Avis sur une notification en vue d'un contrôle préalable reçue du déléguéà la protection des données (DPD) de la Commission européenne ("Commission") à propos de la gestion de la sécurité au travail au sein de l'Institut pour la santé et la protection des consommateurs[1] ("Institut") du Centre commun de recherche ("CCR") à Ispra

Bruxelles, le 20 mai 2009 (dossier 2008-541)

1. La procédure

Le 26 août 2008, le DPD de la Commission a envoyé par courrier électronique au Contrôleur européen de la protection des données ("**CEPD**") sa notification concernant la gestion de la sécurité au travail au sein de l'Institut pour la santé et la protection des consommateurs du CCR à Ispra, accompagnée de ses annexes ("**Notification**").

Le 25 septembre 2008, le CEPD a envoyé au DPD de la Commission une note résumant sa perception des faits et précisant les questions encore en suspens. Jusqu'au 16 octobre 2008, date à laquelle l'Institut a transmis une confirmation écrite des faits et a apporté une réponse à ces questions, le dossier est demeuré en suspens. Le CEPD a transmis à l'Institut son projet d'avis pour commentaire le 20 novembre 2008. Le 11 mai 2009, le CEPD a envoyé au DPD un rappel concernant les commentaires, lui demandant de répondre avant le 18 mai 2009. Aucune réponse ne lui étant parvenue, le CEPD a rendu son avis le 20 mai 2009.

2. Les faits

2.1. Portée de la notification et vue d'ensemble des opérations de traitement. La notification et l'avis du CEPD concernent un fichier spécialisé dénommé: "Gestion de la sécurité au travail" utilisé par l'Institut. Ce fichier est tenu par "le responsable du Service de prévention et de protection" ("**RSPP**")[2] de l'Institut. Les données à caractère personnel susceptibles d'avoir une incidence sur la sécurité au travail sont recueillies et conservées dans ce fichier, puis consultées si nécessaire. L'objectif du traitement est de satisfaire aux obligations de l'employeur en termes de sécurité au travail dans le cadre des lois italiennes: le traitement concerne l'ensemble du personnel de l'Institut.

Des traitements distincts, mais liés, ont été analysés dans les avis du CEPD qui suivent:

- Avis du 6 février 2008 sur une notification en vue d'un contrôle préalable à propos du dossier "Système de gestion dosimétrique à la DG CCR d'Ispra" (Dossier 2007-505);

[1] L'Institut pour la santé et la protection des consommateurs (IHCP) fait partie de la Direction générale du Centre commun de recherche (DG CCR) de la Commission européenne. Sa mission est de protéger les intérêts et la santé des consommateurs dans le cadre de la législation communautaire relative aux produits chimiques, aux denrées alimentaires et aux produits de consommation, en apportant un soutien scientifique et technique, notamment au moyen d'une évaluation des risques et bénéfices et d'une analyse de la traçabilité.

[2] L'Institut a expliqué que le RSPP n'est composé à l'heure actuelle que d'une personne, qui dépend hiérarchiquement de l'unité de soutien à la gestion mais est placée sous l'autorité directe du directeur de l'Institut.

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

- Avis du 6 février 2008 sur une notification en vue d'un contrôle préalable concernant le traitement des dossiers médicaux individuels au Centre commun de recherche à Ispra et à Séville (Dossier 2007-329);
- Avis du 23 janvier 2008 sur une notification en vue d'un contrôle préalable à propos de la médecine du travail à la DG CCR (Dossier 2007-504);
- Avis du 17 janvier 2008 sur une notification en vue d'un contrôle préalable concernant la gestion sous PowerLab) de l'environnement des laboratoires cliniques et toxicologiques à la DG CCR (Dossier 2007-649); et
- Avis du 25 janvier 2008 sur les premiers secours, les accidents du travail et autres examens médicaux au CCR (Centre commun de recherche) d'Ispra (Dossier 2007-372).

