Avis sur une notification de contrôle préalable reçue du délégué à la protection des données de la Commission européenne au sujet de la base de données ARDOS

Bruxelles, le 15 décembre 2008 (dossier 2007/380)

1. Procédure

Le 6 juin 2007, le CEPD a reçu une notification en vue d'un contrôle préalable en vertu de l'article 27, paragraphe 3, du règlement (CE) n° 45/2001 («le règlement») du délégué à la protection des données (DPD) de la Commission européenne. Les traitements de données concernent la base de données ARDOS, le système d'information du Service de sécurité du Centre commun de recherche (CCR) à Ispra. Étaient jointes à la notification plusieurs annexes au traitement.

Le CEPD a demandé des informations complémentaires le 27 juin 2007. En raison de problèmes techniques, ces informations n'ont été transmises que le 17 mars 2008. D'autres informations ont été demandées les 1er et 2 avril, et reçues le même jour. Le 14 avril, le CEPD a envoyé au responsable du traitement le projet d'avis afin qu'il puisse formuler des commentaires, lesquels ont été reçus le 22 avril 2008. Du fait de la complexité du sujet, le CEPD a prolongé le délai d'un mois supplémentaire. Une nouvelle série de questions ont été envoyées au responsable du traitement le 21 mai 2008. Les informations ont été reçues le 19 juin 2008, mais à ce jour, aucune base juridique claire n'a été fournie. En l'absence de réponse concernant cette base juridique, le CEPD rend son avis aujourd'hui.

2. Les faits

Le présent contrôle préalable porte sur une base de données appelée ARDOS. ARDOS est le système d'information du Service de sécurité ainsi que la base de données d'archivage de tous les documents demandés par et présentés au Service de sécurité du CCR d'Ispra.

La base de données ARDOS sert plusieurs **finalités**.

i) Elle soutient l'émission du «nulla osta» pour les candidats à l'embauche de tous les sites du CCR sauf celui de Karlsruhe. La finalité de la procédure «nulla osta» est d'établir et de confirmer la bonne conduite des candidats sélectionnés à l'embauche. ARDOS gère le traitement des demandes de «nulla osta», de même que toute autre information relative à la sécurité collectée au cours de l'existence d'une relation contractuelle avec la personne concernée, y compris tout original de l'extrait de casier judiciaire.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax: 02-283 19 50

Les rapports des enquêtes de sécurité sont également conservés dans ARDOS.
ii) Les photographies collectées sont utilisées pour l'impression des cartes d'identité des membres du personnel (badges) et partagées avec le guide des services de la Commission. Les photographies de tous les membres du personnel du CCR sont conservées. Des badges sont également émis pour le personnel du CCR de Séville.

iii) Les informations concernant la présence de personnes sur le site sont également utilisées pour garantir l'application de la règle relative à la présence sur le site pendant 72 mois, aussi appelée «règle anti-cumul de 6 ans». En vertu de cette règle, la présence sur le site du CCR d'une personne autre qu'un fonctionnaire (notamment les stagiaires, les boursiers, les scientifiques en visite, les experts nationaux détachés, les agents contractuels et les agents temporaires) ne peut excéder 72 mois au cours d'une période de douze ans. Les périodes de travail accomplies dans d'autres services de la Commission sont également prises en considération.

L'émission d'un nulla osta ne peut avoir lieu qu'au terme de l'évaluation du comportement de la personne concernée. La présentation d'un extrait original et authentique du casier judiciaire vierge constitue l'élément le plus important et le plus pertinent à cet égard. Si le casier n'est pas vierge – ce qui est très rare -, il est examiné et, si nécessaire, la personne est interrogée par au moins deux agents du Service de sécurité afin d'évaluer en personne si elle est susceptible de constituer une menace pour la sécurité. Des dispositions sont également prises afin d'établir toute information manquante dans le formulaire de candidature et le curriculum vitae, ainsi que tout séjour dans des pays potentiellement dangereux.

Le nulla osta est décrit comme une attestation de sécurité dans la déclaration de confidentialité des archives du Service de sécurité (ARDOS). Les services de recrutement de tous les sites du CCR collectent l'extrait de casier judiciaire/le certificat de bonnes vie et mœurs nécessaire à l'émission d'une attestation de sécurité[1].

Les traitements de données **manuels** et **automatisés** sont interconnectés. Les documents de la personne concernée sont enregistrés sous version imprimée et/ou scannée. Il est à noter que le CCR ne conserve plus de documents sous format papier et s'active à l'heure actuelle à transformer les anciens documents imprimés en documents numériques. Des données peuvent également être importées de Sysper2 afin de mettre à jour le tableau des effectifs actifs ainsi que les informations concernant le service interne et les adresses des bureaux. Les traitements sont effectués manuellement pour la maintenance de la liste actualisée de toutes les personnes «actives» qui travaillent sur le site pour l'émission des nulla osta et des attestations de «présence sur le site» et pour l'archivage de toutes les informations historiques. Le système de référence pour toutes les autorisations de longue durée (à savoir les badges pour le personnel) ou autorisations spéciales délivrées par le Service de sécurité est un traitement manuel.

Les **personnes concernées** par le traitement sont les candidats présélectionnés pour un poste au CCR, toutes les catégories de personnel du CCR ainsi que les autres catégories de personnel (contractant externe) qui doivent se rendre régulièrement sur le site d'Ispra (ceux qui ont reçu un badge «Personnel»). Il convient de signaler que le traitement ne concerne pas les visiteurs quotidiens qui se rendent sur le site de manière occasionnelle[2].

