adéquat du niveau de protection doit être apprécié au regard des critères énoncés à l'article 9, paragraphe 2. L'article 9, paragraphe 6, présente des cas exceptionnels. Les agences devront veiller au respect de l'article 9 dans tous les transferts à des destinataires ne relevant pas de la directive.

---

6 Le CEPD note que conformément à la notification, les fonctionnaires de l'**ECDC** ont été informés de la confidentialité du traitement des données. Ils ont reçu des instructions du DPD et l'agence est sur le point d'organiser des séances de formation/information. Ces pratiques sont encouragées et devraient être adoptées par toutes les agences.

Lors de tout transfert de ce type, les agences devraient garantir le respect de l'article 9.

2.7. Droit d'accès et de rectification

L'article 13 du règlement (CE) n° 45/2001 prévoit un droit d'accès et définit ses modalités d'application à la demande de la personne concernée par le traitement. L'article 14 du règlement pose le principe que *«la personne concernée a le droit d'obtenir du responsable du traitement la rectification sans délai de données à caractère personnel inexactes ou incomplètes».*

Droit d'accès

Fonctionnaires engagés

i) Droit d'accès dans un délai raisonnable et sans contrainte
La plupart des agences sous-traitent le traitement des données médicales de leurs fonctionnaires et ne conservent donc aucun dossier médical. Il est dès lors nécessaire d'établir une nette distinction entre le droit d'accès au dossier médical et le droit d'accès au dossier personnel d'un fonctionnaire.

- **au dossier médical du fonctionnaire**

Le CEPD estime qu'il serait utile que les agences **ECHA, EU-OSHA**, **AEE, AESA** et **EMSA** garantissent par le biais du contrat conclu avec leurs prestataires médicaux/ médecins-conseil externes la détermination d'un délai raisonnable pour le traitement d'une demande d'accès, sans contrainte, conformément à la directive 95/46/CE. Ceci devra être explicitement indiqué dans les déclarations de confidentialité informant les personnes concernées de leurs droits (voir point 2.8).

- **au dossier personnel du fonctionnaire**

Les agences **ETF**, **ECDC, CEDEFOP, TEN-T, AFE, AESC, ECHA, AEE** et **EMSA** doivent expliquer dans leur déclaration de confidentialité ou toute autre note que les certificats d'aptitude des visites médicales d'embauche et des visites médicales annuelles sont accessibles via le dossier personnel (conservé par le département RH des agences) dans un délai raisonnable et sans contrainte, après l'introduction d'une demande d'accès conformément à l'article 13 du règlement (CE) n° 45/2001.

ii) Accès aux données sous une forme intelligible
Les agences ayant recours à des prestataires médicaux externes, à savoir l'**ECHA,** l'**AESA,** le **CEDEFOP, EUROFOUND,** l'**AEE,** l'**EU-OSHA,** l'**EMSA,** l'**ECDC** et l'**ETF,** doivent veiller à ce que les praticiens en charge des visites médicales communiquent les résultats médicaux aux personnes concernées sous une forme intelligible. Pour ce faire, ils doivent interpréter les données (telles que les codes médicaux ou les résultats des analyses de sang) et/ou rendre les données déchiffrables.

iii) Copies des dossiers médicaux
Lorsque les personnes concernées sollicitent des copies de leurs dossiers médicaux, les agences **ECHA, EU-OSHA**, **AESA** et **EMSA** doivent veiller à ce que les médecins en charge des dossiers médicaux accèdent à la requête de leurs fonctionnaires.

iv) Accès aux données de nature psychologique ou psychiatrique
Lorsque les données traitées sont de nature psychologique ou psychiatrique, les agences **ETF, ECDC, REA, TEN-T, AFE, AESC, ACCP, ERCEA, FRONTEX, ECHA, EU-OSHA, EACI, EUROFOUND**, **AESA** et **EMSA** doivent veiller à ce que les personnes concernées puissent y avoir indirectement accès; en cas d'évaluation au cas par cas, cet accès indirect est nécessaire pour

garantir la protection des personnes concernées en vertu de l'article 20, paragraphe 1, point c), du règlement. Les possibilités d'accès indirect doivent se conformer aux conclusions 221/04 du 19 février 2004, et les agences précitées doivent informer les personnes concernées de ces possibilités (voir point 2.8).

