

Avis sur la notification en vue d'un contrôle préalable adressée par le délégué à la protection des données de la Commission européenne (« Commission ») à propos de la procédure facultative de «Leadership Feedback» mise en place par l'École européenne d'administration (« EAS ») en rapport avec ses cours de management.

Bruxelles, le 15 décembre 2008 (Dossier 2008-527)

1. Procédure

Le 2 septembre 2008, le délégué à la protection des données («**DPD**») de la Commission européenne («**Commission**») a remis au contrôleur européen de la protection des données («**CEPD**») une copie papier d'une notification, avec annexes, à propos d'une procédure facultative de «Leadership Feedback» (retour d'information sur les compétences de direction) mise en place par l'École européenne d'administration («**EAS**») en rapport avec ses cours de management (la «**notification**»).

Le 24 septembre 2008, le CEPD a envoyé au DPD de la Commission un résumé des faits tels qu'il les comprenait, ainsi que ses questions en suspens. L'EAS a répondu le 28 octobre 2008.

Le 4 décembre 2008, le CEPD a envoyé son projet d'avis à l'EAS afin de lui permettre d'apporter ses commentaires. La Commission a répondu le 12 décembre 2008.

2. Les faits

2.1. Champ d'application de la notification et résumé de la procédure de «Leadership Feedback». La notification concerne une procédure facultative de «Leadership Feedback» mise en place par l'EAS en rapport avec ses cours de management.

Dans le cadre de son mandat, l'EAS organise des cours de management pour les fonctionnaires de la Commission et d'autres institutions et organes européens. Pour chaque cours de management, l'EAS offre la possibilité aux participants de recevoir l'avis anonyme des autres participants sur leurs compétences de management. La participation à l'exercice est anonyme et entièrement volontaire. Les informations ne sont pas utilisées par l'EAS ou la Commission à leurs propres fins et elles sont traitées dans le seul intérêt des participants.

L'EAS a externalisé l'organisation de cours de management à une société privée établie dans un État membre de l'Union européenne. À son tour, cette société a externalisé l'organisation de la procédure de retour d'information sur les compétences de direction à une autre société privée, également établie dans un État membre de l'Union européenne. L'EAS, quant à elle, n'a pas accès aux données traitées lors de la procédure. La société extérieure chargée du traitement des données organise et gère la procédure de retour d'information. En particulier, elle met à la disposition des participants un outil en ligne sécurisé pour collecter les retours

d'information, les rassembler sous forme de rapports (tout en garantissant l'anonymat des personnes qui donnent leur avis) et fournit à chaque participant un rapport sur le retour d'information du groupe concernant ses propres compétences de management. S'ils le souhaitent, les participants peuvent aussi remplir un questionnaire d'évaluation de leurs propres compétences de management et autoriser leurs formateurs à consulter les retours d'information.

2.2. Déclaration de confidentialité et description du traitement. Les participants aux cours recevront un dossier d'information imprimé qui contiendra également une description de la procédure de retour d'information. Cette documentation comprendra un lien vers la déclaration spécifique relative à la protection des données reprise ci-dessous, qui est disponible sur le site Internet de l'EAS. Dans ce document, intitulé «Privacy statement in the framework of training activities organised by the European Administrative School (EAS) and the use of leadership feedback» (*Déclaration de confidentialité dans le cadre des activités de formation organisées par l'École européenne d'administration (EAS) et l'utilisation du retour d'information sur les compétences de direction*), l'EAS résume comme suit les principaux aspects du traitement:

La présente déclaration explique comment sont traitées toutes les données à caractère personnel fournies dans le cadre du 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). Elle est remise à chaque membre du personnel des institutions, agences et organes de l'Union européenne qui participe aux cours de formation organisés par l'EAS et qui est volontaire pour demander l'avis de ses collègues sur ses styles de management et de direction. Elle s'applique également aux membres du personnel qui remettent un tel avis. Conformément aux articles 11 et 12 dudit règlement, l'EPSO et l'EAS fournissent les informations suivantes aux personnes qui participent à cet exercice:

Identité du responsable du traitement¹: M. Nicholas David BEARFIELD, Directeur de l'EPSO.

