Avis sur une notification en vue d'un contrôle préalable reçue du délégué à la protection des données de la Commission européenne faisant fonction concernant le "Voice recording of Helpdesk calls" (enregistrement vocal des demandes d'assistance)

Bruxelles, le 23 octobre 2006 (dossier 2006-142)

1. Procédure

1.1 Le 17 mars 2006, le Contrôleur européen de la protection des données (CEPD) a reçu par courriel du délégué à la protection des données (DPD) de la Commission européenne faisant fonction, conformément à l'article 27 du règlement (CE) nº 45/2001, une notification en vue d'un contrôle préalable concernant la procédure et le système du "Voice recording of Helpdesk calls" (enregistrement vocal des demandes d'assistance) de la DG Société de l'information et médias (DG INFSO).

1.2 À la notification étaient joints les documents suivants: une note adressée par le DPD à M. Peter Hustinx, CEPD; la "Privacy Statement - Voice recording of DG INFSO IT HELPDESK calls" (déclaration de confidentialité); une note diffusée par courriel à tout le personnel de la DG; une pièce jointe à la question 15 de la notification DPO-886.1 (le texte du bref message vocal d'information qui sera diffusé au début de chaque appel que reçoit le service d'assistance informatique de la DG).

1.3 Le 30 mars 2006, le CEPD a demandé des informations complémentaires, qu'il a reçues le 5 juillet. Le 4 août, il a demandé d'autres informations, qu'il a reçues le 7 août. La réponse reçue a entraîné une nouvelle demande (faite le 8 août), à laquelle il a été répondu le même jour.

Le 28 août, le CEPD a prolongé le délai de quatre semaines en raison de la complexité du dossier.

Le 8 septembre, il a fait savoir au DPD de la Commission que le système, tel qu'il lui avait été présenté alors, soulevait plusieurs questions de droit importantes. Il a en outre posé plusieurs autres questions, auxquelles des réponses lui ont été fournies le 21 septembre.

Le 9 octobre, le CEPD a suspendu la procédure pour sept jours en envoyant la dernière demande d'informations, afin que le DPD puisse faire des observations utiles et transmettre au besoin d'autres informations. La suspension a été maintenue sept jours de plus.

Adresse postale: rue Wiertz 60 - B-1047 Brussels
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

2. Examen de la question

2.1. Les faits

La DG INFSO envisage d'installer un système d'enregistrement pour améliorer la qualité de l'aide offerte par son service d'assistance informatique: toutes les conversations entre les personnes qui demandent de l'aide et les opérateurs du service d'assistance seront enregistrées et conservées dans un système "NiceCall Focus II" (ci-après dénommé "le NCFS"), qui sera utilisé parallèlement au système *Peregrine* qui, lui, crée des "dossiers d'incidents" ("trouble ticket"). Les conversations d'origine pourront ainsi être associées à un dossier d'incident: lorsqu'un utilisateur appelle, l'incident est enregistré dans ce système pour être ensuite soit réglé, soit transmis à d'autres groupes de soutien; les informations se trouvant dans *Peregrine* (estampille temporelle, nom de l'opérateur) peuvent être associées aux informations fournies par le NCFS pour retrouver les conversations échangées entre les opérateurs et les utilisateurs.

Les finalités déclarées du système sont les suivantes:
1) rationaliser les réponses apportées aux demandes d'aide en permettant de retrouver les conversations d'origine et de vérifier les informations enregistrées dans le dossier d'incident sans devoir rappeler l'utilisateur;
2 a) contrôler la qualité des conversations entre les utilisateurs et les opérateurs dans le but de renforcer l'efficacité de ces derniers en termes de gestion du temps et de collecte des informations;
2 b) simplifier et raccourcir la formation des nouveaux opérateurs, tout en en améliorant la qualité, en disposant d'exemples de conversations réelles avec des utilisateurs.

La déclaration de confidentialité indique expressément que "*l'objectif est dépourvu de tout lien avec le système du rapport d'évolution de carrière ou avec des évaluations similaires du personnel, contexte dans lequel les informations obtenues par le système ne seront pas mentionnées*" (traduction non officielle).

Au regard de la première finalité, la nécessité d'enregistrer les conversations a été justifiée par les motifs suivants: le travail des opérateurs consiste à résumer et essayer de clarifier les informations fournies par les utilisateurs, afin de faciliter le travail des spécialistes (centres de soutien) qui pourraient être appelés à intervenir ultérieurement; or, les conversations se déroulent souvent dans une langue qui n'est pas la langue maternelle de l'opérateur, ce qui, même si les opérateurs ont généralement une bonne connaissance des deux principales langues de travail, peut être source d'imprécision dans l'interprétation desdites informations; l'efficacité des opérateurs sera donc améliorée s'il leur est possible, sans devoir rappeler l'utilisateur, de réécouter les conversations d'origine associées au dossier d'incident pour évaluer le problème et le transmettre au bon groupe de soutien. Le responsable du traitement a fait observer que la possibilité de réécouter les conversations pouvait contribuer à clarifier certains éléments même après la transmission du dossier d'incident à d'autres groupes de soutien spécialisés, et ce sans faire perdre aux utilisateurs leur temps précieux.

Au regard de la deuxième finalité, la nécessité d'enregistrer les conversations a été justifiée par les motifs suivants: les services d'assistance constituent la première ligne des contacts avec les utilisateurs (ou clients) et comptent pour une très grande part dans la façon dont la qualité du service fourni est perçue; dès lors, pouvoir disposer de conversations réelles à titre d'exemples durant la formation est un atout précieux, puisque celles-ci permettent de renforcer les principes de base que sont la courtoisie, l'efficacité et l'exhaustivité dans les dialogues avec les clients.

Le contenu de la conversation sera le seul élément utilisé pour contrôler l'efficacité et la courtoisie des opérateurs. Ces qualités pourront être améliorées par l'analyse des conversations qui sera effectuée par les destinataires du traitement et en mettant en exergue tant les pratiques les meilleures (et les plus efficaces) que celles qui peuvent être améliorées (en faisant, par exemple, un relevé des "erreurs communes"). Ces conversations seront diffusées au cours de la première séance de formation, que le chef d'équipe du système d'assistance donne aux nouveaux opérateurs.

Au CEPD qui lui demandait pourquoi un enregistrement vocal par le NCFS était nécessaire pour assurer le bon fonctionnement du service d'assistance informatique, le responsable du traitement a répondu qu'un système d'enregistrement n'était pas indispensable en tant que tel au fonctionnement d'un service d'assistance, mais qu'il permettait d'améliorer la qualité du service fourni tout en protégeant, moyennant une bonne gestion, la vie privée et la dignité des travailleurs et des utilisateurs concernés.