[1] Ce terme spécifique est utilisé dans les cinq notifications de recrutement du personnel du CCR qui ont été soumises au contrôle préalable du CEPD: 2008-140, 2008-141, 2008-142, 2008-143, 2008-136.
[2] Concernant le badge «Visiteurs» quotidiens, voir la lettre datée du 29 novembre 2007 concernant la base de données SECPAC disponible sur le site du CPED:

Les **données** traitées sont les suivantes: le nom, le prénom, la date et le lieu de naissance, la nationalité, le sexe, l'adresse privée complète, le numéro de téléphone de contact, le type de contrat (fonctionnaire, agent temporaire, agent contractuel, etc.), l'adresse interne, le numéro de téléphone interne, les dates de début et de fin des autorisations de longue durée, les demandes de formulaire d'attestation de sécurité, le CV, le document d'identité, la photographie et le certificat de bonnes vie et mœurs du candidat, l'avis de vacance auquel il répond, les données liées aux installations de la *Foresteria*[3], des documents variés ainsi que des documents de contrôle. Par «documents de contrôle», le Service de sécurité entend les dossiers des enquêtes de sécurité qui sont conservés dans la base de données ARDOS.

Le Service de sécurité a mis en place une procédure de sécurité grâce à laquelle les personnes concernées peuvent demander et vérifier que les données soient enregistrées et associées à leur identité. Le service JRC SECPAC SUPPORT (jrc-secpac-support@ec.europa.eu) est le principal point de contact; il autorise l'**accès** aux données à caractère personnel et leur correction. Par exemple, une procédure spéciale de renvoi de l'extrait original du casier judiciaire a été mise en place. À tout moment, les personnes concernées peuvent demander et effectuer une mise à jour de leur photographie, éventuellement en introduisant une photographie prise par un service de photographie externe. L'adresse privée et les coordonnées privées pour les cas d'urgence sont généralement mises à jour au moment de la délivrance, du renouvellement ou du remplacement d'un badge «Personnel», mais leur mise à jour peut également être effectuée à tout autre moment.

Sur demande motivée de la personne concernée après la cessation d'une relation contractuelle, ses données peuvent être modifiées, gelées, voire effacées en une période maximale de 14 jours.

Concernant la **conservation des données**, ARDOS contient actuellement des informations historiques ainsi que toutes les données collectées qui ont été conservées au fil des années. Le Service de sécurité prévoit d'adopter les périodes de conservation suivantes:
- les données collectées concernant les candidats qui retirent leur candidature ou ne sont pas recrutés mais pour lesquels un traitement «nulla osta» a été réalisé seront conservées pendant une période d'un an;
- les données seront conservées aussi longtemps qu'une relation contractuelle existera avec le membre du personnel concerné ainsi que pendant l'année qui suivra la cessation de la relation contractuelle;
- les données seront conservées aussi longtemps que des actions de suivi liées à la règle relative à la présence sur le site pendant 72 mois seront nécessaires. Les données liées à toute interaction avec le Service de sécurité seront par conséquent supprimées après 12 ans.

La base de données ARDOS est destinée à un usage interne au sein du Service de sécurité. Les données qu'elle renferme ne sont jamais **transférées** directement ou accessibles à des tiers, étant donné que le système d'information constitue un réseau physiquement isolé. Les informations fournies sur la base d'une nécessité motivée à partir des données ARDOS sont toujours traitées et éditées dans un modèle de document uniformisé (modèles Nulla osta ou Présence sur le site). Seuls les membres clés du personnel des ressources humaines responsables du processus de recrutement sur tous les sites peuvent solliciter un nulla osta Sécurité auprès du Service de sécurité. Une clause légale est jointe au nulla osta requis. Elle

---

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Letters/2007/07-11-28_Commission_JRC_SECPAC_EN.pdf

[3] Le CCR met à la disposition du personnel non permanent (boursiers, etc.) les installations de la *Foresteria* (appartements). Le registre des résidents de la *Foresteria* est également conservé dans ARDOS.

mentionne les articles 7, paragraphe 3, et 4, paragraphe 2, du règlement n° 45/2001. Le directeur du site d'Ispra peut demander des informations supplémentaires en cas d'urgence ou d'enquête.

Les photographies des badges du personnel statutaire de tous les sites du CCR sont exportées de la base de données ARDOS et transférées dans le Guide des services, c'est-à-dire le répertoire de la Commission établi sur la base de SYSPER2. Une clause légale, jointe à la liste des photographies des membres du personnel, mentionne les articles 7, paragraphe 3, et 4, paragraphe 2, du règlement n° 45/2001.

Les destinataires sont les suivants: le personnel permanent du Service de sécurité se décline sous divers profils dont ceux de responsable de la sécurité, d'archiviste de la sécurité et d'administrateur. Les responsables de la sécurité ont accès aux données à caractère personnel et aux photographies. Les archivistes de la sécurité ont accès à toutes les informations enregistrées, et notamment aux informations documentaires. Les administrateurs ont un accès illimité à toutes les fonctionnalités d'ARDOS, dont la gestion de ces profils. Parmi les destinataires figurent également le personnel statutaire agréé permanent responsable du processus de recrutement.

Une déclaration de confidentialité doit être publiée sur l'intranet du CCR. Elle inclut des informations sur l'identité du responsable du traitement, les finalités du traitement, les catégories de données concernées, les destinataires des données, l'existence du droit d'accès et de rectification, le délai de conservation des données et le droit de saisir à tout moment le CEPD. Aucune autre communication explicite n'est prévue en raison de la nécessité de remplir diverses obligations dont celle liée à la gestion des sites de recherche sur le nucléaire. Toutes les personnes concernées savent également que leur photographie est nécessaire à la production matérielle de leur badge. Le bureau d'accueil fournit aux membres du personnel les instructions et l'accompagnement nécessaires pour la réalisation de leur photographie.

3. Aspects juridiques

3.1. Contrôle préalable

Le présent avis de contrôle préalable porte sur la collecte et le traitement ultérieur d'informations personnelles réalisés par le CCR en vue de décider s'il convient d'accorder ou de refuser le nulla osta aux candidats présélectionnés (excepté pour le personnel du site de Karlsruhe). La base de données ARDOS traite également les photographies de tous les employés du CCR ainsi que les informations relatives à la présence de personnes sur le site (Ispra).

Le règlement (CE) n° 45/2001 s'applique au *«traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier»* ainsi qu'au *«traitement de données à caractère personnel 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»*[4]. Pour les raisons mentionnées ci-dessous, tous les éléments requis pour l'application du règlement sont présents.