Finalité(s) du traitement: permettre aux participants aux cours de formation de l'EAS d'obtenir un retour d'information anonyme sur leur style de management et de direction de la part de leurs collègues afin de les aider à améliorer leurs compétences de management et de direction. Ce type d'outil est fréquemment utilisé par les prestataires de formation du monde entier dans les cours de management et de direction. Les données ne seront pas utilisées dans le cadre d'une procédure d'évaluation (appréciation), sous quelque forme que ce soit, des personnes impliquées.

Données concernées: les données concernent les membres du personnel des institutions, agences et organes de l'Union européenne qui participent aux cours de formation organisés par l'EAS. Les données demandées aux membres du personnel qui participent aux cours de formation et à leurs collègues, à leur sujet, sont collectées sur la base exclusive du volontariat.

Les participants aux cours ont la possibilité d'utiliser un outil de retour d'information qui prend la forme d'une auto-évaluation de leurs compétences et d'une appréciation par les collègues qu'ils choisissent de consulter. La participation de la personne concernée et de ses collègues à cet exercice est entièrement volontaire et les participants sont libres

¹ En raison du rattachement administratif de l'EAS à l'EPSO pour les trois premières années de son existence, le Directeur de l'EPSO est également responsable du contrôle.

de choisir les personnes qu'ils souhaitent inviter à participer à l'exercice. Il appartient aux personnes sollicitées de décider si elles participent. L'EAS propose cet outil pour aider les participants à connaître leurs compétences professionnelles et à améliorer leur propre développement personnel dans un environnement professionnel. Les participants prennent part à l'exercice.

Les données à caractère personnel concernées sont de quatre types.

Tout d'abord, le participant au cours reçoit des informations exhaustives sur l'exercice de retour d'information et il est invité à décider s'il souhaite y participer. Si tel est le cas, il doit fournir des informations (nom et adresse électronique) sur lui-même et les collègues auxquels il sera demandé de fournir un avis. Actuellement, ces informations sont communiquées à Innotiimi (Finlande), l'un des membres du consortium auquel a été confiée la tâche de fournir des programmes de formation en management. Tout changement ou tout ajout afférent à la société qui fournit ce service sera notifié au DPD. Innotiimi transmet ces données à son sous-traitant, Feedback OY, en charge du site Internet sur lequel se déroule ensuite l'exercice de retour d'information. Ces données servent simplement à identifier le participant au cours et les collègues qui prennent part à l'exercice, ainsi qu'à permettre au sous-traitant de les contacter. À ce stade, le participant au cours reçoit des informations exhaustives sur l'exercice ainsi que sur la nature et les étapes du traitement des données. Le participant reçoit une fiche d'information qui reprend les mêmes informations et doit être remise aux collègues qui acceptent de participer à l'exercice. Il est également demandé au participant de préciser s'il préfère recevoir le rapport final de l'exercice de façon individuelle ou si celui-ci peut être communiqué au formateur du cours de formation. Le participant n'est pas tenu d'accepter de communiquer le rapport final.

Le second traitement des données intervient lorsque le participant au cours fournit sa contribution à l'exercice. Le participant communique ces données en remplissant un questionnaire en ligne sur ses compétences de management. Les données collectées sont des données numériques, c'est-à-dire qu'il s'agit de répondre par oui ou non à une série de questions, et des données textuelles lorsque le participant peut compléter les données numériques par des commentaires personnels. Le participant n'est pas tenu de fournir ces commentaires.

Le troisième traitement des données intervient lorsque les collègues des participants au cours apportent leur contribution à l'exercice en complétant un questionnaire en ligne concernant leur avis sur les compétences de management du participant. Les données collectées sont des données numériques, c'est-à-dire qu'il s'agit de répondre par oui ou non à une série de questions, et des données textuelles lorsque la personne concernée peut compléter les données numériques par des commentaires personnels.

