Avis sur une notification en vue d'un contrôle préalable adressée par le délégué à la protection des données du Conseil concernant la formation eHEST (*Computer based Hostile Environment Security Training*)

Bruxelles, le 22 octobre 2008 (Dossier 2008-0387)

1. Procédure

Le 23 juin 2008, le Contrôleur européen de la protection des données (CEPD) a reçu du délégué à la protection des données du Conseil une notification en vue d'un contrôle préalable relative au traitement des données recueillies pour la formation eHEST (*Computer based Hostile Environment Security Training*).

Le Contrôleur européen de la protection des données a demandé des informations complémentaires les 3 et 11 septembre 2008 et a obtenu les réponses le 12 septembre 2008. Il a reçu le projet d'avis le 18 septembre 2008 et a rendu ses commentaires le 7 octobre 2008. Le délégué à la protection des données du Conseil a également transmis au Conseil, en date du 7 octobre 2008, une version modifiée de cette notification. Les modifications avaient trait aux catégories de personnes concernées, aux procédures accordant leurs droits aux personnes concernées ainsi qu'aux supports utilisés pour le stockage des données.

2. Faits

Finalité de la démarche

La formation eHEST a pour but de sensibiliser à la sécurité afin de réduire les risques encourus par le personnel (fonctionnaires et autres agents des institutions européennes, des États membres et des pays tiers) envoyé en mission dirigée par l'UE (politique européenne de sécurité et de défense, PESD, ou représentant spécial de l'Union européenne, RSUE) à l'extérieur de l'UE, dans le cadre d'une capacité opérationnelle relevant du titre V du traité sur l'Union européenne (TUE).

L'objectif de la formation est de garantir la sécurité des déploiements dans des zones à risques ainsi que de protéger, en cas d'incident grave, le secrétariat général du Conseil contre toute plainte pour négligence ou pour manquement à son devoir de protection.

La formation eHEST est censée devenir la norme en matière de formation de sécurité à l'échelle de l'Union européenne, applicable en tant que telle pour l'ensemble des missions dirigées par l'UE.

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

Description de la démarche

La formation eHEST est une application en ligne disposant d'une fonction d'évaluation automatisée. Au cours du processus d'enregistrement, les utilisateurs sont invités à saisir les données les concernant. Le programme prévoit trois tests, l'utilisateur ne pouvant accéder au test final qu'une fois les deux premiers tests réussis. Ce dernier test délivrera à l'utilisateur son certificat, obligatoire au déploiement dans certaines zones.

Le responsable du traitement est le chef de la direction du bureau de sécurité.

Base légale

Aux termes de la notification, le document du Conseil n° 9490/06 établit la base juridique spécifique du traitement des données. Il traite du projet de politique de l'Union européenne concernant le personnel déployé à l'extérieur de l'Union européenne dans le cadre d'une capacité opérationnelle relevant du titre V du TUE. Ce document fournit un cadre juridique général au déploiement ou aux opérations se déroulant à l'extérieur des frontières de l'Union européenne (cf. paragraphe 36).

Selon la notification, les autres bases juridiques pertinentes sont:
- L'article 14 du TUE;
- L'article 207, paragraphe 2, du traité CE;
- L'article 23, paragraphe 2, deuxième alinéa, du règlement intérieur du Conseil (décision 2006/683/CE du Conseil) disposant que «*Sous son autorité, le secrétaire général et le secrétaire général adjoint prennent toutes les mesures nécessaires pour assurer le bon fonctionnement du secrétariat général*».