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

Premièrement, les données à caractère personnel telles qu'elles sont définies à l'article 2, point a), du règlement sont collectées et traitées ultérieurement afin de déterminer si les candidats sont éligibles au nulla osta. Deuxièmement, les données à caractère personnel collectées sont soumises à un «traitement automatisé», tel que défini à l'article 2, point b), du règlement, ainsi qu'à un traitement manuel (auquel cas les données traitées sont contenues ou appelées à figurer dans un fichier). En effet, les informations personnelles sont dans un premier temps collectées sur format papier et électronique, pour être ensuite introduites dans la base de données ARDOS. Enfin, le traitement est réalisé par un organe communautaire, en l'espèce le CCR, dans le cadre du droit communautaire (article 3, paragraphe 1, du règlement). Par conséquent, tous les éléments requis pour l'application du règlement sont présents dans ce traitement de données.

En vertu de l'article 27, paragraphe 1, du règlement (CE) n° 45/2001, *«(l)es 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 sont soumis au contrôle préalable du contrôleur européen de la protection des données»*. Le paragraphe 2 contient une liste des traitements susceptibles de présenter de tels risques. Cette liste inclut, au point a), les traitements de données *«relatives à des suspicions, infractions, condamnations pénales ou mesures de sûreté»*. Ce type d'informations est collecté afin de permettre au CCR d'évaluer la fiabilité des candidats et de déterminer s'il convient ou non d'émettre un nulla osta. En outre, en vertu du point b), *«les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur (…) comportement»* devraient être soumis à un contrôle préalable. La finalité de la procédure «nulla osta» est d'établir et de confirmer la bonne conduite des candidats sélectionnés à l'embauche. Si les responsables de la sécurité ont des doutes concernant les informations fournies par la personne concernée, ils l'interrogeront afin d'évaluer son comportement. Dès lors, les traitements doivent être soumis au contrôle préalable du CEPD.

Il est à noter que la base de données ARDOS renferme également les rapports publiés dans le cadre d'enquêtes de sécurité sur le site d'Ispra. Ce traitement spécifique a été soumis au contrôle préalable du CEPD le 31 juillet 2008 (dossier 2007-507)[5].

Étant donné que le contrôle préalable vise à évaluer des situations susceptibles de présenter certains risques, le CEPD devrait rendre son avis avant le début du traitement. Dans le cas présent, cependant, le traitement a déjà été établi, et cela pose de graves problèmes au vu des conclusions du présent avis. En effet, pour garantir la conformité avec le règlement (CE) n° 45/2001, il conviendrait d'identifier, de produire ou d'établir une base juridique adéquate et d'adopter les autres recommandations du CEPD (voir les conclusions au point 4).

La notification a été reçue le 6 juin 2007. Conformément à l'article 27, paragraphe 4, du règlement (CE) n° 45/2001, la période de deux mois au cours de laquelle le CEPD doit rendre son avis a été prolongée d'un mois en raison de la complexité du sujet, et suspendue pendant une période totale de 401 jours, plus deux mois d'août.

3.2. Licéité du traitement

Les données à caractère personnel ne peuvent être traitées que s'il existe une base juridique légitimant ce traitement à l'article 5 du règlement. Les motifs qui justifient le traitement semblent être fondés sur l'article 5, point a), en vertu duquel les données peuvent être traitées

[5] Voir le site du CEPD: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2008/08-07-31_Commission_security_investigations_Ispra_FR.pdf

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 en question sont légitimes au titre de l'article 5, point a), du règlement, deux éléments sont à prendre en considération: premièrement, il doit exister, sur la base des traités ou d'autres actes législatifs, une mission effectuée dans l'intérêt public qui requiert le traitement de données à caractère personnel par le responsable du traitement, comme c'est le cas dans la présente affaire (base juridique), et deuxièmement, le traitement doit être effectivement nécessaire à l'exécution de ladite mission (test de nécessité). Il convient de mentionner, à ce stade, qu'aucun autre motif n'a été jugé pertinent; la présente analyse peut dès lors se limiter à l'article 5, point a), du règlement.

Base juridique «nulla osta»

En ce qui concerne la détermination des motifs juridiques compris dans les Traités ou d'autres actes législatifs (y compris les législations nationales) susceptibles de légitimer en principe le traitement (*base juridique*), il convient de souligner, à titre de remarque générale, que la procédure nulla osta s'applique aux membres du personnel de tous les sites du CCR, à l'exception de celui de Karlsruhe. Cela signifie que différents pays sont concernés (Espagne, Italie, Belgique et Pays-Bas), ainsi que différentes activités (protection et sécurité des citoyens, environnement et durabilité, santé et protection des consommateurs, etc.). Par conséquent, une partie des documents juridiques proposés comme base juridique par le responsable du traitement concernant des activités nucléaires et la législation italienne n'est pas pertinente, comme expliqué plus loin, pour les sites non concernés par la recherche nucléaire et/ou les sites italiens.

Les paragraphes qui suivent analysent les différents instruments qui ont été proposés par le responsable du traitement en tant que base juridique.

Premièrement, la loi italienne L. 1° agosto 1960, n.906 portant approbation de l'exécution de l'accord conclu entre le gouvernement italien et la Commission a été mentionnée dans la notification. L'article 2 de l'annexe F fait référence à des mesures de sécurité générales, dont les suivantes: 1) la sécurité extérieure est garantie par les autorités italiennes, 2) les autorités italiennes interviendront sur le site uniquement à la demande unanime des membres de la Commission, et 3) le site d'Ispra ne devrait pas, même temporairement, accueillir une personne qui fait l'objet de poursuites judiciaires pour violation de la législation italienne. Pour information, l'article 21 de l'annexe F insiste sur la protection du secret et l'article 35 établit que toutes les mesures nécessaires devraient être prises par la Commission pour éviter toute violation de l'accord.

Les points 1) et 2) de l'article 2 de l'annexe F constituent en réalité une base juridique permettant de s'opposer à l'intervention des autorités italiennes sur le site d'Ispra sans le consentement de la Commission, tout en veillant à ce que ces autorités prennent en charge tout problème extérieur survenant aux alentours du site, par exemple une manifestation. En revanche, ils ne couvrent pas les contrôles de sécurité individuels tels que la procédure nulla osta, pour laquelle le point 3) pourrait être particulièrement pertinent.