Le quatrième traitement des données intervient lorsque Feedback OY traite les données fournies par le participant et ses collègues. Les données numériques des deux sources sont rassemblées dans un rapport unique.² Ce rapport comprend également une fusion des éventuels commentaires écrits. Le rapport est ensuite envoyé au participant à l'adresse électronique qu'il a communiquée. Le rapport sera également transmis au formateur qui dispense le cours, mais uniquement si le participant a donné son accord.

² L'EAS a expliqué au CEPD que cette «fusion» était générée automatiquement. Le logiciel formate automatiquement les contributions individuelles en tables de données fusionnées et chapitres du rapport final. L'EAS a également expliqué que Feedback OY doit néanmoins pouvoir accéder aux données individuelles afin de supprimer des données à la demande de la personne concernée. Ni Innotiimi, ni l'EAS, n'ont accès aux données.

Cela permet au formateur de s'entretenir seul à seul avec le participant afin de lui donner son avis sur les résultats du rapport.

Nature des données traitées:

- Données à caractère personnel permettant l'identification des membres du personnel concernés (nom, prénom, adresse électronique);
- Informations fournies par le participant au cours sur sa perception de ses propres compétences de management et de direction, dans des domaines tels que la gestion des performances, du changement, des problèmes et des personnes.
- Informations fournies par des collègues sur leur perception des compétences de management et direction du participant, dans des domaines tels que la gestion des performances, du changement, des problèmes et des personnes. Ces informations sont rendues anonymes et rassemblées dans un rapport de retour d'information.

Base légale:

- régime applicable aux fonctionnaires des Communautés européennes, tel que fixé par le règlement (CEE, Euratom, CECA) n° 259/68 du Conseil, modifié en dernier lieu par le règlement (CE, CECA, Euratom) n° 23/2005 du Conseil, et en particulier les articles 45b du statut des fonctionnaires et 7, paragraphe 2, point c), de l'Annexe III du statut des fonctionnaires;
- décision n° 2006/620/CE du Parlement européen, du Conseil, de la Commission européenne, de la Cour de justice des Communautés européennes, de la Cour des comptes, du Comité économique et social européen, du Comité des Régions et du Médiateur européen du 25 juillet 2002 ayant entraîné la création de l'Office européen de sélection du personnel;
- décision n° 2005/118/CE du Parlement européen, du Conseil, de la Commission européenne, de la Cour de justice des Communautés européennes, de la Cour des comptes, du Comité économique et social européen, du Comité des Régions et du Médiateur européen du 26 janvier 2005 ayant entraîné la création de l'Office européen de sélection du personnel;
- décision n° 2005/119/CE des Secrétaires généraux du Parlement européen, du Conseil, de la Commission européenne, de la Cour de justice des Communautés européennes, de la Cour des comptes, du Comité économique et social européen, du Comité des Régions et du Médiateur européen du 26 janvier 2005 concernant l'organisation et le fonctionnement de l'École européenne d'administration.

Destinataires des données: le sous-traitant de l'EAS qui reçoit et traite les données; le participant au cours lui-même qui reçoit le rapport anonyme global de retour d'information; si le participant le souhaite, le responsable du cours qui reçoit également le rapport anonyme global de retour d'information. Ni l'EAS, ni une quelconque personne au sein des institutions, agences ou offices européens ne reçoit les données.

Licéité du traitement: le traitement est utile pour aider le personnel des institutions, agences et offices européens à exécuter ses missions de management dans l'intérêt public, conformément aux actes légaux adoptés sur la base des traités instituant les Communautés européennes.

Date de début du traitement: la date de réception, par le sous-traitant de l'EAS, des données identifiant le participant au cours et les collègues participant à l'exercice de retour d'information.