Candidats non recrutés, visiteurs, stagiaires

D'après les notifications, il apparaît que d'autres catégories de personnes concernées ne sont pas couvertes, à savoir les candidats non recrutés, les visiteurs, les stagiaires ou d'autres personnes qui pourraient être sujettes à un traitement médical durant leur présence au sein des agences. En conséquence, les agences **ECDC, REA, TEN-T, AFE, AESC, ACCP, FRONTEX, ECHA, EU-OSHA, EACI**, **AESA** et **EMSA** doivent accorder à ces personnes concernées un droit d'accès aux données relatives à leur santé lorsqu'elles en font la demande. Cette information doit figurer dans la déclaration de confidentialité.

Droit de rectification

Les agences **ETF, FRA, REA, CEDEFOP, TEN-T, AFE, AESC, ACCP, ERCEA, FRONTEX, ECHA, EU-OSHA, EUROFOUND**, **AEE, AESA** et **EMSA** doivent veiller à ce que ce droit soit compris par les personnes concernées (par exemple, en donnant des informations dans la déclaration de confidentialité) et à ce qu'il leur soit accordé, en particulier le droit de non seulement corriger les erreurs administratives dans leur dossier médical mais également de le compléter, en ajoutant un deuxième avis médical.

2.8. Information des personnes concernées

Les articles 11 et 12 du règlement (CE) n° 45/2001 stipulent que les personnes concernées doivent être informées du traitement des données les concernant et énumèrent une série d'informations générales et complémentaires. Cette dernière disposition s'applique dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations complémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données. Dans le cas présent, les données médicales sont fournies en partie par la personne concernée et en partie par les services médicaux de la Commission ou les médecins et les prestataires de soins médicaux externes.

Déclaration de confidentialité

Les informations fournies par l'**ETF** au point 1.7 de la lettre envoyée au CEPD sont sans rapport avec le droit d'information. En outre, bien que l'**ETF** ait énuméré dans la notification tous les éléments d'information conformément aux articles 11 et 12 du règlement (CE) n° 45/2001, elle n'a pas préparé une déclaration de confidentialité expliquant aux personnes concernées les différentes informations pertinentes énoncées dans ces dispositions. En conséquence, à la lumière des lignes directrices du CEPD, ce dernier invite l'**ETF** à fournir aux personnes concernées une déclaration de confidentialité qui doit être facilement accessible et expliquer toutes les informations énumérées aux articles 11 et 12.

L'**ECDC** doit modifier les durées de conservation des données mentionnées dans les déclarations de confidentialité des visites médicales d'embauche et des visites médicales annuelles (voir point 2.5 ci-dessus) et préciser aux personnes concernées que leurs dossiers médicaux sont conservés par un service médical externe, tandis que les dossiers personnels sont conservés par le département RH de l'agence.

Le CEPD recommande que les agences **FRA, REA, TEN-T, FRONTEX, EU-OSHA,**

EUROFOUND, AEE et **AESA** préparent, dès que possible, une déclaration de confidentialité énumérant tous les droits des personnes concernées prévus aux articles 11 et 12 du règlement (CE) n° 45/2001.

Le **CEDEFOP** a précisé que l'agence envisage d'inclure une déclaration de confidentialité, conforme aux articles 11 et 12 du règlement. Une copie de la déclaration de confidentialité exposant minutieusement toutes les informations appropriées devra être envoyée au CEPD dès qu'elle sera finalisée.

Le CEPD estime que la *«déclaration de confidentialité spécifique e-RH*» fournie par l'**AFE** est sans rapport avec le traitement des données relatives à la santé réalisé par l'agence. Il est dès lors recommandé qu'une déclaration de confidentialité appropriée soit préparée concernant les opérations de traitement spécifiques réalisées par l'agence. Celle-ci doit expliquer clairement aux personnes concernées toutes les informations pertinentes prévues aux articles 11 et 12.