Procédures de traitement automatisées / manuelles

Le traitement prévoit un procédé à la fois manuel et automatisé. La personne concernée introduit ses données dans le système et le bureau de sécurité du secrétariat général du Conseil (SGC) reçoit une demande de création de compte qu'il évalue manuellement et approuve ou rejette. Seules les demandes approuvées par le bureau de sécurité permettent à leur initiateur d'accéder au système. La correction de l'évaluation du programme de formation se fait, quant à elle, automatiquement. En effet, les réponses aux questions sont évaluées par le système sans intervention manuelle. Le certificat est, lui aussi, généré de façon automatique pour le candidat reçu et le secrétariat d'eHEST au sein du SGC est informé de cette réussite. Enfin, les résultats et les réponses aux questions sont stockés dans la base de données électronique d'eHEST.

Catégories de personnes concernées

Les personnes concernées sont: les fonctionnaires et autres agents du Conseil, les délégués des États membres et des autres institutions de l'Union européenne.

Catégories de données

Les données recueillies sont: le prénom, le nom, l'adresse électronique, l'organisation (employeur), le type de mission et la destination (PESD, mission en tant que RSUE), les résultats obtenus et le certificat. Ce dernier reprend le nom de l'utilisateur, la date de validation de la formation et les résultats obtenus.

Informations à fournir aux personnes concernées

Au cours de la procédure d'enregistrement, une déclaration de confidentialité fournit à la personne concernée, avant que celle-ci n'ait entré ses données, certaines informations lui sont délivrées à travers une déclaration de confidentialité lui fournit certaines informations.

Celle-ci l'informe sur:

- L'identité du responsable du traitement des données;
- La nécessité des informations personnelles demandées («approuver la demande d'enregistrement et faciliter le suivi des services de formation électronique proposés»);
- Les différentes catégories de données personnelles demandées;
- Les destinataires des données personnelles;
- Les conséquences probables en cas de manquement ou d'échec à l'examen («ne pas transmettre au SGC vos données personnelles exactes ou ne pas réussir l'évaluation suivant la formation eHEST peut avoir un impact sur votre déploiement sur le terrain»);
- Le droit des personnes concernées d'accéder à leurs données et le moyen de faire valoir ce droit; et
- La conservation des données.

Procédures permettant aux personnes concernées de faire valoir leurs droits

En général, l'application des règles relatives au règlement (CE) n° 45/2001 reprise dans la décision du Conseil du 13 septembre 2004 prévoit les droits des personnes concernées dans sa section 5 (articles 16 à 24). Il n'existe pas de règles spécifiques établies pour ce cas de traitement particulier.

Le responsable du traitement précise qu'à la demande d'une personne concernée il peut fournir à celle-ci une analyse détaillée de ses réponses, question par question.

Le responsable du traitement signale également que les demandes adressées au bureau de sécurité du SGC afin de bloquer ou de supprimer ses données seront traitées immédiatement.

Politique de conservation des données

Les données relatives à l'utilisateur et à la formation seront sauvegardées dans le système pour une période de temps variable fixée au cas par cas selon, par exemple, la durée de la mission ou du contrat passé avec la personne concernée, de la validité de son assurance maladie, ou de la nécessité d'établir des statistiques.

Destinataires

Les données sont transmises à l'unité formation du SGC (DGA 1A) ainsi qu'à l'unité «droits de consultation/modification» (DGA 5 «Systèmes d'information et de communication»). Les services de la DGA 5 ne peuvent avoir accès aux données personnelles des personnes concernées que dans le strict cadre de l'entretien du système et de l'aide fonctionnelle.

Seule la personne concernée recevra le certificat attestant de sa réussite au test eHEST.

Aucun transfert de données en dehors du SGC n'est prévu.

Mesures de sécurité

[...]

3. Aspects juridiques

3.1. Contrôle préalable

Le contrôle préalable porte sur le traitement de données à caractère personnel réalisé par une institution communautaire dans le cadre, du moins partiellement, du droit communautaire (article 3, paragraphe 1, du règlement (CE) n° 45/2001). En effet, bien que la formation eHEST soit prévue pour le personnel déployé sur des missions européennes dans le cadre du titre V du TUE, et non pas en vertu du droit communautaire, elle constitue néanmoins une formation professionnelle ayant trait à la gestion des ressources humaines des services du Conseil. Cette formation n'est manifestement pas une activité opérationnelle réalisée dans le cadre du titre V du TUE, mais une activité liée aux ressources humaines et dont la base juridique est le droit communautaire (voir section 3.2 ci-dessous).