Et à la question de savoir si l'on avait envisagé des solutions moins envahissantes pour atteindre les objectifs du service d'assistance (amélioration de la qualité du soutien et contrôle de la qualité), la réponse a été que les systèmes d'enregistrement se généralisent dans toutes les organisations de soutien et que l'on reçoit de plus en plus souvent des messages annonçant un enregistrement lorsqu'on appelle toutes sortes de centres d'appels; que ces systèmes deviennent apparemment la réponse standard apportée par un centre d'appels à un problème assez commun; que le marché les adopte progressivement, car ils constituent la solution offrant la meilleure qualité et le meilleur rendement; et qu'il est très difficile d'améliorer globalement le service sans disposer de données réelles (au lieu d'interprétations ou de rapports à leur sujet).

Les personnes qui appellent le service d'assistance de la DG INFSO sont principalement des membres du personnel de la DG, mais rien n'empêche des personnes de l'extérieur de l'appeler aussi. Les opérateurs du service qui reçoivent les appels sont soit des fonctionnaires soit des contractuels engagés par le biais d'un contrat cadre DIGIT pour fournir des services de soutien informatique.

Le NCFS a été choisi pour sa simplicité technique, car il ne possède pas d'outil d'analyse de la parole ni de fonctions de contrôle plus avancées ou plus sophistiquées. Il ne permet pas d'effectuer des enregistrements sélectifs: il est simplement actif ou inactif. Il n'est pas non plus possible de l'activer ou le désactiver manuellement, via les outils de gestion du système. Les enregistrements ne peuvent dès lors être sélectionnés "qu'après coup". On a aussi fait observer que les opérateurs ne pouvaient prévoir, au début de la conversation, si les informations allaient être nécessaires plus tard, et que retarder le début de l'enregistrement pouvait entraîner la perte d'éléments essentiels.

Le responsable du traitement n'envisage pas de rendre anonymes les enregistrements ou les informations qui s'y rapportent, et ce pour deux raisons principales: 1) le système ne contient pas de mécanisme permettant de le faire automatiquement; 2) la modification de la voix ou la suppression de certaines parties d'une conversation risquent de porter atteinte à la compréhensibilité du contenu, ce qui compromettrait l'une des finalités (rationaliser les réponses apportées aux demandes d'aide en permettant de retrouver les conversations d'origine et de vérifier les informations enregistrées dans le dossier d'incident sans devoir rappeler l'utilisateur).

La notification en vue du contrôle préalable énumère les données concernées: numéro de téléphone des opérateurs du service d'assistance, estampille temporelle du début et de la fin de chaque conversation, enregistrement de chaque conversation. La déclaration de confidentialité précise en outre que le numéro de canal est enregistré et [1] qu'il est associé au numéro de téléphone de l'opérateur. Il y est mentionné que "*parmi les autres informations pouvant être enregistrées dans le*

[1] Note relative au texte même de la déclaration, qui n'est disponible qu'en anglais.

cadre d'une conversation figurent entre autres vos nom, prénom, titre, unité, numéro de fax, adresse électronique et adresse. Ces données ne feront néanmoins l'objet d'aucun traitement et ne seront utilisées qu'en vue du contrôle de la qualité de l'opération et de l'amélioration des activités du service d'assistance informatique de la DG INFSO" (traduction non officielle). L'opérateur ne demandera à l'utilisateur de s'identifier que si lui même ne peut le faire par d'autres moyens (par exemple, l'affichage sur l'appareil téléphonique). Les utilisateurs appelant de l'extérieur de la Commission et qui pourraient devoir être rappelés pour recevoir un soutien sont invités à donner leur numéro de téléphone. Il convient d'observer qu'il est impossible d'enregistrer un dossier d'incident et de fournir un soutien sans connaître l'identité de l'utilisateur.

Le responsable du traitement a fait observer que l'identité de l'opérateur pouvait être associée au résultat des recherches, tout comme elle l'est à un numéro de téléphone précis. Pour pouvoir retracer les appels, conformément aux finalités du système, il est nécessaire de connaître l'identité de l'opérateur. La plupart du temps, le lien physique entre le numéro de canal du NCFS et le numéro de téléphone permet de retrouver le numéro de téléphone de l'opérateur ayant participé à la conversation. Or, un opérateur peut utiliser exceptionnellement le téléphone d'un collègue (en raison d'une défaillance de son poste ou du réseau téléphonique, de la rotation du personnel chargé du service d'assistance, etc.).

On ne peut exclure que la voix de collègues opérateurs soit reconnue pendant la formation, alors même que le formateur n'indiquera pas expressément leur nom. Le responsable du traitement a fait observer que "*l'on ne peut être sûr de reconnaître à 100 % la voix d'un opérateur sans disposer d'outils sophistiqués, qui ne sont pas fournis dans le cadre de services standard comme un service d'assistance*".

Le chef d'équipe du service d'assistance enverra à ses opérateurs un courriel indiquant qu'un enregistrement donné (défini sur la base de l'estampille temporelle, du numéro d'appel du système du service d'assistance et du numéro de poste de l'opérateur) va être utilisé aux fins d'une formation.

Sur demande écrite expresse de l'opérateur concerné, adressée au chef d'équipe, l'enregistrement ne sera pas utilisé aux fins d'une formation. La demande écrite devra contenir les éléments permettant de retrouver l'enregistrement (date et heure précises, ainsi que numéro d'appel du système du service d'assistance et numéro de poste de l'opérateur).

Un opérateur pourrait demander globalement qu'aucun enregistrement correspondant au numéro de poste associé à son nom ne soit utilisé. Rappelons toutefois que le responsable du traitement a fait observer que l'opérateur pourrait, à certaines occasions, utiliser un autre poste que le sien.

L'administrateur du système dispose d'outils pour rechercher et réécouter les conversations, soit directement, soit après les avoir exportées vers des fichiers informatiques (format WAV). Des fonctions "établissement de rapports" (*reporting*) sont disponibles pour fournir des informations statistiques. Le mot "rapport" (*report*) désigne le résultat d'une recherche faite en utilisant le logiciel Nice Query fourni par le NCFS. Les termes "établissement de rapports" désignent l'action d'utiliser l'outil de recherche pour obtenir une liste des conversations, avec leur durée, enregistrées pendant une période donnée et sous les numéros de canaux indiqués. Ainsi, les outils de recherche permettent d'effectuer tant des recherches que des traitements portant sur le numéro de téléphone des opérateurs du service d'assistance, le numéro de canal connexe (généré par le système et généralement associé au même numéro d'opérateur), le nombre d'appels enregistrés pendant des périodes données et la durée des appels.

Les données statistiques ne permettent pas de retrouver le numéro de téléphone du demandeur: n'étant pas enregistrée dans le NCFS, cette information ne se prête pas à une recherche.

L'outil de recherche ne peut utiliser le contenu de la conversation comme critère de recherche.

Les fonctions de recherche seront installées sur les ordinateurs personnels du chef d'équipe du service d'assistance, des personnes chargées du soutien, du responsable du traitement et de l'adjoint de ce dernier. Les catégories de destinataires sont:

- les administrateurs du système: administrateurs locaux, chefs d'équipe du service d'assistance, responsable du soutien aux utilisateurs;
- IDOC, ADMIN/DS (direction de la sécurité), OLAF, AUDIT, médiateur, DPO, CEPD;
- établissement de rapports: chef d'équipe du service d'assistance, responsable du soutien aux utilisateurs, responsable du traitement et son adjoint;
- le CEPD fait observer que, lorsqu'une conversation enregistrée leur est présentée, les personnes qui suivent une formation sont aussi des destinataires de données.