Durée de conservation des données: les données concernant l'identité du participant au cours et de son/ses collègues sont conservées pendant une durée maximale de 2 mois à compter de la fin du cours de formation suivi par le participant et pour lequel sont communiquées les données. Les données concernant le retour d'information des collègues (individuelles ou fusionnées) sont conservées pendant une durée maximale de 2 mois à compter de la fin de la session de retour d'information pour laquelle les données sont nécessaires.³

Droit d'accès et vérification: les membres du personnel concernés peuvent demander la prise en compte de changements dans leurs données à caractère personnel. En tout état de cause, suite à une demande écrite avec copie d'une preuve de l'identité, ils peuvent obtenir une copie de leurs données à caractère personnel telles qu'elles ont été enregistrées par le sous-traitant de l'EAS.⁴ Les demandes peuvent être envoyées à: **epso-eas-pdp@ec.europa.eu**.

Suite à une demande écrite avec copie d'une preuve de l'identité, les participants peuvent obtenir une copie écrite de toutes les informations qu'ils ont communiquées sous forme de retour d'information afin de vérifier que celles-ci ont été correctement enregistrées.

Suite à une demande écrite avec copie d'une preuve de l'identité, les collègues qui donnent leur avis peuvent obtenir une copie écrite des informations qu'ils ont communiquées sous forme de retour d'information afin de vérifier que celles-ci ont été correctement enregistrées.

Cette procédure ne confère aucun droit de rectification au sens de l'article 14 du règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000.

Le personnel a également le droit de s'adresser à tout moment au contrôleur européen de la protection des données (edps@edps.europa.eu).

2.3. Transferts de données aux sous-traitants, sécurité des données. L'EAS a fourni les informations complémentaires suivantes concernant les transferts de données aux sous-traitants et la sécurité des données:

- Innotiimi dispose d'un contrat écrit avec l'EAS qui comprend une clause spécifique relative à la protection des données. Cette clause dispose que
 - les données doivent être traitées conformément aux dispositions du règlement (CE) n° 45/2001,

³ L'EAS a expliqué qu'elle avait fixé la durée de conservation à deux mois parce qu'elle la jugeait raisonnable dans la mesure où il pouvait s'avérer nécessaire de générer de nouveaux rapports si le destinataire du rapport égarait son rapport et souhaitait en obtenir un nouvel exemplaire, ou si la personne fournissant un retour d'information individuel souhaitait révéifier les informations communiquées.

⁴ L'EAS a expliqué que chaque participant ayant fourni un retour d'information sur les performances de l'un ou l'autre des participants pouvait uniquement accéder aux informations qu'il avait lui-même fournies. C'est-à-dire qu'il ne peut avoir accès au rapport global final qui a été remis au participant recevant le retour global d'information.

- les données peuvent être traitées uniquement aux fins de l'exécution, de la gestion et du suivi du contrat conclu avec l'EPSO/EAS et selon les instructions du responsable du traitement des données,
 - les données sont confidentielles, le sous-traitant doit en limiter l'accès par le personnel aux cas de stricte nécessité, et
 - le sous-traitant s'engage à prendre des mesures de sécurité technique et organisationnelle appropriées (avec une liste détaillée de ce que doivent garantir ces mesures).
- Les termes de la clause ne limitent pas la capacité d'Innotiimi à choisir ses sous-traitants et n'obligent pas spécifiquement Innotiimi à transférer ces obligations à ses sous-traitants. Toutefois, l'EAS a confirmé que, si le CEPD le jugeait nécessaire, il était encore possible d'inclure cette précision par écrit dans les obligations contractuelles d'Innotiimi. L'EAS a également expliqué qu'Innotiimi avait conclu un contrat écrit et un accord de non divulgation avec Feedback OY.
 - Chez Feedback, tous les employés doivent signer un accord de non divulgation lorsqu'ils rejoignent l'entreprise et seuls ceux qui ont été affectés à ce projet ont accès aux données. Feedback OY a également conclu un accord de non divulgation avec la société d'hébergement du serveur informatique et seules les personnes qui ont signé un accord de non divulgation ont accès au serveur et à la base de données.
 - Le serveur de données est installé dans une salle sécurisée uniquement accessible au personnel autorisé.
 - La maintenance des systèmes se fait par l'intermédiaire d'une connexion sécurisée SSL ou SSH. Les données transférées aux participants sont envoyées par courrier électronique sous forme de fichier zip. Le mot de passe du fichier est ensuite envoyé dans un courrier électronique distinct.