Les données sont principalement traitées de façon automatisée (article 3, paragraphe 2 du règlement).

De ce fait, le règlement (CE) n° 45/2001 est applicable.

L'article 27 du règlement soumet au contrôle préalable du CEPD les traitements présentant des risques particuliers au regard des droits et libertés des personnes concernées. L'article 27, paragraphe 2, comporte une liste des traitements susceptibles de présenter de tels risques.

L'article 27, paragraphe 2, point b), du règlement dispose que les traitements susceptibles de présenter de tels risques comprennent *«les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur compétence, leur rendement ou leur comportement»*.

Selon la notification, eHEST n'est pas une simple formation mais comprend également un module d'évaluation et une certification. Il s'agit d'une formation obligatoire pour certaines catégories de personnel, et les résultats obtenus lors de l'évaluation peuvent avoir un impact important pour la personne concernée.

Les traitements doivent donc permettre d'évaluer certains aspects de la personne concernée, y compris ses compétences. Le but de l'opération étant donc l'évaluation, eHEST doit être vue comme tombant sous l'article 27, paragraphe 2, point b), du règlement n° 45/2001.

Le CEPD a reçu la notification du contrôle préalable le 23 juin 2008. En vertu de l'article 27, paragraphe 4, le présent avis doit être rendu dans les deux mois qui suivent la réception. Il doit donc être rendu le 22 octobre au plus tard (22 jours de suspension, et le mois d'août compris).

3.2. Licéité du traitement et base juridique

Le règlement (CE) n° 45/2001 dispose que le traitement de données à caractère personnel doit respecter l'un des points figurant en son article 5 afin de pouvoir être reconnu licite.

L'article 5, point a), du règlement dispose que le traitement de données à caractère personnel peut être effectué 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*».

Au préalable, en vertu de l'article 5, point a), il y lieu de déterminer si le traitement est destiné à remplir une mission bien précise, prévue dans les dispositions d'un traité ou d'un autre instrument législatif adopté sur base des Traités. Ensuite, il convient d'évaluer si l'activité en question est d'intérêt public. Enfin, il faut déterminer si le traitement est nécessaire à la réalisation de cette mission.

Il existe une autorité générale d'organisation des services de l'institution. L'article 23, paragraphe 2, sous-paragraphe 2, du règlement intérieur du Conseil (décision 2006/683/CE du Conseil) constitue la base juridique de cette autorité générale et dispose que *«sous son autorité, le secrétaire général et le secrétaire général adjoint prennent toutes les mesures nécessaires pour assurer le bon fonctionnement du secrétariat général»*.

Le document n°9490/06 du Conseil précise cette base juridique générale et fournit un cadre d'action global au déploiement ou aux opérations se déroulant à l'extérieur de l'Union européenne. Son paragraphe 36 dispose que «*le Secrétariat général du Conseil, agissant sous la responsabilité du Secrétaire général/Haut Représentant assisté du Secrétaire général adjoint: [...] i) veillera à ce que les mesures qui s'imposent soient prises pour assurer la sécurité du personnel non affecté à une opération de gestion de crise effectuant une visite sur le terrain sous l'autorité administrative du Secrétaire général/Haut Représentant dans une zone qui connaît ou pourrait connaître une crise. Ces mesures comprennent notamment, mais pas exclusivement, une formation adaptée[…]»*

La formation eHEST relève de l'exercice légitime de l'autorité publique dont est investie l'institution, à condition qu'elle soit considérée comme nécessaire et qu'elle contribue au bon fonctionnement de celle-ci. En outre, le préambule du règlement formule explicitement que «*le traitement de données à caractère personnel effectué pour l'exécution des missions d'intérêt public par les institutions et les organes communautaires comprend le traitement de données à caractère personnel nécessaires pour la gestion et le fonctionnement de ces institutions et organes*» (considérant 27).