En effet, pour mieux comprendre la *ratio legis* de l'article 2 de l'annexe F, il doit être rappelé que la législation susmentionnée établit l'accord conclu entre la Commission et l'État italien en vue du financement d'un centre de recherche nucléaire. Dans ce cadre particulier ainsi que dans le cadre général de l'établissement d'une autorité ou institution communautaire au sein

d'un État membre, l'État hôte et l'institution conviennent de coopérer sur les questions de sécurité. Les dispositions de l'article 2 leur permettent de définir leurs compétences respectives. L'application de l'article 2, point 3), requiert que des mesures de sécurité spécifiques soient prises par le Service de sécurité d'Ispra afin d'empêcher le recrutement de personnes faisant l'objet de poursuites judiciaires pour infraction à la législation italienne. Néanmoins, cette base juridique générale ne s'appliquerait que sur le site d'Ispra et, même dans pareil cas, ne peut justifier d'investiguer sur des éléments autres que l'existence de poursuites judiciaires. Quant aux autres sites concernés, la loi italienne ne s'applique pas aux sites du CCR établis dans d'autres pays.

Deuxièmement, le plan de protection physique du CCR, approuvé par décret du ministère italien de l'industrie (VII-260, 21/7/1987) et auquel le CEPD n'avait pas accès, ne peut pas non plus être utilisé comme base juridique pour l'émission du nulla osta. Ainsi que l'entend le CEPD, ce plan est établi afin de garantir la sécurité physique dans le sens de la protection sanitaire de la population travaillant sur le site d'Ispra ainsi que la sûreté des installations nucléaires (évacuation, etc.), et non pour définir la procédure nulla osta. De plus, le plan s'applique au site d'Ispra et non à tous les sites du CCR.

Le document de la protection physique du matériel nucléaire et des installations nucléaires élaboré par l'Agence internationale de l'énergie atomique (AIEA) fournit des lignes directrices sur l'accès au matériel et aux installations nucléaires. Le CEPD ne remet pas en cause le contrôle de cet accès qui, par essence, devrait être très rigoureux. Il conteste le fait que l'accès général à chaque site du CCR soit gouverné par ce plan relatif au nucléaire, indépendamment des activités réalisées sur le site. Ce document ne peut dès lors être considéré comme une base juridique pour la procédure nulla osta.

Troisièmement, la décision de la Commission du 8 septembre 1994 décrit les missions du bureau de sécurité de la Commission en termes de protection des personnes, de protection des bâtiments et de la propriété et de protection de l'information et de transmission et de traitement des données. Selon cette décision, ces missions doivent inclure la collecte d'informations aux fins de l'évaluation des menaces ou risques potentiels pour les départements de la Commission (article 3, point a)) et la vérification du respect des règles de sécurité par les départements de la Commission (article 3, point d)). L'article 6 prévoit que le bureau de sécurité gère les relations avec les services nationaux de sécurité et de renseignement en vue de collecter les informations requises afin d'évaluer les menaces et risques potentiels pour la Commission, ainsi qu'avec les autorités nationales en ce qui concerne les questions relatives à la protection des bâtiments de la Commission, à l'application des législations pénales et à l'immunité des fonctionnaires contre toute poursuite judiciaire en cas problème de sécurité.

Comme indiqué plus bas, il semble nécessaire d'adopter des mesures de sécurité spéciales afin de garantir la protection des sites du CCR. La décision de la Commission détaille les missions du bureau de sécurité. Elle ne prévoit toutefois aucun contrôle de sécurité individuel sauf en cas de flagrant délit ou d'enquête administrative. La procédure nulla osta, qui est un contrôle de sécurité «a priori» systématique, va au-delà des situations couvertes par la décision.

Le CEPD est d'avis que même si la décision de la Commission pouvait être utilisée comme base juridique générale pour la mise en œuvre de la procédure nulla osta, son texte ne décrit pas de manière suffisamment explicite la nature et la portée de cette procédure pour satisfaire aux exigences d'accessibilité et de prédictibilité d'une base juridique en vertu de l'article 8,

paragraphe 2, de la Convention européenne des droits de l'homme, qui sont aussi pertinentes au titre des articles 7 et 52 de la Charte des droits fondamentaux de l'Union européenne.

En outre, le CEPD constate que le cadre juridique susmentionné ne dresse pas un tableau clair des tâches et compétences concrètes du bureau de sécurité de la Commission (direction de la sécurité de la DG ADMIN) et de celles des bureaux de sécurité des institutions, services et départements, tels que le service de sécurité du CCR d'Ispra. À cet égard, il convient de déterminer si le service de sécurité du CCR d'Ispra est habilité à mener les activités décrites dans la décision ou si cette compétence est limitée au bureau de sécurité de la Commission (DG ADMIN).

Enfin, l'article 28 du statut des fonctionnaires et les articles 12, paragraphe 2, point c), et 82, paragraphe 3, point c), du régime applicable aux autres agents des Communautés européennes ont été mentionnés dans la notification. Ces articles soulignent que nul ne peut être engagé comme agent s'il n'offre les garanties de moralité requises pour l'exercice de ses fonctions et s'il ne jouit de ses droits civiques. Les traitements de données notifiés en vue d'un contrôle préalable vont bien au-delà du critère établi par le statut des fonctionnaires: *«requises pour l'exercice de ses fonctions»*. Le traitement nulla osta n'est pas réalisé par les unités de recrutement mais par le service de sécurité et est décrit dans divers documents traités tant par les unités de recrutement que par les services de sécurité comme étant une «attestation de sécurité». Cette attestation, dans le contexte de la CE, est établie pour des personnes sollicitant l'accès à des informations classifiées (2001/844/CE, CECA, Euratom: Décision de la Commission du 29 novembre 2001 modifiant son règlement intérieur [notifiée sous le numéro C(2001) 3031]) et non automatiquement dans le cadre d'un recrutement. Le CEPD souligne la distinction qui devrait être établie entre la collecte d'extraits de casiers judiciaires comme condition préalable au recrutement et le traitement effectué en vue de l'émission d'un nulla osta. Le traitement ne peut dès lors être réalisé en application de cette base juridique.