2.2. Déclaration de confidentialité et description des traitements. La notification précise que les informations relatives à la sécurité au travail sont disponibles sur le réseau Intranet de l'Institut, à l'adresse: http://ihcp-agora.jrc.it. Ces informations comprennent des documents et des procédures destinées à empêcher les risques dits "résiduels". En outre, une déclaration de confidentialité est également disponible sur ce même site Web. Ce document, intitulé "Déclaration de confidentialité relative à la gestion de la sécurité au travail au sein de l'Institut IHCP-CCR d'Ispra", présente un résumé des aspects les plus significatifs des opérations de traitement:

1. Description

Le Responsable du service de prévention et de protection (RSPP) de l'Institut pour la santé et la protection des consommateurs (IHCP) du Centre commun de recherche (CCR) est chargé de collecter et de consulter des données à caractère personnel dans le but de mettre à jour et de vérifier l'aptitude au travail de chacun des membres du personnel de l'Institut CCR au regard de la sécurité au travail. Les données à caractère personnel sont recueillies puis traitées dans le but détaillé ci-après au point 2.

Ce traitement des données à caractère personnel relève de la responsabilité du Directeur de l'Institut pour la santé et la protection des consommateurs (IHCP) du CCR.

Le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données s'applique à la collecte et au traitement ultérieur des données à caractère personnel susmentionnés

2. Quelles informations à caractère personnel collectons-nous? Sur quelle base juridique? Dans quel but et avec quels moyens techniques?

Données d'identification

Les données à caractère personnel collectées puis traitées sont: le nom, le prénom, la date de naissance, la nationalité, le sexe, le numéro de contribuable, la direction/l'institut/l'unité, l'employeur/le supérieur hiérarchique, la date de début de contrat, la description du poste, l'action/activité scientifique/technique/administrative, l'identifiant de connexion à la Commission, le numéro personnel, le bâtiment/l'emplacement du bureau/laboratoire, le type de contrat, le régime de l'employé et de l'employeur.

Parmi les autres données figurent les données relatives à la formation provenant de SYSLOG Formation, les données relatives à la sécurité au travail telles que les

expositions à des risques professionnels, les données relatives aux accidents du travail, les données relatives à l'aptitude médicale et professionnelle.

Base juridique

- Directive 89/391/CEE
- Decreto Legislativo n° 81/2008 (remplaçant la Loi italienne 626/94 sur la sécurité au travail)

Finalité

La finalité de la mise à jour et de la vérification des données des membres du personnel est de satisfaire aux obligations de l'employeur en termes de sécurité au travail.

Informations techniques

Les données de l'utilisateur sont recueillies par le biais de formulaires/ou fiches papier ou de supports électroniques.

3. Qui a accès à vos informations et à qui sont-elles divulguées?

L'accès à toutes les données à caractère personnel n'est accordé qu'à certains types d'utilisateurs bien définis qui doivent saisir un identifiant et un mot de passe. Ces utilisateurs comprennent généralement le Directeur, le chef de l'unité, le responsable de la sécurité et le membre du personnel. Aucune donnée à caractère personnel ne peut être transmise à des tierces parties, étrangères aux destinataires et au cadre légal mentionnés.

4. Comment protégeons-nous et sauvegardons-nous vos informations?

Les données à caractère personnel recueillies sont conservées sur les serveurs du CCR conformément à la Décision C (2006) 3602 de la Commission du 17/08/2006 "relative à la sécurité des systèmes d'information utilisés par les services de la Commission européenne", qui définit les mesures de sécurité en vigueur pour les ystèmes informatiques. L'Annexe I définit les exigences en matière de sécurité des systèmes d'information de la CE. L'Annexe II définit les différents acteurs et leurs responsabilités. L'Annexe III définit les règles applicables par les utilisateurs.

5. Comment pouvez-vous vérifier, modifier, verrouiller ou supprimer les informations qui vous concernent?

Au cas où vous souhaiteriez vérifier les données à caractère personnel vous concernant qui sont conservées par le responsable du traitement, les modifier, les corriger, les verrouiller ou encore les supprimer, veuillez adresser un courrier électronique à l'adresse électronique spécifique mentionnée ci-après, sous "Coordonnées", en précisant votre demande de manière explicite.

6. Combien de temps conservons-nous vos données?

Les données à caractère personnel sont conservées aussi longtemps que la personne employée est sous contrat.