L'**AESC** a indiqué dans sa notification que les informations pertinentes peuvent être consultées sur l'intranet de l'agence. L'**EMSA** a fourni au CEPD certains liens vers les documents consultables sur l'intranet, qui ne semblent pas être conformes aux articles 11 et 12 du règlement. Le CEPD invite donc l'**AESC** et l'**EMSA** à préparer une déclaration de confidentialité concernant les opérations de traitement dans le cadre de l'embauche, des visites médicales annuelles et des congés de maladie. Cette déclaration de confidentialité doit fournir des informations claires et détaillées concernant les droits d'information de la personne concernée, tels qu'énumérés aux articles 11 et 12 du règlement.

La finalité du traitement, à savoir *«gérer les droits et obligations des fonctionnaires de la ACCP et des END»*, tel que défini par la **ACCP** dans la déclaration de confidentialité, est vague et peut être trompeuse. Le CEPD recommande que l'agence ajoute une clause/phrase expliquant que la finalité du traitement concerne les droits et obligations des *fonctionnaires de l'agence dans le cadre du traitement de leurs données relatives à la santé.*

Le CEPD estime que la déclaration de confidentialité de l'**ERCEA** concerne la procédure de recrutement et la constitution de dossiers personnels. Ceci n'est pas suffisant, puisqu'elle ne concerne pas les données relatives à la santé traitées par l'agence. En conséquence, le CEPD recommande qu'une déclaration de confidentialité appropriée soit rédigée, énumérant tous les droits prévus aux articles 11 et 12 en rapport avec les opérations de traitement spécifiques à l'examen.

L'**ECHA** a inséré une déclaration de protection des données dans les invitations adressées aux personnes concernées concernant les visites médicales d'embauche au service médical de la Commission et au centre médical d'Helsinki. Les mêmes clauses de protection des données figurent sur les invitations relatives aux visites médicales annuelles, les congés spéciaux d'ordre médical et les congés de maladie.
L'**ECHA** doit également préparer une déclaration de protection des données concernant les visites médicales réalisées par un médecin-conseil externe.
L'**ECHA** doit inclure les recommandations du CEPD concernant le droit d'accès et de rectification (voir point 2.7 ci-dessus) dans toutes les déclarations de protection des données. Il convient également d'ajouter les informations suivantes à la lumière des lignes directrices du CEPD sur les données relatives à la santé:

- la base juridique de chaque opération de traitement des données relatives à la santé;
- la durée de conservation des données médicales par le médecin-conseil externe aussi bien des candidats recrutés que des candidats non recrutés;
- la durée de conservation des données relatives aux congés de maladie et

- le droit des personnes concernées de saisir à tout moment le CEPD.

Le CEPD fait remarquer à toutes les agences que la déclaration de confidentialité ne doit pas être adressée seulement aux fonctionnaires fraîchement recrutés (comme la **REA** l'a indiqué dans sa notification) mais à l'ensemble des fonctionnaires des agences. Il convient dès lors que celle-ci soit facilement accessible sur le site web d'une agence.

Informations complémentaires à fournir

Mis à part les droits énumérés aux articles 11 et 12, la déclaration de confidentialité doit fournir des informations complémentaires concernant les opérations de traitement à l'examen. Le CEPD réitère ses recommandations, telles que formulées dans ses lignes directrices sur les données relatives à la santé.

Les agences **REA**, **TEN-T**, **AFE**, **ERCEA**, **FRONTEX, AESC, EU-OSHA, EUROFOUND, AEE, CEDEFOP, AESA** et **EMSA** doivent préciser dans la déclaration de confidentialité quelle partie (service médical de la Commission, prestataire externe, médecin de l'agence) est chargée de réaliser les visites médicales d'embauche, les visites médicales annuelles et les autres visites préventives, ainsi que le lieu où sont conservés les dossiers médicaux des fonctionnaires.

Les agences **REA**, **CEDEFOP**, **TEN-T**, **AFE**, **AESC**, **ERCEA**, **FRONTEX, EU-OSHA, EUROFOUND** et **AEE** doivent en outre indiquer quelles données relatives à la santé doivent être collectées et conservées par le département RH des agences, et à quelles fins.

Questionnaires médicaux

L'agence **ETF** doit indiquer sur les deux questionnaires «sorveglianza sanitaria» et «visite periodiche» (utilisés lors de la visite médicale annuelle réalisée par le médecin-conseil de l'agence) si les réponses aux questions sont volontaires ou obligatoires et les éventuelles conséquences d'une absence de réponse.