3. Aspects juridiques

3.1. Contrôle préalable

Champ d'application de la notification. Comme évoqué au point 2.1 ci-dessus, la notification et le présent avis portent sur une procédure facultative de «Leadership Feedback» (retour d'information sur les compétences de direction) mise en place par l'EAS en rapport avec ses cours de management.

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

Tous les éléments qui déclenchent l'application du règlement sont réunis en l'espèce.

Premièrement, le traitement de données notifié implique la collecte et le traitement ultérieur de données à caractère personnel telles que définies à l'article 2, point a), du règlement.

Le CEPD souligne que, bien que le retour d'information soit anonyme, cela ne signifie pas que ces données doivent être considérées comme anonymes au sens de l'article 4, paragraphe 1, point e), du règlement. En particulier, Feedback OY peut vérifier à tout moment pendant la période de conservation de deux mois quelle personne a fourni quel retour d'information. En outre, les rapports globaux, bien que ne contenant pas de données à caractère personnel sur les personnes qui donnent leur avis, contiennent les données à caractère personnel (données d'évaluation) sur celles qui reçoivent les rapports.

Deuxièmement, les données à caractère personnel collectées font l'objet de traitements automatisés (article 3, paragraphe 2, du règlement).

Troisièmement, le traitement est réalisé pour le compte de l'EAS, un organe communautaire, dans le cadre du droit communautaire (article 3, paragraphe 1, du règlement).

Compte tenu de ce qui précède, le règlement est applicable.

Motifs du 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 inclut en particulier, au point b), «les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leurs compétences, leur rendement ou leur comportement». L'objet du traitement notifié est l'évaluation des compétences de direction des demandeurs. Les demandeurs commencent par s'évaluer entre eux de façon anonyme, comme décrit ci-dessus. Puis les demandeurs peuvent aussi s'évaluer eux-mêmes et s'entretenir avec leurs formateurs au sujet du retour d'information. Partant, le traitement notifié requiert un contrôle préalable du CEPD.

Notification et date de remise de l'avis du CEPD. La notification a été reçue le 2 septembre 2008. Conformément à l'article 27, paragraphe 4, du règlement, le présent avis doit être rendu sous deux mois. La procédure a été suspendue pendant une durée totale de 42 jours. Partant, l'avis doit être rendu au plus tard le 15 décembre 2008 (3 novembre 2008 + suspension de 34 jours + 8 jours pour les observations).

Véritable contrôle préalable. Le traitement a été notifié avant sa mise en place; par conséquent, il s'agit bien d'un véritable contrôle préalable en l'espèce. Le contrôle préalable étant destiné à régler des situations susceptibles de présenter des risques, l'EAS peut uniquement commencer les traitements après avoir examiné et mis en œuvre les recommandations formulées dans le présent avis.

3.2. Licéité du traitement

L'article 5, point a), du règlement dispose que le traitement de données à caractère personnel est autorisé si «le traitement 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 que soulève l'article 5, point a), est de savoir s'il existe une base légale spécifique pour le traitement: une clause des traités ou d'un autre acte législatif adopté sur la base de ces traités. La deuxième question est de déterminer si le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public.