7. Coordonnées

Pour toute question concernant le traitement de vos données à caractère personnel, veuillez contacter le responsable du traitement à l'adresse suivante: jrc-ihcp-dir-sec@ec.europa.eu

Pour toute question relative à la protection des données à caractère personnel, vous pouvez contacter:

- le Coordinateur de la protection des données de la DG CCR: jrc-data-protection-coordinator@ec.europa.eu
- le Délégué à la protection des données de la Commission: data-protection-officer@ec.europa.eu

8. Recours

En cas de litige, vous pouvez adresser votre réclamation au:
- Contrôleur européen à la protection des données : edps@edps.europa.eu

2.3. Données recueillies dans le fichier. La notification explique que trois types de données relatives au personnel sont recueillies dans le fichier:

Tout d'abord, les données à caractère personnel et administratif sont importées pour chacun des membres du personnel selon leur disponibilité dans une base de données appelée "DATAPOOL":

- nom;
- date de naissance;
- nationalité;
- sexe;
- numéro de contribuable;
- direction/institut/unité;
- employeur/supérieur hiérarchique;
- date de début du contrat;
- description du poste;
- action/activité scientifique/technique/administrative;
- identifiant de connexion à la Commission;
- numéro personnel;
- bâtiment/emplacement du bureau/laboratoire;
- type de contrat;
- dates/signatures de l'employé et de l'employeur sur les formulaires/fiches/documents.

Ensuite, pour les données relatives à la formation, un lien est établi à partir d'une base de données appelée "SYSLOG Formation":

- données provenant de la carte de formation (cours de formation requis) et
- du passeport de formation (cours de formation suivis)
- en matière de cours de langues;
- de cours à contenu général;
- de cours obligatoires de formation à la sécurité; et
- d'autres formations issues de la base de données d'apprentissage en ligne.

Troisièmement, les données relatives à la sécurité au travail sont également introduites dans le fichier. Parmi ces dernières figurent:

- les expositions aux risques professionnels;
- les données relatives aux accidents du travail, y compris la date de l'accident, le lieu de l'accident, l'identité des témoins, les détails de l'accident, la période d'absence, les lésions subies;
- l'éventuelle exposition à certaines substances/radiations; durée d'exposition/opération, nombre d'opérations/mois, quantité/opération, méthode d'exposition, substance utilisée;

- équipements de protection ou mesures de sécurité obligatoires;
- aptitude physique/sensorielle; Cat. A, Cat. B, aptitude médicale/professionnelle.

Les données relevant de cette troisième catégorie proviennent des sources suivantes:

- Liste de contrôle administrative des nouveaux arrivants (direction générale du personnel et de l'administration) (documentant les procédures administratives);
- Laboratoire et sécurité - nouveaux arrivants (documentant les éléments relatifs à la sécurité et au laboratoire);
- Données relatives aux accidents du travail (*Rapporto d'Infortunio*);
- Liste de contrôle des départs;
- Fiche d'évaluation des risques (*Scheda Blu Inglese*);
- Fiche relative aux risques professionnels V.1;
- Fiche technique sur l'exposition aux substances carcinogènes (*Registro Esposizione*);
- Fiche technique sur l'exposition aux nanoparticules (*Modulo Esposti Nanoparticelle*);
- Données relatives à l'aptitude médicale et professionnelle.

3. Aspects juridiques

3.1. Contrôle préalable

Portée de la notification. Comme évoqué dans la section 2.1 ci-avant, la notification et le présent avis concerne un fichier spécialisé dénommé: "Gestion de la sécurité au travail" utilisé par l'Institut.

Applicabilité du règlement. Le règlement (CE) n° 45/2001 (le "règlement") s'applique "au traitement de données à caractère personnel, automatisé en tout ou partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier" de même qu'au traitement "par toutes les institutions et tous les organes communautaires, dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou partie du champ d'application du droit communautaire" (article 3).

Tous les éléments qui entraînent l'application de ce règlement sont réunis ici:

Premièrement, la procédure de sélection et de recrutement notifiée comporte la collecte et le traitement ultérieur de données à caractère personnel, définis à l'article 2, point a), du règlement.