La production de transcriptions des dialogues enregistrés n'est pas prévue; seuls les enregistrements sonores seront utilisés lors des formations.

Information des personnes concernées:

- dans la *page d'information sur l'intranet de la DG (déclaration de confidentialité)*, on trouve des informations sur le système en général, l'identité du responsable du traitement, la mention du règlement 45/2001, le type de données à caractère personnel collectées, les finalités du traitement, la base juridique, des informations techniques sur l'enregistrement (contenu et données relatives au trafic), l'accès aux informations contenues dans le système et les personnes auxquelles les données peuvent être communiquées, une brève description des mesures de sécurité, les procédures permettant de vérifier, de modifier et de supprimer des données à caractère personnel, la période de conservation des données (six mois), les points de contact et le droit de saisir le CEPD ("*en cas de conflit, une réclamation peut être adressée au contrôleur européen de la protection des données"*);
- par le biais d'un *courriel adressé à tout le personnel de la DG* sont diffusés des informations sur la finalité du système et sur la procédure même, le message d'accueil que chaque personne entendra au début de chaque conversation (voir le texte infra), un lien vers la déclaration de confidentialité et un autre lien vers le texte du règlement 45/2001;
- les nouveaux venus recevront des informations dans le cadre des présentations consacrées aux outils informatiques de la DG, faites par le gestionnaire des ressources informatiques;
- le bref message vocal suivant peut être entendu au début de chaque appel au service d'assistance informatique de la DG: "*Bienvenue au service d'assistance informatique de la DG INFSO. La présente conversation est enregistrée pour permettre un contrôle de la qualité*" (traduction non officielle).

Chaque intéressé peut obtenir une copie de l'enregistrement de sa conversation avec le personnel du service d'assistance, à condition de pouvoir être identifié clairement et sans équivoque au moyen du contenu. Une demande en ce sens peut être adressée par courriel à l'adresse "INFSO HELPDESK". La même procédure permet aux personnes concernées de demander à vérifier quelles sont les données à caractère personnel qui sont conservées par le responsable du traitement, de demander leur modification, leur rectification ou leur suppression. Une demande de rectification est soumise par le biais de l'enregistrement d'une nouvelle conversation, qui précise sans équivoque l'enregistrement à rectifier.

La durée de conservation ne peut dépasser six mois, ce qui s'applique aussi aux enregistrements dont l'opérateur du service d'assistance ne souhaite pas qu'ils soient utilisés à des fins de formation.

Bien qu'il soit possible, comme le responsable du traitement l'a fait observer, d'adapter le système pour conserver les données jusqu'à sept ans (date à laquelle la suppression serait automatique), c'est la période de conservation indiquée ci-dessus qui a été définie, pour des raisons pratiques et pour respecter le règlement. Le service d'assistance recevant plus de 20 000 appels par an, le nombre d'enregistrements suffit à garantir qu'il y en aura toujours de disponibles pour une formation.

Le délai pour verrouiller des données (sur demande légitime étayée des personnes concernées) est de quatre mois. Selon le responsable du traitement, ces quatre mois suffisent pour assurer aux utilisateurs la possibilité de demander, s'ils le souhaitent, le verrouillage de données. Les périodes de vacances, de maladie, de missions et autres formes d'absence ont aussi été prises en compte. Cette durée permettra au responsable du traitement d'intervenir avant que les mécanismes automatiques liés à la durée maximale de conservation n'effacent les enregistrements.

Mesures de sécurité

[…]

2.2 Aspects juridiques

2.2.1 Contrôle préalable

Le règlement (CE) nº 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 (ci-après dénommé "le règlement") s'applique au traitement de données à caractère personnel effectué par la Commission européenne.

Les "données à caractère personnel" y sont définies comme étant toute information concernant une personne physique identifiée ou identifiable. "*Est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale*" (article 2, point a)). Le considérant 8 précise que, "*afin de déterminer si une personne est identifiable, il convient de prendre en considération l'ensemble des moyens susceptibles d'être raisonnablement utilisés par le responsable du traitement ou par toute autre personne pour identifier ladite personne*". Le nom de la personne qui appelle est affiché sur l'appareil téléphonique ou, si elle appelle de l'extérieur de la Commission, ses données d'identification (par exemple, son numéro de téléphone) sont enregistrées durant la conversation. De toute façon, son identification est un élément nécessaire pour que le service d'assistance puisse résoudre son problème informatique. L'opérateur du service d'assistance peut être identifié par sa voix. Il n'est pas non plus exclu que des personnes qui suivent une formation puissent reconnaître la voix de leurs collègues dans le dialogue enregistré qu'ils écoutent. En général, le lien physique entre le numéro de canal pour entrer dans le NCFS et le numéro de téléphone permet aussi d'identifier les opérateurs du service d'assistance participant à la conversation. Les données contenues dans les appels enregistrés ou écoutés pouvant être associées à certaines personnes précises (opérateurs ou utilisateurs), l'article 2, point a), s'applique.

Le traitement de données à caractère personnel est effectué par la DG INFSO de la Commission européenne, dans l'exercice d'activités qui relèvent du champ d'application du droit communautaire (article 3, paragraphe 1).

Le présent dossier concerne essentiellement un traitement automatisé (article 3, paragraphe 2).

Dès lors, le règlement est applicable.

L'article 27, paragraphe 1, 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. La protection des données à caractère personnel et de la vie privée dans le contexte des réseaux internes de télécommunications constitue un problème particulier. Le chapitre IV du règlement contient une disposition spécialement consacrée à la confidentialité des communications (article 36). Comme le système d'enregistrement vocal restreint cette confidentialité, il présente à l'évidence un risque particulier au regard des droits et libertés des personnes concernées et est dès lors couvert par l'article 27, paragraphe 1.

La notification du DPD a été reçue le 17 mars 2006. Selon l'article 27, paragraphe 4, le présent avis doit être rendu dans les deux mois, soit au plus tard le 18 mai 2006. La procédure ayant été suspendue pendant 97 jours + 3 jours, l'avis devait être rendu le 28 août (le 26 étant un samedi). Cependant, la complexité du dossier a nécessité une prolongation du délai: le 28 août, le CEPD l'a prolongé de quatre semaines supplémentaires. Une nouvelle demande d'informations ayant entraîné une suspension de 13 jours, l'avis aurait dû être rendu le 9 octobre (le 8 étant un dimanche). La dernière demande d'informations transmise au DPD ayant suspendu à nouveau la procédure pendant 14 jours, l'avis devait être rendu le 23 octobre 2006 au plus tard.

2.2.2 Licéité du traitement

Le système d'enregistrement vocal des appels transmis au service d'assistance informatique est conçu pour réaliser deux finalités principales: 1) assurer un bon niveau des services offerts par le service d'assistance en disposant de l'enregistrement de la conversation pour résoudre l'incident informatique signalé; 2) contrôler la qualité, ce qui se ramène essentiellement à utiliser des enregistrements choisis à des fins de formation.