Sur le premier point, l'avis relatif au respect de la vie privée dont les termes sont repris ci-dessus consacre une section spécifique à cette question («base légale») et cite un certain nombre de documents. Même si aucun d'entre eux ne prévoit expressément une procédure de retour d'information sur les compétences de direction, le CEPD est convaincu qu'il appartient à l'EAS de proposer une telle procédure. Sur le second point, le CEPD est également convaincu et ne conteste pas que le traitement notifié est nécessaire et proportionné, compte tenu, notamment, de son caractère facultatif et anonyme, du fait que l'EAS et Innotiimi n'ont pas accès à des données à caractère personnel, quelles qu'elles soient, et que les données de retour d'information sont utilisées uniquement dans l'intérêt des participants qui reçoivent un retour d'information.

En conclusion, le CEPD considère que les traitements notifiés sont licites, pour autant que les recommandations formulées dans le présent avis soient suivies.

3.3. 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».

L'adéquation, la pertinence et la proportionnalité des données collectées dans le but de fournir un retour d'information doivent être évaluées au cas par cas et peuvent dépendre de la matière enseignée dans le cours de management en question.

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 analysée ci-dessus (voir point 3.2). La question de la loyauté est étroitement liée aux informations qui sont fournies aux personnes concernées (voir point 3.7 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 [doivent être] prises pour que les données inexacts ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées».

L'exactitude peut avoir différents sens dans le contexte du traitement en question. Tout d'abord, elle est étroitement liée à l'adéquation et à la pertinence des questions posées lors de la demande de retour d'information. Plus les questions sont adéquates et pertinentes, plus il est probable que les participants seront à même de donner des réponses significatives afin de fournir un retour d'information utile à chaque participant. En ce sens, l'exactitude doit aussi être évaluée au cas par cas et peut dépendre de la matière enseignée dans le cours de management en question.

L'exactitude dépend également du jugement subjectif des participants qui donnent leur avis, ainsi que des efforts qu'ils déploient pour répondre aux questions. Compte tenu du caractère facultatif de la procédure de retour d'information, du fait que les participants peuvent choisir eux-mêmes les personnes qu'ils invitent à donner leur avis et du fait qu'ils peuvent aussi décider eux-mêmes s'ils souhaitent communiquer le rapport final à leur formateur, le CEPD ne considère pas la subjectivité inhérente à la procédure de retour d'information comme un problème majeur.

3.4. Conservation des données. Le principe général énoncé par le règlement est que les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement (article 4, paragraphe 1, point e), du règlement).

Le CEPD ne remet pas en question le caractère raisonnable de la période de conservation de deux mois envisagée par l'EAS.

3.5. Destinataires et transferts de données. Le CEPD se réjouit que l'accès aux données soit strictement limité et s'inscrive uniquement dans l'intérêt de la personne qui reçoit le retour d'information. Le CEPD est particulièrement satisfait qu'il soit clairement indiqué que l'EAS et les autres institutions européennes n'ont pas accès aux données.

Les sociétés extérieures spécialisées qui sont impliquées dans l'externalisation de la fourniture d'un retour d'information sont soumises à la législation des États membres et, partant, à la directive 95/46/CE. Le CEPD se réjouit que le contrat conclu par l'EAS avec Innotiimi contienne également une clause spécifique relative à la protection des données.

Le CEPD recommande en outre que la clause renvoie expressément à l'article 23, paragraphe 2, point b), du règlement, et aux articles 16 et 17, paragraphe 3, second alinéa, de la directive 95/46/CE (même si les termes de ces dispositions sont déjà résumés dans la clause relative à la protection des données elle-même).

Par ailleurs, le CEPD recommande que le contrat conclu par l'EAS et Innotiimi, qui contient déjà une clause relative à la protection des données, stipule également que

- Innotiimi est tenue de s'assurer que tous ses sous-traitants directs et indirects s'engagent par écrit à respecter les mêmes obligations, et que
- le choix des sous-traitants directs ou indirects d'Innotiimi est soumis à l'approbation de l'EAS, laquelle peut être refusée si la sécurité des données ou le maintien d'autres mesures de protection des données n'est pas garanti.