Le CEPD ne conteste pas la nécessité, pour le CCR, de collecter les extraits de casiers judiciaires afin de satisfaire à la condition de recrutement prévue à l'article 28. Il ne conteste pas non plus la nécessité d'obtenir l'attestation de sécurité CE pour certains membres du personnel (voir l'analyse plus bas). Par contre, il remet en cause l'existence d'une base juridique claire pour l'exécution, par le service de sécurité, d'un contrôle de sécurité/nulla osta préalable systématique pour chaque membre du personnel du CCR. Pour les aspects/besoins spécifiques non couverts par l'article 28 ou par l'attestation de sécurité CE, le service de sécurité du site d'Ispra devrait être doté de compétences spécifiques supplémentaires pour répondre aux besoins de sécurité strictement définis. Une base juridique spécifique devrait ensuite être identifiée, produite ou élaborée pour le système, en gardant à l'esprit que la base juridique devrait être suffisamment précise, couvrir différents pays et activités du CCR et respecter les critères de nécessité et de proportionnalité qui sont détaillés ci-dessous.

Base juridique pour les badges réservés au personnel et les données relatives à la foresteria

La base juridique pour l'impression de badges pour toutes les catégories de personnel du CCR et les autres catégories de personnel qui doivent se rendre régulièrement sur le site d'Ispra est contenue dans le règlement italien 626/1994 sur la sécurité, qui renferme des articles liés à la nécessité de maintenir des listes d'accès sur le site et dans les zones critiques ainsi que des listes d'évacuation en temps réel dans l'éventualité d'un incident conventionnel ou nucléaire. L'article 34, paragraphe 2, de la loi L. 1° agosto 1960, n.906 constitue la base juridique pour la collecte et la conservation des données relatives à la *foresteria*.

Test de nécessité

Concernant la nécessité du traitement, le CEPD note que la protection des sites du CCR représente un aspect sensible en raison de la nature de certaines activités et de la confidentialité des informations traitées. Au regard de la pertinence de ces intérêts et afin d'éviter toute divulgation non autorisée de ces informations (p. ex. la protection du secret telle qu'elle est mentionnée dans la loi italienne L. 1° agosto 1960, n.906, article 21), il apparaît nécessaire que le CCR adopte des mesures de sécurité spéciales, concernant non seulement les risques externes, mais également les risques internes. La procédure nulla osta semble être une mesure de contrôle interne visant à protéger les informations confidentielles du CCR et relatives à la politique nucléaire.

Ces contrôles internes visent notamment à empêcher l'accès aux locaux du CCR aux personnes qui, au vu de leurs antécédents, en particulier de leur casier judiciaire, sont susceptibles de représenter une menace pour le CCR. Pareillement, pour réduire les risques au minimum, il importe que le Centre ne recrute que des personnes dont le casier judiciaire ne remet pas en cause leur capacité à maintenir des normes élevées d'éthique professionnelle dans le cadre de l'exécution de leurs tâches au sein du CCR. Afin de filtrer les candidats qui ne répondraient pas à ces normes ou dont la seule présence dans les locaux du CCR pourrait représenter une menace pour le Centre, il semble nécessaire de collecter et de traiter ultérieurement les données à caractère personnel qui révèlent les antécédents de ces personnes.

Toutefois, le CEPD est d'avis que l'émission d'un nulla osta du même niveau pour toutes les catégories de personnel est excessive au vu du principe de nécessité. Les données ou zones sensibles devraient requérir des autorisations spécifiques, ce qui ne serait pas le cas pour les dossiers administratifs normaux, par exemple, et les locaux ordinaires. Par ailleurs, comme décrit plus haut, la procédure uniformisée de délivrance des attestations de sécurité vise à accorder l'accès aux informations et locaux sensibles.

Le CEPD est d'avis que le CCR devrait réviser sa politique de procédure nulla osta en matière de proportionnalité et de nécessité, en gardant à l'esprit un instrument tel que l'attestation de sécurité CE.

3.3. Traitement portant sur des catégories particulières de données

Le traitement de données notifié ne porte pas sur des données appartenant aux catégories visées à l'article 10, paragraphe 1, du règlement (CE) n° 45/2001.

Le traitement inclut manifestement des données relatives aux infractions et aux enquêtes en cours, qui sont couvertes par l'article 10, paragraphe 5, du règlement. Par exemple, les candidats doivent dans tous les cas soumettre un extrait de leur casier judiciaire. Le CEPD rappelle à cet égard l'application de l'article 10, paragraphe 5, du règlement (CE) n° 45/2001, qui établit que *«(l)e traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que s'il est autorisé par les traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités ou, si cela s'avère nécessaire, par le contrôleur européen de la protection des données, sous réserve des garanties spécifiques et appropriées».* En l'espèce, le traitement des casiers judiciaires est autorisé au titre des actes législatifs mentionnés au point 3.2 ci-dessus en ce qui concerne le recrutement.

Comme indiqué plus haut dans l'analyse de la base juridique, la condition prévue à l'article 10, paragraphe 5, ne sera remplie que si un acte législatif autorisant le Service de sécurité du site d'Ispra à collecter les données requises pour l'application d'une procédure nulla osta peut être invoqué.

Concernant les autres catégories particulières de données, l'article 10, paragraphe 1, du règlement établit que *«(l)e traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé ou à la vie sexuelle sont interdits»*.

D'après la notification de contrôle préalable, aucune catégorie de données visées à l'article 10, paragraphe 1, n'est traitée dans ARDOS. Au vu de la finalité globale des traitements nulla osta effectués par le CCR d'Ispra, le CEPD en déduit que le site d'Ispra n'envisage pas la collecte de ces catégories particulières de données.