Deuxièmement, les données à caractère personnel collectées font l'objet d'un traitement automatisé de même que d'un traitement manuel, et figurant dans un fichier (article 3, paragraphe 2, du règlement).

Troisièmement, le traitement est effectué par l'Institut, qui est un organe communautaire relevant du champ d'application du droit communautaire (article 3, paragraphe 1, du règlement).

Sur la base de ce qui précède, le règlement est applicable.

Motifs justifiant un contrôle préalable. L'article 27, paragraphe 1, du règlement soumet à un contrôle préalable du CEPD tous les "traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités".

L'article 27, paragraphe 2, contient une liste des traitements susceptibles de présenter de tels risques. Cette liste comporte expressément (au point a) les données relatives à la santé. Partant, le traitement notifié doit faire l'objet d'un contrôle préalable par le CEPD.

Notification et date limite de remise de l'avis du CEPD. La notification a été reçue le 26 août 2008. Conformément à l'article 27, paragraphe 4, du règlement, le présent avis doit être rendu dans les deux mois. La procédure a été suspendue pendant 6 mois et 24 jours au total. Dès lors, l'avis doit être rendu le 21 mai 2009 au plus tard (27 octobre 2008 + suspension pour le reste du mois d'août [5 jours] + 21 jours + 5 mois et 28 jours pour commentaire).

Contrôle préalable a posteriori ("ex-post"). Les traitements ont débuté préalablement à la notification du CEPD. Le contrôle préalable étant conçu pour les situations susceptibles de présenter des risques, l'avis du CEPD doit normalement être sollicité et rendu avant que ne commence le traitement. Or, ce traitement a été notifié alors qu'il était déjà appliqué depuis un certain temps; le contrôle préalable doit donc être réalisé ex-post. Cela ne constitue pas un problème majeur en l'espèce du fait que toutes les recommandations du CEPD ont été prises en compte.

3.2. Licéité des traitements

L'article 5, point a), du règlement dispose que le traitement des données à caractère personnel peut être effectué s'il "est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités […] ou d'autres actes législatifs adoptés sur la base de ces traités".

La première question soulevée par l'article 5, point a), est de déterminer s'il existe une base juridique spécifique au traitement, à savoir une disposition d'un traité ou un autre acte législatif adopté sur la base de ces traités. La deuxième est de déterminer si le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public. Dans le cas qui nous occupe, ce second élément requiert la prise en compte du considérant 27 du règlement, qui précise que "le traitement de données à caractère personnel effectué pour l'exécution de missions d'intérêt public par les institutions et les organes communautaires comprend le traitement de données à caractère personnel nécessaire pour la gestion et le fonctionnement de ces institutions et organes". Par conséquent, ce second aspect consiste, en l'espèce, à déterminer si le traitement est nécessaire et proportionné au regard de la gestion et le fonctionnement de l'Institut.

S'agissant de la première question, la gestion de la sécurité au travail au sein de l'Institut se fonde sur les dispositions de la directive 89/391/CEE et sur le *Decreto Legislativo n° 81/2008* (remplaçant la loi italienne 626/94 sur la sécurité au travail).

Par conséquent, les actes législatifs spécifiques adoptés sur la base des traités autorisent les traitements notifiés. S'agissant du décret italien, il s'applique à l'Institut d'Ispra car il n'interfère aucunement avec les devoirs et privilèges énoncés dans le droit communautaire, comme stipulé dans la jurisprudence de la CJE[3]. En ce qui concerne la seconde question, le CEPD est également convaincu que tel est bien le cas et ne conteste pas la nécessité ni le caractère proportionné des traitements pour la gestion et le fonctionnement de l'Institut.

[3] Voir l'ordonnance rendue dans l'affaire 1/88 SA Générale de Banque/Commission, Recueil 1989, p. 857, point 9; l'affaire C-2/88 Imm. Zwartfeld et autres, Recueil 1990, p. I-3365, points 19 et 20, ainsi que l'arrêt rendu dans l'affaire T-80/91 Campogrande/Commission, Recueil 1992, p. II-2459, point 42.