L'examen de la licéité du traitement en cause commande d'analyser conjointement le principe de la nécessité, le principe de proportionnalité et la question de la restriction de la confidentialité des communications, parce que ces trois points sont étroitement liés.

Des données à caractère personnel ne peuvent être traitées que pour les motifs énoncés à l'article 5 du règlement. La notification mentionne le point a) de cette disposition, qui prévoit qu'un traitement est licite s'il est "*nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités ou relevant de l'exercice légitime de l'autorité publique dont est investi l'institution ou l'organe communautaire nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités ou relevant de l'exercice légitime de l'autorité publique dont est investi l'institution ou l'organe communautaire*". Le considérant 27 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 nécessaires pour la gestion et le fonctionnement de ces institutions et organes*". La finalité du système qui consiste à vérifier les informations dont on a besoin pour résoudre le problème est vraiment à la limite de cette nécessité. S'il peut comprendre les raisons pratiques avancées par le responsable du traitement pour justifier l'enregistrement de chaque appel afin de résoudre l'incident, le CEPD fait néanmoins valoir qu'il ne va pas de soi qu'un enregistrement aussi extensif soit nécessaire pour que la tâche de la Commission soit exécutée dans l'intérêt du public. La première finalité du système étant un cas limite, il convient d'examiner attentivement les questions de la proportionnalité et de la confidentialité des communications (voir la section 2.2.3 infra). Quant à enregistrer chaque appel que reçoit le service d'assistance informatique afin d'avoir suffisamment d'échantillons pouvant être

sélectionnés à des fins de formation, cela dépasse le cadre de ce qui est "nécessaire" à l'exécution des tâches de la Commission (pour remédier à ce constat, voir infra).
En ce qui concerne la base juridique, les exigences vont dépendre du traitement: la nécessité de prévoir des garanties légales diffère selon les risques que présente le traitement et doit être évaluée en tenant compte de ceux-ci. L'enregistrement de communications et l'usage ultérieur de ces enregistrements exigent davantage de garanties parce qu'ils présentent des risques plus élevés pour les droits et libertés des personnes.

Il est indiqué dans la notification en vue d'un contrôle préalable que le traitement effectué par le NCFS est nécessaire pour assurer la bonne qualité de l'exécution et du soutien des tâches de la DG, qui lui sont déléguées par les articles 6 [2] et 7 [3] du traité UE et 211 à 219 [4] et 255 [5] du traité CE [6]. Le Code de bonne conduite administrative pour le personnel de la Commission européenne dans ses relations avec le public (annexe de la décision de la Commission du 17 octobre 2000) requiert un service de qualité dans les termes suivants: "*Le public est en droit d'attendre un service de qualité et une administration ouverte, accessible et gérée correctement.*" [7] Comme nous l'avons déjà dit, traiter des données à caractère personnel pour résoudre un incident rentre tout juste dans les limites de ce qui peut être considéré comme étant nécessaire pour fournir le service. Ce traitement est juste acceptable compte tenu de la base juridique qu'est le Code de bonne conduite administrative. En raison de cette situation délicate, il convient de prévoir davantage de garanties, comme un délai de conservation très court (voir la section 2.2.5 infra).

L'utilisation des enregistrements pour une autre finalité que le contrôle de la qualité (à savoir, la formation) dépasse les limites acceptables de la nécessité (voir supra). Dès lors, pour que le traitement soit licite à des fins de formation tout en conservant une marge de manœuvre, le responsable du traitement devrait recourir à l'une des deux solutions suivantes: a) rendre les données à caractère personnel anonymes (la protection des données n'étant dès lors plus un problème); b) étant donné que la solution a) présente, selon les explications du responsable du traitement, un certain nombre de difficultés techniques, il faudrait faire reposer le traitement sur une base juridique appropriée pour qu'il soit licite. Si les personnes concernées (utilisateurs et opérateurs) consentent à ce que des dialogues non anonymes soient vérifiés en vue d'un contrôle de la qualité et à ce que ces enregistrements soient utilisés à des fins de formation, le traitement pourrait être licite au regard de la deuxième finalité en vertu de l'article 5, point d), du règlement.

Selon l'article 2, point h), du règlement, "*on entend par "consentement de la personne concernée": toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement*".
Pour donner un consentement véritable, la personne concernée doit être au courant du fonctionnement du système en général et de certains de ses détails (voir la section 2.2.8 infra). Il convient d'observer aussi que le présent dossier porte sur un "consentement" dans le contexte

---

[2] *"1. L'Union est fondée sur les principes de la liberté, de la démocratie, du respect des droits de l'homme et des libertés fondamentales, ainsi que de l'État de droit, principes qui sont communs aux États membres.*
2. L'Union respecte les droits fondamentaux, tels qu'ils sont garantis par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, et tels qu'ils résultent des traditions constitutionnelles communes aux États membres, en tant que principes généraux du droit communautaire."

[3] *"Le Conseil (…) peut constater l'existence d'une violation grave et persistante par un État membre de principes énoncés à l'article 6, paragraphe 1, après avoir invité le gouvernement de cet État membre à présenter toute observation en la matière."*

[4] Ayant trait à la Commission.

[5] Sur le droit d'accès aux documents des institutions et les limites de ce droit.

[6] Après modification par le traité d'Amsterdam (JO C 340 du 10.11.1997).

[7] Le responsable du traitement a précisé que, malgré la divergence entre les bases juridiques mentionnées dans la notification et dans la déclaration de confidentialité, c'est la première qui est la base appropriée.

professionnel - qui a fait l'objet de l'avis 8/2001 [8] (sur le traitement des données à caractère personnel dans le contexte professionnel au regard de la directive 95/46/CE) du groupe de l'article 29, où il est souligné au point 10 que "*si le consentement du travailleur est nécessaire et que l'absence de consentement peut entraîner un préjudice réel ou potentiel pour le travailleur, le consentement n'est pas valable au titre de l'article 7 ou de l'article 8, dans la mesure où il n'est pas donné librement. Si le travailleur n'a pas la possibilité de refuser, il ne s'agit pas de consentement. Le consentement doit toujours être donné librement. En conséquence, le travailleur doit avoir la possibilité de se dégager de son consentement sans préjudice*". L'exigence de consentement prévue par le règlement devrait être interprétée de la même manière.

Les personnes qui appellent le service d'assistance informatique entendent le message d'accueil, qui évoque l'enregistrement de la conversation en vue du premier objectif; lorsqu'elles communiquent ensuite les données à caractère personnel nécessaires à répondre à leur besoin d'aide informatique, on pourrait considérer qu'elles consentent au traitement à condition que les informations contenues dans le message d'accueil soient plus claires (voir la section 2.2.8 sur l'information de la personne concernée). Pour ce qui est du consentement dans le cadre de la deuxième finalité, le responsable du traitement peut choisir entre les deux solutions suivantes: 1) soit commencer par sélectionner les dialogues, puis demander aux personnes concernées leur consentement pour utiliser dans une formation l'enregistrement où elles interviennent; 2) soit prévoir que, à la fin de chaque appel, les opérateurs demandent à la personne concernée si elle accepte que le conversation enregistrée soit utilisée à des fins de formation. En cas de refus, ces enregistrements ne peuvent être utilisés et doivent être détruits. Le consentement ou le refus est donc aussi enregistré et doit être respecté.