3.4. Qualité des données

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 s'agit du principe de qualité des données. Dans son analyse du respect de ce principe par le traitement en question, qui implique essentiellement le traitement de données relatives à des suspicions, infractions ou condamnations pénales, le CEPD note ce qui suit.

Premièrement, la déclaration de confidentialité mentionne la collecte d'un extrait de casier judiciaire alors que la lettre d'invitation pour le recrutement requiert du fonctionnaire et de l'agent temporaire un certificat de bonnes vie et mœurs récent, et de l'agent contractuel un certificat de bonnes vie et mœurs récent et d'un extrait de casier judiciaire. En termes juridiques et en particulier dans certains États membres, les certificats de bonnes vie et mœurs contiennent des informations qui vont au-delà de celles contenues dans un extrait de casier judiciaire. Dans certains États membres notamment, un certificat de bonnes vie et mœurs peut contenir des informations sur la personnalité, la moralité, etc. d'une personne. Même si, en principe, le CEPD estime que la collecte de ce type de documents est licite, une analyse au cas par cas du contenu du casier judiciaire national ou du certificat de bonnes vie et mœurs devrait être réalisée afin de collecter uniquement des données pertinentes au regard des exigences prévues par le statut des fonctionnaires.

Deuxièmement, en l'absence de base juridique claire, les données collectées par le Service de sécurité (formulaires de candidature, CV, etc.) sont excessives au regard des finalités pour lesquelles elles sont collectées. Le formulaire de candidature et le CV ne sont pas collectés aux fins de l'émission d'un nulla osta, mais pour assurer à l'institution les services des personnes présentant le niveau de compétence, de performance et d'intégrité le plus élevé. Le CEPD est d'avis que la nécessité de chaque catégorie de données collectées par le Service de sécurité dans la base de données ARDOS doit être démontrée par le CCR. En outre, cela soulève la question de la légitimité du transfert de ces données par les services de recrutement au service de sécurité (voir le point 3.6 ci-dessous). Le fichier nulla osta constitué dans la base de données ARDOS ne devrait en aucun cas devenir un duplicata du dossier individuel. Le CEPD souhaiterait rappeler qu'en vertu de l'article 26 du statut des fonctionnaires, «(i)l ne peut être ouvert qu'un dossier pour chaque fonctionnaire». Dès lors, les CV, formulaires de candidature, etc. qui sont inclus dans le dossier individuel ne devraient pas être copiés et conservés dans la base de données ARDOS.

Troisièmement, il n'existe aucun critère spécifique pour guider les responsables de la sécurité dans l'émission des nulla osta. Il en résulte, comme indiqué plus haut, une collecte excessive de données. Le CEPD est d'avis que l'adoption d'un document formel décrivant et définissant la procédure en place aiderait le CCR à veiller au respect du principe de qualité des données.

Pour ce qui est des enquêtes et demandes individuelles, la nécessité et la pertinence des données collectées sont analysées dans l'avis 2007-507 susmentionné relatif aux enquêtes de sécurité au Centre commun de recherche d'Ispra.

L'article 4, paragraphe 1, point a), du règlement exige que les données soient traitées loyalement et licitement. La question de la licéité a été analysée plus haut (voir le point 3.2), tandis que celle de la loyauté est étroitement liée à l'information des personnes concernées, qui sera examinée au point 3.9.

En vertu de l'article 4, paragraphe 1, point d), du règlement, les données à caractère personnel doivent être «exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables sont prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées». En l'espèce, les données incluent les extraits de casier judiciaire. Le système en tant que tel devrait garantir que les données sont exactes. La personne concernée fournit les données qui seront traitées: CV, formulaire de candidature, extrait du casier judiciaire. Une procédure permettant aux personnes concernées de demander quelles données les concernant sont enregistrées et de vérifier ces données a été mise en place (voir, à cet égard, la discussion au point 3.8).

3.5. Conservation des données

En vertu de l'article 4, paragraphe 1, point e), du règlement (CE) n° 45/2001, les données à caractère personnel peuvent 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 juge appropriée la période de conservation prévue par le CCR (les données sont conservées aussi longtemps qu'il existe une relation contractuelle avec le membre du personnel concerné ainsi que pendant l'année qui suivra la cessation de la relation contractuelle). En effet, dans les cas où le CCR pourrait invoquer une base juridique pour la mise en œuvre d'une procédure nulla osta, il semble approprié que le Service de sécurité puisse reconsulter les informations sur la base desquelles le nulla osta a été émis à tout moment pendant la durée du contrat de travail et pendant une période déterminée suivant la fin du contrat. En revanche, il ne semble pas approprié que le CCR conserve des informations – aux fins de la procédure nulla osta ou aux fins du recrutement – sur des délits pour lesquels il y a prescription et qui ne figureraient plus dans le casier judiciaire. Pour cette raison, le CCR devrait mettre en place un système garantissant la suppression de ces informations. Le droit d'accès et de rectification (voir le point 3.8) pourrait être utile à cet égard. Une autre solution consisterait à conserver dans le dossier un «formulaire standard» indiquant l'aptitude de la personne à exécuter les tâches qui lui incombent, tandis que l'extrait de casier judiciaire serait restitué à la personne. Le CEPD insiste sur le fait que la durée de conservation des données prévue par le Centre devrait être introduite au plus tôt.

En outre, des données sont également nécessaires pour l'application de la règle relative à la présence sur le site pendant 72 mois. Dans ce domaine, les données relatives à toute interaction avec le Service de sécurité seront effacées après douze ans. Le CEPD est d'avis que seules les données nécessaires aux fins de la gestion de la règle des 72 mois devraient être conservées.

Le CEPD recommande que toutes les informations historiques soient conservées sous une forme anonyme ou supprimées de la base de données, conformément à l'article 4, paragraphe 1, point e), du règlement.