3.6. Droit d'accès et de rectification. L'article 13 du règlement confère à la personne concernée le droit d'accéder aux données à caractère personnel la concernant. L'article 14 prévoit un droit de rectification des données à caractère personnel.

Le CEPD ne remet pas en question le caractère adéquat ou suffisant des mesures mises en place par l'EAS pour garantir les droits d'accès et de rectification des personnes concernées. Il souligne cependant que la marge de rectification est relativement restreinte eu égard à la subjectivité des rapports de retour d'information et à l'usage limité auquel ces rapports sont destinés. Par exemple, une personne qui donne son avis peut s'apercevoir par la suite qu'elle a commis une erreur dans son retour d'information (notamment inscrit les notes les plus mauvaises des collègues ayant suivi le cours au lieu des meilleures, parce qu'elle pensait à tort que 1 était la meilleure note et 5 la moins bonne, ou inversement). De même, un participant sûr de lui qui a reçu un rapport global donnant une mauvaise image de ses compétences peut demander à Feedback OY de vérifier qu'il n'y pas eu d'erreur de calcul dans la compilation du rapport.

3.7. Informations sur la personne concernée. Les articles 11 et 12 du règlement requièrent que certaines informations soient fournies 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 des réponses des

participants aux questionnaires de retour d'information. L'article 12 s'applique lorsque les données n'ont pas été collectées auprès de la personne concernée, ce qui est le cas des données figurant dans les rapports globaux.

Le CEPD se réjouit que la déclaration de confidentialité figure sur le site Internet de l'EAS et que la documentation remise aux participants aux cours contienne un lien vers celle-ci. À titre de recommandation complémentaire, le CEPD suggère que les informations minimales suivantes figurent au moins aussi dans les imprimés du dossier d'information afin de garantir la loyauté du traitement:

- la procédure de retour d'information est totalement facultative et anonyme,
- toutes les données sont traitées dans le seul but de fournir un retour d'information,
- les données seront supprimées dans un délai de 2 mois, et
- toutes les données sont traitées par des sous-traitants et ni EAS, ni une quelconque personne au sein des Institutions, n'a accès aux données.

3.8. 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 de sécurité 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 pas identifié d'éléments laissant supposer qu'il existe des doutes quant à l'adéquation des mesures de sécurité. Il rappelle cependant les recommandations formulées au point 3.5 ci-dessus concernant l'externalisation.

Conclusion

Rien ne porte à croire que les dispositions du règlement ne seront pas respectées dès lors que les observations formulées aux points 3.2 à 3.8 ci-dessus seront toutes prises en considération.

Les recommandations du CEPD comprennent les éléments suivants:

- Le contrat entre l'EAS et Innotiimi, qui contient déjà une clause relative à la protection des données, devrait également stipuler (i) qu'Innotiimi est tenue de s'assurer que tous ses sous-traitants directs et indirects s'engagent par écrit à respecter les mêmes obligations et (ii) que le choix des sous-traitants directs ou indirects d'Innotiimi est soumis à l'approbation de l'EAS, laquelle peut être refusée si la sécurité des données ou le maintien d'autres mesures de protection des données n'est pas garanti.
- En plus de la déclaration de confidentialité détaillée sur le site Internet de l'EAS, il conviendrait de faire figurer les informations minimales suivantes dans les imprimés du dossier d'information: (i) la procédure de retour d'information est

totalement facultative et anonyme, (ii) toutes les données sont traitées dans le seul but de fournir un retour d'information, (iii) les données seront supprimées dans un délai de 2 mois, et (iv) toutes les données sont traitées par des sous-traitants et ni EAS, ni une quelconque personne au sein des Institutions, n'a accès aux données.

Fait à Bruxelles, le 15 décembre 2008

(signé)

Peter HUSTINX
Contrôleur européen de la protection des données