En conclusion, le CEPD considère que les traitements notifiés sont licites dans la mesure où les recommandations formulées dans le présent avis sont respectées.

3.3. Traitement de catégories particulières de données

Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques et l'appartenance syndicale, ainsi que le traitement des données relatives à la santé ou à la vie sexuelle, sont interdits, sauf exception prévue à l'article 10, paragraphes 2 à 4, du règlement.

Cette interdiction est entre autre levée lorsque le traitement est nécessaire afin de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par les traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités ou dans la mesure où il est accepté par le contrôleur européen de la protection des données, moyennant des garanties adéquates (article 10, paragraphe 2, point b), du règlement).

Dans l'affaire qui nous occupe, le fichier, en raison de sa finalité spécifique, comporte un nombre significatif de données relatives à la santé. Cela est "nécessaire afin de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail" et autorisé par le décret italien susmentionné dans la partie consacrée à la base juridique du traitement. Le traitement des données relatives à la santé est donc licite en vertu de l'article 10, paragraphe 2, point b) du règlement.

3.4. Qualité des données

Adéquation, pertinence et proportionnalité. Conformément à l'article 4, paragraphe 1, point c) du règlement, les données à caractère personnel doivent être "adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement".

Sur la base des informations qui lui ont été transmises, le CEPD ne conteste pas l'adéquation, la pertinence ni la proportionnalité des données collectées dans le fichier.

À une exception toutefois: le CEPD recommande à l'Institut de reconsidérer la nécessité, pour le responsable de la sécurité, d'avoir un accès direct à l'ensemble des informations relatives à la formation énumérées ci-dessus au point 2.3, y compris aux informations sur les cours de langues et cours à contenu général, ainsi qu'aux "autres formations issues de la base de données d'apprentissage en ligne". Ces informations semblent en effet n'avoir aucun lien avec la sécurité au travail.

Loyauté et licéité. L'article 4, paragraphe 1, point a), du règlement requiert que les données soient traitées loyalement et licitement. La question de la licéité a été examinée ci-dessus (voir point 3.2). La question de la loyauté est étroitement liée à la nature des informations fournies aux personnes concernées (voir point 3.8 ci-dessous).

Exactitude. Conformément à l'article 4, paragraphe 1, point d), du règlement, les données à caractère personnel doivent être "exactes et, si nécessaire, mises à jour" et "toutes les mesures raisonnables sont prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement soient effacées ou rectifiées".

Sur la base des informations qui lui ont été fournies, le CEPD ne conteste pas l'exactitude des données collectées dans le cadre des procédures de sélection et de recrutement.

3.5. Conservation des données. Le principe général du règlement est que 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 (article 4, paragraphe 1, point e), du règlement).

Sur la base des informations qui lui ont été fournies, le CEPD ne conteste pas la nécessité de conserver les données collectées dans le fichier pendant la durée du contrat des membres du personnel de l'Institut.

3.6. Destinataires et transferts de données. Le CEPD se félicite de ce que l'accès au fichier soit limité sur la base du principe du besoin de connaître.

Le CEPD attire en outre l'attention de l'Institut sur l'obligation qui lui incombe, dans le cas où une tierce partie demande un transfert de données imprévu, d'autoriser ce transfert pour autant que i) le consentement de la personne concernée ait été exprimé sans équivoque et en connaissance de cause (c'est-à-dire de manière explicite en ce qui concerne les données sensibles) ou que ii) le règlement l'autorise expressément. Le CEPD souligne également que conformément à l'article 7, paragraphe 3, les destinataires pourront uniquement traiter les données à caractère personnel aux fins qui ont motivé leur transmission.

En cas de doute, le CEPD recommande au responsable du traitement de consulter le DPD de l'Institut avant d'effectuer le transfert de données demandé.

3.7. Droit d'accès et de rectification. L'article 13 du règlement accorde aux personnes concernées le droit d'accéder aux données à caractère personnel les concernant. L'article 14 prévoit un droit de rectification des données à caractère personnel.