3.6. Transfert de données

D'après les faits, des informations peuvent être transférées au directeur du site d'Ispra en cas d'urgence ou d'enquête de sécurité (voir l'avis 2007-507). Les photographies des badges du personnel statutaire de tous les sites du CCR sont exportées de la base de données ARDOS pour être transférées dans le Guide des services de la Commission. Le nulla osta ne peut être transféré qu'aux membres clés du personnel des ressources humaines responsables du processus de recrutement sur tous les sites, mais en aucun cas les données ne seront transférées en dehors de la Commission. En conséquence, l'article 7 du règlement, qui établit certaines obligations pour les responsables du traitement lorsqu'ils transfèrent des données à caractère personnel aux institutions et organes communautaires, sera d'application.

Le CEPD rappelle que l'article 7 n'autorise les transferts de données que si ces dernières sont «nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire». Aux fins du respect de cette disposition, le Service de sécurité doit s'assurer, lorsqu'il transfère des données à caractère personnel, i) que le destinataire possède les compétences requises et ii) que le transfert est nécessaire. Ces conditions semblent être remplies dans le cas présent. Il convient de noter que le CEPD a été consulté au sujet de l'introduction de photographies dans le répertoire de la Commission[6].

En vertu de l'article 7, paragraphe 2, lorsque les données sont transférées à la suite d'une demande du destinataire, tant le responsable du traitement que le destinataire assument la responsabilité de la légitimité de ce transfert. Le destinataire veille à ce que la nécessité du transfert des données puisse être ultérieurement vérifiée. Dans le cas à l'examen, la procédure nulla osta est ouverte à la demande de l'unité des ressources humaines, mais le transfert des documents justificatifs (CV, formulaire de candidature) est demandé par le responsable de la sécurité. La nécessité du transfert devrait être évaluée après que la base juridique a été déterminée.

Outre les éléments susmentionnés, il importe, au titre de l'article 7 du règlement, que le destinataire soit informé que les données à caractère personnel doivent être traitées uniquement aux fins qui ont motivé leur transmission[7]. Pour rappel, ces avis sont transmis aux membres clés du personnel des ressources humaines responsables du processus de recrutement ainsi qu'au Guide des services de la Commission.

[6] Voir la lettre du 6 janvier 2005, 2005-347

[7] Ce point a été discuté dans l'avis du CEPD du 8 mars 2006 concernant une notification de contrôle préalable au sujet du dossier «Affaires disciplinaires (comprenant l'examen administratif connexe des réclamations et doléances et les affaires dont sont saisis le médiateur et la Cour)» (dossier 2004-270).

3.7. Traitement du numéro personnel ou identifiant unique

L'article 10, paragraphe 6, du règlement prévoit que *«(l)e contrôleur européen de la protection des données détermine les conditions dans lesquelles un numéro personnel ou tout autre identifiant utilisé de manière générale peut faire l'objet d'un traitement par une institution ou un organe communautaire»*.

La base de données ARDOS contient le numéro personnel de la personne concernée. Le CEPD estime que le numéro personnel peut être utilisé de manière adéquate dans ce contexte, étant donné qu'il permet l'identification du membre du personnel concerné et facilite la mise en œuvre d'un suivi adéquat. Il n'y a pas lieu d'établir d'autres conditions dans le cas présent.

3.8. Droit d'accès et de rectification

En vertu de l'article 13 du règlement (CE) n° 45/2001, la personne concernée a le droit d'obtenir, sans contrainte, à tout moment dans un délai de trois mois à partir de la réception de la demande d'information et gratuitement, du responsable du traitement la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données. L'article 14 octroie à la personne concernée le droit de rectifier toute donnée inexacte ou incomplète.

Le Service de sécurité accorde le droit d'accès et de rectification des données incluses dans la base de données. Il notifie aux personnes concernées la possibilité d'exercer ces droits et leur fournit des informations sur la personne à contacter à cette fin. Pour s'assurer que les demandes d'accès seront traitées dans les délais et sans contrainte, le CCR fixe un délai raisonnable de 14 jours. À titre d'exemple, les personnes concernées peuvent, à tout moment, demander et effectuer une mise à jour de leur photographie, éventuellement en introduisant une photographie prise par un service de photographie externe.

L'application du droit de rectifier des données inexactes peut permettre aux personnes concernées de demander la mise à jour de leur casier judiciaire. En effet, comme il a été souligné au point 3.5, après un certain temps, il y a prescription et, à compter de ce moment, il n'est plus fait mention du délit dans le casier judiciaire. L'article 14 du règlement prévoit le droit de rectifier toute donnée inexacte ou incomplète, ce qui signifie dans le cas présent que les personnes concernées devraient être capables de mettre à jour – fournir une version mise à jour de – leur casier judiciaire afin de refléter au plus près leur situation du moment. Comme indiqué plus haut, en conservant des informations sur des délits pour lesquels il y a prescription, le CCR enfreindrait le principe de qualité des données décrit plus haut, en vertu duquel les données à caractère personnel doivent être *«exactes et, si nécessaire, mises à jour»*.

Afin de garantir le respect des articles 14, et 4, paragraphe 1, points d) et e), du règlement (droit de rectification, principes de qualité des données et de conservation des données), le CCR devrait établir un système destiné à garantir l'application effective du contenu de ces droits et principes en ce qui concerne le certificat de bonnes vie et mœurs et l'extrait du casier judiciaire.

Le CEPD fait remarquer que, dans le cadre de l'instauration d'un tel système, assurer seul le fonctionnement d'un système destiné à supprimer automatiquement les informations relatives aux délits pour lesquels il y a prescription peut s'avérer une tâche lourde et difficile pour le CCR, notamment du fait des disparités éventuelles entre les pays. Le CCR peut ne pas être en mesure de vérifier constamment que le délai de prescription est ou non écoulé pour les délits contenus dans les certificats de bonnes vie et mœurs. En revanche, il est en mesure d'informer

les personnes concernées de la possibilité de fournir des versions mises à jour de leurs certificats de bonnes vie et mœurs ou de leurs extraits de casier judiciaire tout au long de leur relation de travail avec le CCR.

Ainsi, le CEPD invite le CCR à rappeler aux personnes concernées l'existence de cette possibilité, soit dans la déclaration de confidentialité, soit dans un document distinct. En offrant cette possibilité, le CCR permet en réalité aux personnes concernées d'exercer leur droit de rectification des données inexactes au titre de l'article 14 du règlement. Il contribue également à l'application du principe de qualité des données. En outre, il met en œuvre le principe qui limite la conservation des informations lorsqu'elles ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été traitées.