Les opérateurs ont une possibilité de refuser ("opt-out") l'usage ultérieur des enregistrements à des fins de formation. Comme prévu, ils peuvent demander globalement que les enregistrements liés à leur numéro de téléphone ne soient pas utilisés et, à leur demande écrite expresse, certains enregistrements précis seront exclus de l'utilisation à des fins de formation.

Pour des raisons de loyauté à l'égard des opérateurs, le CEPD recommande que, une fois sélectionnés les dialogues qui pourraient être utilisés en formation (dans le délai de cinq jours ouvrables suivant la date de l'enregistrement), les opérateurs non seulement reçoivent les données d'identification de l'enregistrement dont l'utilisation est envisagée, mais aient aussi l'occasion d'écouter le dialogue sélectionné, avec leur voix et leurs données à caractère personnel. Ce n'est que dans ces conditions que leur consentement pourrait être qualifié de "spécifique" et "informé".

Un consentement donné librement suppose aussi qu'il puisse être retiré; les personnes concernées devraient donc pouvoir demander de ne plus utiliser l'enregistrement sélectionné.

2.2.3 Confidentialité des communications

Selon l'article 36 du règlement, les *"institutions et organes communautaires garantissent la confidentialité des communications réalisées au moyen de réseaux de télécommunications et des équipements de terminaux dans le respect des principes généraux du droit communautaire."*

Le principe de la confidentialité des communications peut être interprété dans deux sens: les institutions communautaires doivent non seulement assurer la confidentialité des communications contre toute interférence extérieure, mais aussi respecter elles-mêmes cette confidentialité. Le premier aspect est lié à la sécurité du réseau (voir la section 2.2.9 infra).

---

[8] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48fr.pdf

Il faut préciser d'emblée que le principe de la confidentialité des communications s'inspire de l'article 5 de la directive 97/66 [9], qui prévoit notamment que les États membres interdisent à toute autre personne que les utilisateurs, sans le consentement des utilisateurs concernés, d'écouter, d'intercepter, de stocker les communications ou de les soumettre à quelque autre moyen d'interception ou de surveillance, sauf lorsque ces activités sont légalement autorisées, conformément aux principes généraux du droit communautaire. La directive 97/66 a entre-temps été remplacée par la directive 2002/58 [10], mais le principe est resté le même: si les parties à la communication ont donné leur consentement, le principe de la confidentialité des communications n'est pas atteint (article 5). Le CEDP estime qu'il faut interpréter de la même manière l'article 36 du règlement.

Selon cet article 36, toute restriction apportée au principe doit être conforme aux "principes généraux du droit communautaire". Ce concept des "principes généraux du droit communautaire" renvoie aux droits fondamentaux, en particulier tels qu'ils sont énoncés dans la Convention européenne des droits de l'homme, dont l'article 8 énonce, au paragraphe 1, le droit au respect de la vie privée et familiale et précise, au paragraphe 2, le critère selon lequel ce droit peut être restreint. Ainsi, toute ingérence dans l'exercice de ce droit doit être "prévue par la loi" et "dans une société démocratique, (être) nécessaire à la sécurité nationale, à la sûreté publique, (…) à la défense de l'ordre et à la prévention des infractions pénales, à la protection de (…) la morale, ou à la protection des droits et libertés d'autrui". Le critère de la nécessité dans une société démocratique inclut le principe de "proportionnalité".

Les principes de la protection des données selon lesquels le traitement doit être "nécessaire" au regard de sa finalité et "proportionné" à la fin poursuivie doivent donc être respectés en l'espèce.

Le CEPD estime qu'un enregistrement non sélectif des appels arrivant au service d'assistance, en vue des finalités définies, ne devrait être autorisé que dans des cas très limités, lorsque des garanties suffisantes sont mises en place.

La première finalité du système est de vérifier les informations données afin de résoudre le problème informatique. Le travail de l'opérateur consistant à résumer et clarifier le problème signalé et à faciliter par là le travail du groupe de soutien spécialisé, il peut être utile de réécouter la conversation avec l'utilisateur ou le client pour élucider des points de détail lorsque le dossier d'incident a été transmis à d'autres groupes de soutien en vue de résoudre le problème. Cette possibilité revêt en outre une importance certaine dans un milieu de travail où des langues autres que la langue maternelle sont utilisées, situation qui peut créer une certaine imprécision. Le CEPD estime dès lors que, aux fins de l'exécution des tâches de la DG consistant à résoudre le problème signalé, un enregistrement non sélectif peut être nécessaire pour des raisons pratiques, mais uniquement s'il est accompagné de garanties suffisantes et à condition que la durée de conservation des données soit très courte (voir supra, sextion 2.2.2, "Licéité du traitement", et infra, section 2.2.5, "Conservation des données").

Par contre, l'enregistrement de chacun des appels dans le but de disposer d'un nombre suffisant de cas pour sélectionner des échantillons de "bonnes pratiques" et d'"erreurs fréquentes" est disproportionné par rapport aux buts poursuivis. Le CEPD n'est pas d'accord avec l'argument du responsable du traitement, qui soutient que les systèmes d'enregistrement sont de plus en plus courants et que la réponse donnée par le marché au besoin de disposer de centres d'appels justifie un enregistrement systématique et l'utilisation ultérieure des enregistrements. Un enregistrement

---

9 Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.

10 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

systématique des appels reçus par le service d'assistance dans le but de disposer de suffisamment d'exemples à choisir en vue d'une formation est une collecte de données excessive (voir infra, section 2.2.4, "Qualité des données").

Le CEPD recommande au responsable du traitement d'envisager d'autres moyens, moins envahissants, pour atteindre l'objectif consistant à disposer d'échantillons en vue de la formation et de l'amélioration tant de l'efficacité de la gestion du temps que de la courtoisie des opérateurs lorsqu'ils collectent des informations. Par exemple, on pourrait utiliser, pour la formation, une simulation de pratiques de communication, bonnes et moins bonnes, reposant sur l'expérience des opérateurs. Ou encore, les nouveaux venus pourraient s'asseoir près de l'opérateur et suivre de près son travail.

2.2.4 Qualité des données

Les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement (article 4, paragraphe 1, point c), du règlement). Cette exigence fait écho au principe de proportionnalité, en vertu duquel seules peuvent être utilisées les données qui sont nécessaires pour atteindre la finalité particulière pour laquelle elles ont été collectées. Il faut qu'il existe un lien suffisant entre la finalité et les données traitées. Le système examiné ici a deux finalités: vérification des informations pour résoudre un problème, d'une part, contrôle de la qualité et formation, d'autre part. Il faut examiner séparément si les données collectées sont adéquates, pertinentes et non excessives au regard de chacune de ces deux finalités.