À cet égard, le CEPD recommande qu'une série minimale de garanties soit instaurée et communiquée dans la déclaration de confidentialité afin de faire en sorte que toute demande d'accès soit traitée en temps utile et sans restriction. En cas de doute quant à l'octroi de l'accès aux données, le responsable du traitement devrait consulter le DPD de l'Institut.

3.8. Informations transmises aux personnes concernées. Les articles 11 et 12 du règlement requièrent la communication de certaines informations aux personnes concernées afin de garantir la transparence du traitement des données à caractère personnel. L'article 11 s'applique aux données collectées auprès de la personne concernée, ce qui est le cas, par exemple, s'agissant des données contenues dans les documents que le responsable du traitement a demandé aux personnes concernées de remplir. L'article 12, quant à lui, s'applique lorsque les données n'ont pas été collectées auprès de la personne concernée. C'est le cas, entre autres, des données contenues dans les documents qui n'ont pas été remplis par la personne concernée, à la demande du responsable du traitement, comme par exemple les données relatives à la formation provenant de la base de données SYSLOG Formation.

Le CEPD se félicite du fait que la déclaration de confidentialité apparaît sur le site Intranet de l'Institut, avec les informations pertinentes consacrées à la "sécurité au travail". S'agissant du contenu de la déclaration de confidentialité, le CEPD formule les recommandations additionnelles suivantes:

Le point 2 ("Quelles informations à caractère personnel collectons-nous? Sur quelle base juridique? Dans quel but et avec quels moyens techniques?") devrait être rédigé plus clairement. En premier lieu, concernant les données collectées, alors que les "données d'identification" sont abordées de manière très détaillée, aucun détail similaire n'est apporté s'agissant des données relatives à la sécurité au travail. Le CEPD recommande que les catégories de données collectées soient décrites dans la déclaration de confidentialité, de manière au moins aussi détaillée qu'au point 2.3 du présent avis. Ensuite, dans la rubrique "Informations techniques", il conviendrait de clarifier la phrase suivante: "*Les données de l'utilisateur sont recueillies par le biais de formulaires ou fiches papier ou de supports*

électroniques". Encore une fois, il serait approprié de présenter le même niveau de détail qu'au point 2.3 du présent avis ou encore de rédiger un résumé.

3.9. Mesures de sécurité. Conformément à l'article 22 du règlement, le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à caractère personnel à protéger. Ces mesures sont prises notamment afin d'empêcher toute diffusion ou tout accès non autorisés, toute destruction accidentelle ou illicite, toute perte accidentelle ou toute altération, ainsi que toute autre forme de traitement illicite.

Le CEPD n'a découvert aucun élément susceptible de susciter le moindre doute quant à l'adéquation des mesures de sécurité mises en œuvre pour les données traitées dans le cadre du fichier "Sécurité au travail" de l'Institut. Quoi qu'il en soit, le CEPD attire l'attention sur le fait que l'Institut doit garantir que les données à caractère personnel contenues dans le fichier ne sont pas accessibles par des tiers et ne doivent pas être divulguées à des tiers, à l'exception des personnes mentionnées dans le présent avis.

Conclusion

Rien ne permet de conclure à un manquement aux dispositions du règlement, pour autant que les considérations figurant aux points 3.2 à 3.9 du présent avis soient pleinement prises en compte. Les recommandations du CEPD sont les suivantes:

- Qualité et proportionnalité des données:
  L'Institut devrait reconsidérer la nécessité, pour le responsable de la sécurité, d'avoir un accès direct aux données générales sur la formation provenant du système SYSLOG Formation, aux données relatives à la formation aux langues et à l'apprentissage en ligne, ainsi qu'aux informations sur la formation qui sont directement pertinentes pour la sécurité au travail.

- Droit d'accès:
  L'Institut devant instaurer une série minimale de garanties pour faire en sorte que les demandes d'accès soient traitées en temps utile et sans restriction.

- Informations fournies aux personnes concernées:
  les informations concernant certains éléments relevant des articles 11 et 12 du règlement devront être rédigées de manière plus précise.

Fait à Bruxelles, le 20 mai 2009

(signé)

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données