Le CEPD note, à cet égard, que le CCR peut se voir dans l'obligation de conserver les certificats de bonnes vie et mœurs pendant un certain temps afin d'avoir à sa disposition des preuves justifiant sa décision d'émettre un nulla osta négatif. Cette nécessité peut justifier la conservation des certificats de bonnes vie et mœurs jusqu'au terme du délai établi pour la contestation d'une décision défavorable. La personne concernée ne devrait toutefois pas hésiter à fournir un certificat de bonnes vie et mœurs mis à jour, qui sera conservé aux côtés de l'ancien, lequel sera définitivement supprimé au terme du délai susmentionné.

En dernier lieu, le CEPD tient à souligner que la procédure spéciale mise en place pour la restitution de l'extrait original du casier judiciaire ne constitue pas un moyen pour la personne concernée d'exercer son droit d'accès ou de rectification. Par ailleurs, une copie du casier judiciaire est conservée dans ARDOS, alors que le formulaire «Demande de restitution de l'extrait de casier judiciaire» laisse à penser le contraire. Cette procédure ne respecte pas le principe de loyauté du traitement; la procédure n'est pas transparente et la «Demande de restitution de l'extrait de casier judiciaire» devrait par conséquent être modifiée afin d'éviter toute confusion.

3.9. Information de la personne concernée

En vertu des articles 11 et 12 du règlement (CE) n° 45/2001, les responsables de la collecte des données à caractère personnel sont tenus d'informer les personnes concernées que leurs données sont collectées et traitées. Les personnes concernées ont également le droit d'être informées, entre autres, des finalités du traitement, des destinataires des données et de leurs droits spécifiques en tant que personnes concernées. L'article 12 s'applique du fait que les données n'ont pas été collectées auprès de la personne concernée, mais sont fournies au Service de sécurité par les services de recrutement.

La déclaration de confidentialité sera affichée sur l'intranet. Le CEPD juge cette méthode appropriée pour fournir des informations, mais suggère qu'une copie de la déclaration soit transmise à chaque personne concernée, afin que le CCR puisse s'assurer que chacune d'entre elles (même les candidats non recrutés) soit informée de son existence, par exemple si elle souhaite savoir comment exercer ses droits et comment le traitement de données se déroule.

Au terme de l'analyse du contenu des informations mentionnées dans la déclaration de confidentialité, le CEPD estime que la majorité des informations requises à l'article 12 du règlement y figurent. Il estime toutefois que plusieurs modifications contribueraient à garantir le plein respect de l'article 12, en particulier:

i) la finalité de la «règle relative à la présence sur le site pendant 72 mois» devrait être ajoutée;

ii) le CCR devrait préciser quelles sont les données couvertes dans la phrase «de même que toute autre information relative à la sécurité collectée au cours de l'existence d'une relation contractuelle avec la personne concernée»;
iii) pour garantir une transparence totale et un traitement loyal, il conviendrait d'informer les personnes concernées de l'origine des données;
iv) il conviendrait d'indiquer que la déclaration «nulla osta» est transférée aux services de recrutement;
v) après établissement d'une base juridique pour la procédure nulla osta, il conviendrait de mentionner cette base juridique dans la déclaration de confidentialité;
vi) les termes «attestation de sécurité» devraient être évités étant donné que le Service de sécurité du CCR a clairement indiqué que le nulla
osta et l'«attestation de sécurité» n'ont aucun point commun (voir le vocabulaire utilisé dans la déclaration de confidentialité et par les unités de recrutement).

3.10. Mesures de sécurité

xx

4. Conclusion:

Le traitement décrit semble en violation des dispositions du règlement (CE) n° 45/2001 à moins qu'une base juridique claire soit identifiée, produite ou établie. Le CEPD recommande par ailleurs qu'aux fins du respect du règlement, les considérations susmentionnées soient pleinement prises en considération également dans d'autres domaines, à savoir:

- une analyse au cas par cas du contenu du casier judiciaire national ou du certificat de bonnes vie et mœurs devrait être réalisée afin de collecter uniquement des données pertinentes au regard des exigences prévues par le statut des fonctionnaires;
- la nécessité de chaque catégorie de données collectées par le Service de sécurité dans la base de données ARDOS aux fins de l'émission du nulla osta doit être démontrée par le CCR;
- un document formel décrivant et définissant la procédure en place devrait être adopté afin de garantir le respect du principe de qualité des données en vertu de l'article 4, paragraphe 1, point c);
- le CCR devrait mettre en place un système garantissant la suppression des informations sur les délits pour lesquels il y a prescription. Le droit d'accès et de rectification pourrait être utile à cet égard, ou encore, par exemple, l'adoption d'un «formulaire standard» indiquant l'aptitude de la personne à exécuter les tâches qui lui incombent, qui serait conservé dans le dossier, tandis que l'extrait de casier judiciaire serait restitué à la personne;
- la durée de conservation des données prévue par le Centre devrait être introduite au plus tôt conformément à l'article 4, paragraphe 2, point e), du règlement;
- seules les données nécessaires aux fins de la gestion de la règle des 72 mois devraient être conservées conformément à l'article 4, paragraphe 1, point e);
- toutes les informations historiques devraient être conservées sous une forme anonyme ou supprimées de la base de données, conformément à l'article 4, paragraphe 1, point e), du règlement;
- le CCR devrait établir un système destiné à garantir l'application effective du contenu des droits d'accès et de rectification en ce qui concerne le certificat de bonnes vie et mœurs et l'extrait du casier judiciaire;

- la «demande de restitution de l'extrait de casier judiciaire» devrait être modifiée suivant la recommandation formulée au point 3.8;
- plusieurs modifications devraient être apportées à la déclaration de confidentialité afin de garantir le plein respect de l'article 12, tel que décrit dans le présent avis.

Fait à Bruxelles, le 15 décembre 2008

(**signé**)

Peter HUSTINX
Contrôleur européen de la protection des données