Visites médicales préventives

i) Choix d'un médecin privé

Dans le cas des visites médicales préventives, les agences **ETF, REA, TEN-T, AFE, AESC, ERCEA, FRONTEX, ECHA, EU-OSHA, EACI, EUROFOUND, AEE**, **AESA** et **EMSA** doivent informer les personnes concernées de leur droit de choisir leur médecin traitant et des démarches pratiques qu'elles doivent entreprendre pour que la visite médicale soit réalisée par le praticien de leur choix.

ii) Transfert des résultats des visites médicales

En outre, les agences **ETF, REA, CEDEFOP, TEN-T, AFE, AESC, ERCEA, FRONTEX, ECHA, EU-OSHA, EACI, EUROFOUND, AEE**, **AESA** et **EMSA** doivent spécifier dans leur déclaration de confidentialité si le médecin traitant de la personne concernée devra transférer un quelconque résultat de la visite médicale au médecin de l'agence ou au service médical de la Commission, ou à tout autre prestataire médical externe, et si oui, à quelles fins. Comme expliqué dans les lignes directrices, le CEPD insiste pour que les résultats médicaux d'une visite médicale annuelle ne soient pas communiqués au médecin de l'agence ou au service médical de la Commission sans le consentement éclairé et volontaire de la personne concernée.

iii) Accès indirect aux données psychologiques ou psychiatriques

Enfin, le CEPD recommande que les agences **ETF, ECDC, FRA, REA, CEDEFOP, TEN-T, AFE, AESC, ACCP, ERCEA, FRONTEX, ECHA, EU-OSHA, EACI, EUROFOUND, AEE**, **AESA** et **EMSA** informent les personnes concernées par le biais d'une déclaration de

confidentialité ou d'une note interne des possibilités d'accès indirect aux données psychologiques ou psychiatriques, à la lumière des conclusions 221/04 du 19 février 2004.

2.9. Mesures de sécurité

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

Le CEPD note que la Commission a signé un «mémorandum d'entente» relatif à l'application de la politique de sécurité des systèmes d'information de la Commission européenne avec un certain nombre d'agences, dont l'**EACI,** l'**AESC,** l'**ERCEA,** la **REA** et l'**AFE**. En outre, l'**ERCEA** a fourni une «synthèse» concernant l'état d'avancement de sa politique de sécurité informatique, préparée par le Responsable local de la sécurité informatique[7]. Toutefois, ce mémorandum d'entente ne vise pas à dicter ou remplacer la politique de sécurité informatique des agences ou toute autre mesure de sécurité qu'elles se doivent d'adopter en vertu de l'article 22 du règlement.

Comme mentionné au point 2.4, les agences **ETF, ECDC, FRA, REA, AFE, AESC, ACCP, FRONTEX, EU-OSHA, EACI**, **EUROFOUND**, **AEE** et **EMSA** ne semblent pas avoir adopté un relevé des accès pour suivre les actions des utilisateurs, en particulier dans le cas des congés de maladie où les données administratives relatives à la santé sont collectées de manière électronique. Cette mesure de sécurité doit être mise en œuvre conformément aux mesures techniques et organisationnelles énoncées à l'article 22 du règlement.

En outre, le CEPD note que quelques agences ont produit des documents relatifs à leur politique d'information et de communication. Ces documents sont sans rapport avec les exigences spécifiques de l'article 22 du règlement. En conséquence, le CEPD recommande que toutes les agences adoptent leur propre politique de sécurité en tenant compte de la liste des éléments fournis à l'article 22, paragraphe 2, points a) à j), du règlement. Cette politique de sécurité spécifique doit être basée sur un exercice d'évaluation des risques mené par chaque agence, et doit être mise en œuvre dans le cadre du traitement des données médicales et/ou relatives à la santé dans leurs locaux. Toutes les agences devront envoyer une copie de leurs mesures de sécurité spécifiques au CEPD.

2.10. Sous-traitance

À la lumière de l'article 23 du règlement (CE) n° 45/2001, les agences doivent choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation dans le cadre du traitement des données médicales.

Le CEPD a identifié trois catégories de sous-traitance:
i) le service médical de la Commission agit en tant que sous-traitant pour l'agence et le traitement est régi par un ANS,
ii) un centre médical externe réalise une partie ou la plupart des visites médicales pour le compte de l'agence et
iii) le médecin-conseil traite les données médicales dans les locaux de l'agence pour le compte de l'agence.