Dans ce contexte, le traitement des données personnelles peut donc être considéré comme étant une activité effectuée dans l'intérêt public.

En outre, il y a lieu d'évaluer la nécessité du traitement au vu de l'objectif qu'il poursuit. En l'occurrence, le traitement est en principe nécessaire pour atteindre les objectifs fixés.

3.3. Qualité des données

En vertu de l'article 4, paragraphe 1, point c), 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*».

Étant donné le nombre réduit d'informations d'identification demandées, ce point est en l'occurrence respecté.

En vertu de l'article 4, paragraphe 1, point d), du règlement, les données personnelles 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»*.

Ce principe est lié de près à l'exercice des personnes concernées de leur droit d'accès, de rectification, de verrouillage ou d'effacement de leurs données (voir point 3.7 ci-dessous).

Enfin, les données doivent également être *«traitées loyalement et licitement»* (article 4, paragraphe 1, point a), du règlement). La question de la licéité a déjà été traitée; quant à la question de la loyauté, elle est liée aux informations à transmettre aux personnes concernées (voir section 3.8 ci-dessous).

3.4. Conservation des données

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. L'institution ou l'organe communautaire prévoit, pour les données à caractère personnel qui doivent être conservées au-delà de la période précitée à des fins historiques, statistiques ou scientifiques, soit qu'elles ne seront conservées que sous une forme qui les rend anonymes, soit, si cela est impossible, qu'elles ne seront stockées qu'à condition que l'identité de la personne concernée soit cryptée. Les données ne doivent en tout cas pas être utilisées à des fins autres qu'historiques, statistiques ou scientifiques*» (article 4, paragraphe 1, point e), du règlement.

Comme indiqué ci-dessus, les données sont conservées pendant une période variable, fixée au cas par cas. Le CEPD recommande de rédiger une procédure efficace permettant d'effacer des données dont la conservation ne sert plus les buts poursuivis par le traitement. En l'occurrence, le CEPD suggère de fixer une limite temporelle à leur stockage, ce qui en faciliterait la gestion et l'effacement. Le CEPD rappelle également que seules les données anonymes peuvent être conservées à des fins statistiques.

3.5. Décisions individuelles automatisées

L'article 19 du règlement (CE) 45/2001 dispose que *«la personne concernée a le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, sa fiabilité ou son comportement, sauf si cette décision est expressément autorisée en vertu de la législation nationale ou communautaire ou, si cela s'avère nécessaire, par le Contrôleur européen de la protection des données. Dans les deux cas, des mesures garantissant la sauvegarde des intérêts légitimes de la personne concernée doivent être prises, telles que des mesures lui permettant de faire valoir son point de vue.»*

Cette disposition s'applique au traitement actuel. En effet, l'évaluation des capacités des personnes concernées se fait ici de façon exclusivement automatisée. Les tests sont corrigés et le certificat délivré automatiquement à la personne sans intervention humaine.

Le CEPD autorise ce traitement pour autant que le responsable du traitement prenne les mesures nécessaires à la protection des intérêts légitimes des personnes concernées. Il s'agit en l'occurrence de leur droit d'accès aux données évaluées, à leur rectification, ainsi que du fait d'informer les personnes concernées de manière adéquate. Ces mesures sont spécifiées aux sections 3.7 et 3.8.

3.6. Transfert de données

Les articles 7, 8 et 9 du règlement prévoient certaines obligations qui s'appliquent en cas de transfert de données à une tierce personne. Dans le cas actuel, le responsable du traitement transfère exclusivement les données au secrétariat général du Conseil. Le transfert de données

entre institutions et organes communautaires ou en leur sein est régi par l'article 7 du règlement.