Si le système enregistre la conversation qui se déroule entre l'opérateur du service d'assistance et la personne qui appelle, c'est afin de disposer d'informations précises quant à la nature de l'incident signalé et de faciliter le travail du groupe de soutien spécialisé. Il traite ensuite les éléments d'identification des enregistrements (jour et heure précis, ainsi que numéro d'appel du système du service d'assistance et numéro associé du poste téléphonique de l'opérateur). Après sélection des échantillons dans la base de données, les conversations enregistrées sont écoutées lors de sessions de formation.

Pour ce qui est de la finalité consistant à résoudre un problème, le CEPD conclut que l'enregistrement du contenu exact et précis de la conversation répond à l'exigence prévue par le règlement quant à la qualité des données. En revanche, collecter des données à caractère personnel en enregistrant chacune des conversations entre les opérateurs et les personnes qui appellent est largement excessif au regard de la finalité que sont le contrôle de la qualité et la formation.

Le groupe de l'article 29 sur la protection des données a rappelé le sens du principe de proportionnalité dans son document de travail "concernant la surveillance des communications électroniques sur le lieu de travail" [11]: "*le principe de proportionnalité exclut (…) toute surveillance générale (…). Lorsqu'une solution impliquant une intrusion moindre dans la vie privée des salariés permet d'atteindre l'objectif identifié, l'employeur devrait envisager de la mettre en œuvre (il devrait notamment éviter les systèmes effectuant une surveillance automatique en continu)*". Il a aussi insisté sur le fait que "*des systèmes de traitement des communications électroniques devraient être mis sur pied pour limiter au strict minimum la quantité de données personnelles traitées*" [12]. Même si ces principes ont été énoncés dans le cadre de l'application de la directive 95/46/CE et portent sur la surveillance générale des courriels personnels de l'ensemble du personnel et de l'utilisation faite par celui-ci de l'Internet, le CEPD estime qu'ils s'appliquent en l'espèce.

---

[11] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_fr.pdf (adopté le 29 mai 2002).

[12] Bien que décrit à propos de la surveillance des communications électroniques sur le lieu de travail dans le contexte de la directive 95/46/CE, le CEPD estime que le principe de proportionnalité s'applique aussi en l'espèce.

La "surveillance générale" (blanket monitoring) des appels reçus par le service d'assistance pour atteindre la deuxième finalité ne limite pas au strict minimum la collecte des données, parce qu'elle vise à engranger une grande quantité d'échantillons potentiels qui comportent des données à caractère personnel. Elle ne respecte donc pas l'exigence propre à la qualité des données prévue par le règlement. (Pour se conformer au règlement, voir infra la partie consacrée à l'anonymat dans la section "Conservation des données").

En ce qui concerne l'utilisation à des fins de formation d'enregistrements sélectionnés, le CEPD ne peut souscrire au point de vue du responsable du traitement selon lequel la suppression de certaines parties de la conversation risque de nuire à la compréhension du contenu, ce qui compromettrait la première finalité du système. Une fois que le problème informatique signalé au service d'assistance a été résolu, les enregistrements devraient en principe être effacés dans un délai très court (voir la section "Conservation des données"). Il est possible de sélectionner des échantillons pour la formation dans ce bref délai. Le responsable du traitement dispose d'une marge de manœuvre pour décider soit de rendre les enregistrements anonymes - les personnes concernées n'étant alors plus identifiables, les principes de la protection des données ne s'appliquent pas - soit d'utiliser les enregistrements lors de formations après avoir obtenu le consentement des personnes concernées - auquel cas les données à caractère personnel inutiles au regard de la finalité qu'est la formation devraient être supprimées du dialogue qui sera écouté dans ce contexte.

En outre, les données doivent être exactes et mises à jour (article 4, paragraphe 1, point d), du règlement). L'enregistrement direct des communications garantit l'exactitude des données contenues dans les enregistrements vocaux. L'exactitude des données est aussi assurée en donnant aux personnes concernées un droit de rectification (voir la section 2.2.7, "Droit d'accès et de rectification").

2.2.5 Conservation des données et verrouillage 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 (…) 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).

Les données de contenu sont enregistrées par le système. Le CEPD fait observer que, pour se conformer au point e) précité, il convient de ne conserver les dialogues que jusqu'à la disparition du problème informatique signalé par l'utilisateur. Une fois fournie l'aide informatique demandée, les enregistrements devraient être effacés le plus vite possible; en d'autres termes, la durée de conservation devrait être courte: cinq jours ouvrables au maximum.

Si le responsable du traitement décide d'utiliser les enregistrements pour une autre finalité que le règlement d'un problème informatique, à savoir à des fins de contrôle de la qualité et de formation, il devrait choisir soit de rendre les données à caractère personnel anonymes, soit de les conserver sous une forme qui n'est pas anonyme (avec les garanties énoncées dans le présent avis). Sélectionner les enregistrements et les rendre anonymes ne peut se faire que pendant la courte durée de conservation des données définie dans le cadre de la première finalité du système (soit cinq jours ouvrables au maximum).

Quant à la première possibilité, précisons que rendre les enregistrements anonymes, tant en ce qui concerne les personnes qui appellent que les opérateurs, est une exigence fondamentale de l'article 4, paragraphe 1, point e), du règlement. Il s'agit aussi d'une garantie prévue par le point b), qui exige que le responsable du traitement prévoie des garanties appropriées afin de veiller, en particulier, à ce que les données ne soient pas utilisées à l'appui de dispositions ou décisions concernant une personne en particulier. L'anonymat est spécialement important dans le contexte de la formation: s'il est possible d'identifier la voix des opérateurs dans les enregistrements présentés en tant qu'échantillons, les personnes formées risquent de reconnaître la voix de leurs collègues et former des jugements subjectifs sur leur compétence, leur efficacité et leur comportement professionnel.

Conserver les données pendant six mois dans le but de disposer de suffisamment de dialogues pour la formation, comme l'envisage le responsable du traitement, constitue une violation de l'article 4, paragraphe 1, point e), du règlement.

Pour conserver des données sous une forme qui n'est pas anonyme au-delà de la période maximum de cinq jours ouvrables (qui permet de procéder à une sélection des enregistrements) dans le but d'utiliser les dialogues pour une formation, il faut obtenir le consentement des personnes concernées (voir la section 2.2.2, "Licéité du traitement").

Comme indiqué plus haut dans la section consacrée aux faits, le recours à deux systèmes parallèles permet l'identification des conversations qui ont eu lieu entre les opérateurs et les clients: le NCFS enregistre les conversations, et un système créant des dossiers d'incidents (Peregrine) est utilisé parallèlement. Quand un utilisateur appelle, l'incident est signalé dans Peregrine, où il est soit réglé, soit transmis à d'autres groupes de soutien. Les informations conservées dans Peregrine sont l'estampille temporelle et le nom de l'opérateur. Elles peuvent être associées aux informations fournies par le NCFS pour permettre d'identifier les conversations entre les opérateurs et les clients. Le numéro de canal (lié au téléphone de l'opérateur) et l'estampille temporelle sont les seules informations disponibles lorsqu'on fait une recherche pour obtenir une liste des conversations, avec leur durée, enregistrées pendant une certaine période, et ce pour les numéros de canal indiqués. Ces éléments permettent d'identifier l'appel lui-même, ainsi que l'opérateur et la personne qui a appelé.