[7] Le Responsable local de la sécurité informatique de l'**ERCEA** a informé le CEPD, par une note envoyée le 23 septembre 2010, de l'état d'avancement de la politique de sécurité informatique applicable dans le domaine des données relatives à la santé.

Le CEPD souligne que la mise en œuvre des mesures de sécurité diffère dans chacune des catégories de sous-traitance précitées:

- dans le cas des ANS, les mesures de sécurité sont déjà en place à la Commission. Ceci bien sûr n'exclut pas que les agences appliquent un système de sécurité au sein de leurs propres locaux (voir point 2.9 ci-dessus);
- dans les cas où les agences ont conclu des contrats avec des centres médicaux externes, elles doivent veiller à ce qu'un niveau de sécurité approprié soit adopté et mis en œuvre par le sous-traitant externe, conformément à l'article 23, paragraphe 2, point b), et à l'article 23, paragraphe 3, du règlement; et
- dans les cas où les médecins-conseil exécutent leurs tâches dans les locaux des agences, celles-ci devront s'assurer par le biais du contrat conclu avec le médecin-conseil que celui-ci respecte les mesures de sécurité internes de l'agence, qui doivent être conformes à l'article 22 du règlement, comme le stipule l'article 23, paragraphe 1.

Plus particulièrement, l'agence ***EU-OSHA*** doit veiller à ce qu'un contrat ou tout autre instrument juridique contraignant soit établi entre le service médical externe et l'agence, conformément à l'article 23 du règlement. Cet instrument juridique doit disposer que le sous-traitant ne peut agir que sur instruction de l'agence. En outre, le prestataire devra se conformer à la législation nationale mettant en œuvre l'article 16 ou 17, paragraphe 3, deuxième tiret, de la directive 95/46/CE, et il devra assurer le respect des dispositions de la législation nationale en matière de sécurité et de confidentialité. L'agence **EU-OSHA** doit envoyer une copie du contrat au CEPD, y compris de ces éléments, dès qu'il a été conclu.

Les agences **AESC** et **AESA** ont conclu un ANS avec le service médical de la Commission à Luxembourg en 2006. Cependant, cet ANS ne fait pas référence à l'applicabilité du règlement. Le CEPD souligne que les ANS signés avec le service médical de la Commission à Bruxelles en 2008 par les agences concernées se réfèrent bien au règlement (CE) n° 45/2001. Le CEPD recommande par conséquent que tant l'**AESC** que l'**AESA** mettent à jour leur ANS avec le service médical de la Commission à Luxembourg et indiquent que le service médical applique les dispositions du règlement.

Les agences **ETF, ECHA, CEDEFOP, EUROFOUND** et **AESA** ont fourni au CEPD des copies similaires des contrats passés avec leurs prestataires médicaux externes et les médecins-conseil, agissant en tant que sous-traitants. Le CEPD recommande que les éléments suivants soient inclus dans leurs contrats:

- dans les contrats avec les centres médicaux externes, les agences **ECHA, AESA** et **EMSA** doivent inclure un addendum indiquant clairement les mesures de sécurité qui sont requises par l'agence et qui doivent être adoptées par le sous-traitant, conformément à l'article 23, paragraphe 2, point b), et l'article 23, paragraphe 3, du règlement;
- dans les contrats avec les médecins-conseil, les agences **ETF**, **ECHA** et **AESA** doivent inclure les mesures de sécurité que l'agence a adoptées en son sein, et les deux agences doivent veiller à ce que le niveau de sécurité requis soit respecté par le médecin-conseil, à la lumière de l'article 23, paragraphe 1, du règlement;
- en ce qui concerne l'article I.9 des contrats relatifs à la protection des données, le CEPD souligne qu'une simple référence aux données personnelles du contractant et à son droit d'accès n'est pas suffisante. Les personnes concernées doivent également être incluses puisqu'elles font partie de l'exécution du contrat. Le CEPD recommande par conséquent que l'article I.9 de tous les contrats fasse référence au «contractant», les agences **ETF**, **ECHA**, **AESA** et **EMSA** devant ajouter la phrase *«et les personnes concernées dont les données sont traitées par le contractant»*.