Le CEPD rappelle que l'article 7, paragraphe 1, du règlement prévoit que les données à caractère personnel sont uniquement transférées *«si elles sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire»*. Afin de respecter cet article, le responsable du traitement doit s'assurer que lors d'un transfert de données, (i) le destinataire dispose des compétences appropriées et (ii) de la nécessité dudit transfert.

Dans le cas actuel, les données sont transférées à l'unité formation du SGC (DGA 1A) pour l'établissement de statistiques, ainsi qu'à l'unité «Droits de consultation/modification» (DGA 5 «Systèmes d'information et de communication»). Les services de la DGA 5 ne peuvent accéder aux données personnelles que dans le strict cadre de l'entretien du système et de l'aide fonctionnelle. Ces transferts sont nécessaires à l'exécution légitime des missions couvertes par la compétence du destinataire et sont donc conformes à l'article 7 du règlement.

3.7. Droit d'accès et de rectification

En vertu de l'article 13 du règlement, la personne concernée a le droit d'obtenir, sans contrainte de la part du responsable du traitement, la communication sous forme intelligible des données faisant l'objet du traitement, ainsi que toute information disponible sur l'origine de ces données.

Comme détaillé au point 2 du présent avis, la personne concernée peut avoir accès à son compte eHEST qui contient ses données d'identification; quant à l'accès aux réponses fournies au cours du test, le responsable du traitement délivrera sur demande une analyse détaillée des réponses de la personne concernée, question par question.

L'article 14 du règlement prévoit que la personne concernée dispose d'un droit de rectification des données inexactes ou incomplètes. Le risque qu'elle en use est néanmoins restreint, étant donné qu'elle saisit elle-même les données d'identification directement dans le système et que les autres données (les résultats de l'évaluation) sont générées automatiquement par ce dernier.

Dans le cas, improbable, d'une erreur humaine ou d'une défaillance du programme, les personnes concernées ont la possibilité de s'adresser au responsable du traitement afin qu'il corrige leurs données.

Par conséquent, le CEPD estime que les articles 13 et 14 du règlement sont respectés.

3.8. Informations à fournir aux personnes concernées

En vertu des articles 11 et 12 du règlement, certaines informations doivent être fournies à la personne concernée. Dans le cas actuel, les données sont principalement obtenues directement de la personne concernée. Les données relatives à l'évaluation et au certificat sont, quant à elles, délivrées automatiquement par le système. Les articles 11 et 12 sont donc d'application.

Comme mentionné précédemment dans la section 2, la déclaration de confidentialité informe les personnes concernées conformément aux articles 11 et 12 du règlement.

Afin de satisfaire entièrement à ces dispositions, le CEPD recommande de mentionner dans la déclaration de confidentialité:
- la base juridique du traitement;

- le caractère obligatoire ou volontaire des réponses aux questions;
- la liste spécifique des destinataires possibles des données (noms des unités du SGC);
- l'existence du droit de rectification des données et le moyen de faire valoir ce droit (conformément aux données d'identification et d'évaluation/de certification);
- la durée précise de conservation des données;
- le droit de saisir à tout moment le CEPD.

3.9. Mesures de sécurité

Des mesures de sécurité ont été mises en place afin d'éviter l'altération, la destruction ou tout accès non-autorisé aux données. À cet égard, le CEPD a reçu des informations qui lui ont permis de déclarer que les mesures de sécurité instaurées semblent être satisfaisantes.

Conclusions

Le procédé proposé ne semble pas enfreindre le règlement (CE) n° 45/2001 tant que les recommandations suivantes sont prises en compte:

- Établir une procédure spécifique d'effacement des données dont la conservation n'est pas nécessaire selon les objectifs du traitement.

- Modifier la déclaration de confidentialité comme établi dans la section 3.8 de cet avis.

Fait à Bruxelles, le 22 octobre 2008

(signé)

Joaquín BAYO DELGADO
Contrôleur européen adjoint de la protection des données