Au regard de la première finalité du système, il est essentiel d'identifier l'appel et d'utiliser le contenu du dialogue, si nécessaire en remontant à la source et en vérifiant l'information, pour résoudre le problème informatique signalé. La même courte période de conservation des données s'applique aux éléments d'identification des appels, qui ne devraient donc pas être conservés plus de cinq jours ouvrables. Comme indiqué plus haut, on peut, dans la perspective de la seconde finalité des enregistrements, utiliser pendant ce délai les éléments d'identification afin de sélectionner les dialogues devant servir en formation et obtenir le consentement tant des personnes ayant appelé que des opérateurs. Cela fait, les éléments susceptibles de permettre l'identification des personnes concernées doivent être rendus anonymes ou effacés (par exemple, le numéro de canal associé au téléphone de l'opérateur).

L'article 15 du règlement prévoit que la personne concernée a le droit d'obtenir du responsable du traitement le verrouillage des données dans certains cas précis. Le responsable du traitement a prévu que la durée de ce verrouillage, accordé sur la base d'une demande légitime motivée des personnes concernées, serait de quatre mois - les utilisateurs étant ainsi assurés de pouvoir demander le verrouillage s'ils le souhaitent. Les périodes de vacances, les maladies, les missions et autres formes d'absences ont été prises en compte, de sorte que ce délai permettrait au responsable du traitement d'intervenir avant que les mécanismes automatiques liés à durée maximale de conservation (six mois) n'effacent les enregistrements.

Une demande de verrouillage de données à caractère personnel ne peut être présentée que lorsque les données sont conservées sous une forme permettant l'identification de la personne concernée (c'est-à-dire durant la période maximale de cinq jours de conservation des données ou si les enregistrements sont sélectionnés et utilisés lors d'une formation sous une forme qui n'est pas anonyme). Au lieu de fixer une durée de verrouillage uniforme de quatre mois, le CEPD recommande de faire correspondre cette durée au motif particulier (tel que prévu par l'article 15) sous-tendant la demande: conserver des preuves, traitement illicite (par exemple, quand l'opérateur n' pas consenti à l'utilisation de l'enregistrement pour une formation et exige le verrouillage plutôt que l'effacement), etc.

2.2.6 Transfert des données

Les données à caractère personnel sont transférées entre les institutions ou organes communautaires ou en leur sein si elles sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire. Le destinataire traite les données à caractère personnel uniquement aux fins qui ont motivé leur transmission (article 7, paragraphes 1 et 3, du règlement).

Les données à caractère personnel figurant dans les enregistrements et s'y rapportant sont transférées aux administrateurs locaux du système, au chef d'équipe du service d'assistance, au responsable du soutien à l'utilisateur, au responsable du traitement et à son adjoint, et aux personnes qui suivant une formation. Le système devrait garantir que seules reçoivent ces données les personnes pour lesquelles elles sont *nécessaires* à l'exécution de leurs missions. Il faudrait définir clairement en les distinguant les personnes qui peuvent être destinataires de données à caractère personnel compte tenu de la finalité qu'est la résolution d'un problème et celles qui peuvent en recevoir (si les dialogues ne sont pas rendus anonymes) compte tenu de la finalité que constituent le contrôle de la qualité et la formation (voir aussi la section 2.2.5 supra).

Selon la notification en vue du contrôle préalable, des données peuvent aussi être transférées à l'IDOC [13], la DG ADMIN/DS (direction de la sécurité), l'OLAF [14], la DG Contrôle financier [15], au médiateur, au DPD et au CEPD. Ces transferts peuvent avoir lieu s'ils sont "nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire", qui détermine la nécessité dans le contexte de l'enquête.

2.2.7 Droit d'accès et droit à la rectification

Selon l'article 13 du règlement, "*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: a) la confirmation que des données la concernant sont ou ne sont pas traitées; b) des informations au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées; c) 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 (…)*".

Les personnes concernées devraient être à même d'exercer leurs droits chaque fois que des données sont identifiables.

L'article 14 énonce dans les termes suivants le droit de rectifier des données à caractère personnel: "*La personne concernée a le droit d'obtenir du responsable du traitement la rectification sans délai de données à caractère personnel inexactes ou incomplètes*". Pour autant qu'une rectification puisse

---

[13] Voir l'avis du 20 avril 2005 sur la notification en vue d'un contrôle préalable à propos du dossier "Enquêtes administratives et procédures disciplinaires internes de la Commission européenne" - IDOC (dossier 2004-187). Disponible sur http://www.edps.europa.eu.

[14] Voir l'avis du 23 juin 2006 sur la notification en vue d'un contrôle préalable à propos des enquêtes internes effectuées par l'OLAF (dossier 2005-418).

[15] Le CEPD procède actuellement à un contrôle préalable du "Processus d'audit interne" (dossier 2006-298).

se faire dans un système d'enregistrement vocal, qui enregistre précisément l'information en cause, les personnes concernées devraient être mises en mesure d'exercer ce droit : elles pourraient demander de supprimer, de modifier ou de corriger leurs données à caractère personnel en envoyant un courriel explicite à l'adresse du service d'assistance de la DG INFSO. Dans le système actuel, la demande de correction est enregistrée par le biais de l'enregistrement d'une nouvelle conversation, en identifiant clairement l'enregistrement à corriger. Bien qu'il ne s'agisse pas d'une solution facile pour l'utilisateur, on peut considérer la procédure comme appropriée, à condition qu'elle soit assortie de règles claires prévoyant que la deuxième conversation demandant la correction du dialogue antérieur ne peut être conservée plus longtemps que l'enregistrement corrigé.

Le système permet que chaque personne qui est clairement identifiée au moyen du contenu puisse obtenir une copie de l'enregistrement de sa conversation avec le service d'assistance informatique de la DG INFSO en envoyant un courriel à cette fin à l'adresse du service. Par le biais de la même procédure, les personnes concernées peuvent vérifier quelles sont leurs données à caractère personnel qui sont conservées par le responsable du traitement. Le CEPD estime que cette procédure convient, tout en soulignant que le droit d'accès à ses données à caractère personnel, y compris celui d'obtenir une copie du dialogue, devrait aussi être accordé aux opérateurs du service d'assistance informatique. Ceux-ci devraient être informés de la procédure à suivre pour accéder à leurs données à caractère personnel.