Pour ce qui est d'**EUROFOUND**, lorsque l'article I.8 de son contrat fait référence au «contractant», l'agence devra ajouter la phrase *«et les personnes concernées dont les données sont traitées par le contractant»*.

L'**ECDC** et le **CEDEFOP** doivent inclure dans leurs contrats avec les prestataires médicaux externes, une clause de protection des données ainsi qu'un addendum sur les mesures de sécurité que les agences exigent que leurs sous-traitants mettent en place, conformément aux articles 23, paragraphe 2, point b), et 23, paragraphe 3, du règlement.

L'**AEE** n'a pas fourni au CEPD une copie du contrat conclu avec le prestataire médical externe. Le CEPD recommande que l'AEE veille à ce que le contrat soit conforme aux exigences de l'article 23 du règlement et invite l'agence à lui envoyer une copie du contrat.

Conclusion

Les lignes directrices du CEPD ont aidé les agences à réfléchir à l'impact des principes de protection des données du règlement (CE) n° 45/2001 sur le traitement des visites médicales d'embauche, des visites médicales annuelles et des congés de maladie. Comme énoncé au point 2.1, malgré l'explication claire proposée dans les lignes directrices du CEPD sur le concept des «données relatives à la santé» au sens large, quelques agences ont néanmoins affirmé que les données qu'elles traitaient ne présentaient pas de risques spécifiques au sens de l'article 27, paragraphe 2, point a), du règlement.

Le CEPD souhaite attirer l'attention sur deux autres points dérivés de la présente analyse: la base juridique de la sous-traitance et la déclaration de confidentialité. Le CEPD note que certaines agences ont omis certains éléments courants dans leurs contrats avec des prestataires médicaux externes, notamment les mesures de sécurité et les clauses de protection des données. Ce sont là des éléments fondamentaux qu'il convient d'inclure dans les contrats avec les sous-traitants.

De plus, les agences n'ont pas saisi l'importance de la déclaration de confidentialité. Seule l'agence **EACI** a rédigé une déclaration de confidentialité quasi complète et conforme aux articles 11 et 12 du règlement. Le CEPD met l'accent sur le principe selon lequel les personnes concernées doivent être dûment informées pour que le traitement soit licite, et il convient dès lors qu'il soit basé sur les informations fournies conformément aux articles 11 et 12 du règlement. Le responsable du traitement doit donc fournir aux personnes concernées toutes les informations nécessaires sur le traitement, et sur leurs droits afférents, avant que l'opération de traitement ne commence. Ceci est particulièrement vrai dans les cas où le traitement est basé sur le consentement de la personne concernée.

Après analyse des lettres d'accompagnement des DPD, des informations fournies dans les notifications et de certaines remarques sur le projet d'avis envoyé pour commentaire, le CEPD juge nécessaire de souligner qu'une simple déclaration d'intention ou confirmation qu'une pratique spécifique en matière de protection des données sera appliquée conformément aux lignes directrices et aux recommandations du CEPD n'est pas suffisante pour la mise en œuvre des recommandations du CEPD. Il convient de prendre des mesures concrètes. Après émission et envoi de l'avis du CEPD au responsable du traitement, ce dernier devra totalement prendre en considération les recommandations du CEPD, adopter des mesures concrètes pour les mettre en œuvre dans les plus brefs délais et informer le CEPD de ces mesures. Cette partie de la procédure constitue le suivi des recommandations du CEPD pour une opération de traitement soumise à un

contrôle préalable. Le suivi doit avoir lieu dans les 3 mois à compter de l'émission de l'avis.

En conséquence, à la lumière du dernier document stratégique du CEPD relatif au contrôle et au respect du règlement (CE) n° 45/2001[8], le responsable du traitement de chaque agence concernée est maintenant invité à adopter des mesures concrètes et spécifiques afin de mettre en œuvre les recommandations du CEPD concernant le traitement des données relatives à la santé. Dans le cadre du suivi, chaque agence devra donc transmettre au CEPD des documents démontrant que les recommandations du CEPD ont bien été mises en œuvre.

Fait à Bruxelles,

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données

[8] Contrôler et garantir le respect du règlement (CE) n° 45/2001, Bruxelles, 13 décembre 2010,. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/10-12-13_PP_Compliance_FR.pdf