2.2.8 Information de la personne concernée

Le règlement prévoit que les données à caractère personnel doivent être traitées "loyalement et licitement" (article 4, paragraphe 1, point a)). Pour être loyal, le traitement ne peut se faire de façon cachée. En pratique, ce principe est mis en œuvre par le biais de l'obligation de donner certaines informations à la personne concernée conformément aux articles 11 et 12. L'article 11 énumère une série d'informations que le responsable du traitement doit fournir à la personne concernée lorsque les données sont collectées auprès de celle-ci; l'article 12 précise les informations à fournir lorsque les données n'ont pas été collectées auprès de la personne concernée.

En l'espèce, les données sont collectées auprès des personnes concernées. Le responsable du traitement leur fournit les informations exigées à l'article 11 dans les divers documents et sources d'informations. Le CEPD se félicite de ce que, outre les informations générales énoncées à l'article 11, le responsable du traitement fournisse aussi des informations sur la base juridique, les durées de conservation des données et le droit de saisir le CEPD. Ces informations sont nécessaires pour des raisons de loyauté envers la personne concernée, compte tenu de la nature plus délicate des traitements. Le CEPD demande cependant que trois corrections soient apportées dans la déclaration de confidentialité: 1) la durée de conservation des données devrait être modifiée pour l'aligner sur le présent avis; 2) la phrase sur le droit de saisir le CEPD devrait être harmonisée avec celle de l'article 11 du règlement (indiquer expressément que les personnes concernées peuvent saisir le CEPD "à tout moment"); 3) il y est indiqué, dans la partie "données d'identification", que "*parmi les autres informations pouvant être enregistrées dans le cadre d'une conversation figurent entre autres vos nom, prénom, titre, unité, numéro de fax, adresse électronique et adresse. Ces données ne feront néanmoins l'objet d'aucun traitement et ne seront utilisées qu'en vue du contrôle de la qualité de l'opération et de l'amélioration des activités du service d'assistance informatique de la DG INFSO*" (traduction non officielle). Il faudrait corriger ce passage de sorte qu'il soit clair pour les personnes concernées que le système traite leurs données à caractère personnel en vue de la finalité qu'est la vérification des informations afin de résoudre l'incident et, si les données ne sont pas rendues anonymes, également en vue de la finalité que constituent le contrôle de la qualité et la formation.

Si les données à caractère personnel ne sont pas rendues anonymes pour la finalité que constituent le contrôle de la qualité et la formation, il faut, pour garantir un traitement loyal à l'égard des personnes concernées, demander le consentement de ces dernières à leur traitement. Donner des informations plus précises dans le message vocal d'accueil transmis au début de chaque appel est

une condition indispensable d'un consentement informé. Dans sa conception actuelle, le système va diffuser le message suivant: "*Bienvenue au service d'assistance informatique de la DG INFSO. La présente conversation est enregistrée à des fins de contrôle de la qualité* (traduction non officielle)". Pour donner des informations plus précises quant à ce qui est visé par les termes "à des fins de contrôle de la qualité", il faudrait que le message soit rédigé comme suit: "*Bienvenue au service d'assistance informatique de la DG INFSO. La présente conversation est enregistrée pour que nous soyons certains de disposer des informations exactes sur l'incident que vous signalez. Elle sera effacée lorsque l'incident sera réglé, et au plus tard cinq jours ouvrables après l'enregistrement.*"

Si le responsable du traitement devait décider de ne pas rendre les enregistrements anonymes, les opérateurs pourraient demander, à la fin de chaque enregistrement: "Consentez-vous à ce que cet enregistrement soit utilisé à des fins de formation?" (voir aussi la section 2.2.2 supra). Si le responsable du traitement trouve cette solution difficile, il peut demander ce consentement par d'autres moyens (par exemple, en rappelant la personne à cette fin). De toute façon, les personnes concernées devraient être informées de l'éventualité que leur consentement soit demandé, ainsi que des détails du système auquel elles consentent.

Les opérateurs du service d'assistance devraient recevoir des informations précises sur le fait qu'ils peuvent s'opposer globalement à l'utilisation des enregistrements, et aussi en particulier à l'utilisation de l'enregistrement de leurs dialogues. Ils devraient aussi être informés des modalités de la procédure leur permettant d'exercer ce droit.

2.2.9 Mesures de sécurité

À l'issue d'un examen attentif des mesures de sécurité qui ont été adoptées, le CEPD estime que celles-ci sont suffisantes au regard des articles 22 et 35 du règlement.

Conclusions

Certains éléments du traitement ne respectent pas les principes de nécessité et de proportionnalité et violent les dispositions du règlement relatives à la qualité des données et à la conservation des données. Le CEPD recommande que les considérations qui précèdent soient prises en compte pour assurer le respect du règlement, et en particulier les point suivants:

- les dialogues enregistrés peuvent être utilisés à des fins de formation soit en rendant les données à caractère personnel anonymes, soit en obtenant le consentement des personnes qui appellent et des opérateurs;
- les personnes concernées devraient être informées sur le fonctionnement du système en général et sur certains de ses détails avant de consentir au traitement de leurs données;
- le message d'accueil devrait donner des informations plus claires sur la finalité qu'est le contrôle de la qualité et sur la courte période de conservation des données;
- le responsable du traitement devrait envisager le recours à des moyens moins envahissants pour atteindre la finalité qu'est la formation;
- il faudrait que les données à caractère personnel non nécessaires au regard de la finalité qu'est la formation soient effacées;

- une fois fournie l'assistance informatique demandée, il faudrait effacer le plus vite possible les enregistrements et leurs éléments d'identification; en d'autres termes, la période de conservation devrait être courte, soit cinq jours ouvrables au maximum;
- la sélection des enregistrements à des fins de formation ne peut se faire que si des données sont conservées dans le système en vue de la première finalité (cinq jours ouvrables au maximum);
- il faut obtenir le consentement des personnes concernées pour conserver au-delà du délai de cinq jours ouvrables, à des fins de formation, des données qui n'ont pas été rendues anonymes;
- la période de verrouillage devrait correspondre au motif particulier pour lequel une demande de verrouillage a été présentée;
- il faudrait définir clairement, en les distinguant, les personnes susceptibles d'être les destinataires de données à caractère personnel lorsqu'il s'agit d'informations de vérification enregistrées afin de régler l'incident et les personnes susceptibles de recevoir des données à caractère personnel (si les dialogues ne sont pas rendus anonymes) compte tenu de la finalité que constituent le contrôle de la qualité et la formation;
- si des informations sont rectifiées par le biais d'un nouvel enregistrement, la période de conservation de ce dernier ne devrait pas être plus longue que celle de l'enregistrement originel qui a été corrigé;
- les opérateurs devraient bénéficier du droit d'accès aux données;
- il faudrait corriger les informations figurant dans la déclaration de confidentialité;
- les opérateurs du service d'assistance devraient être avertis de façon précise qu'ils ont la possibilité de s'opposer globalement à l'utilisation des enregistrements, ainsi qu'en particulier à l'utilisation de leurs dialogues. Ils devraient aussi être mis au courant des modalités de la procédure leur permettant d'exercer ce droit.

Fait à Bruxelles le 23 octobre 2006.

Peter HUSTINX
Contrôleur européen de la protection des données