Avis sur la notification d'un contrôle préalable reçue du Délégué à la protection des données du Conseil de l'Union européenne à propos du dossier "Enregistrement des communications effectuées sur les lignes téléphoniques du Centre de Sécurité, les interphones du bâtiment et les radios utilisées par les services du Secrétariat Général du Conseil (SGC) Sécurité, Prévention et Médical "

Bruxelles, le 23 janvier 2006 (Dossier 2005-364)

1. Procédure

1.1. Le 23 Novembre 2005, le Contrôleur Européen de la Protection des données (CEPD) a reçu une notification pour contrôle préalable en vertu de l'article 27 du Règlement (CE) 45/2001 (ci-après "le Règlement") du délégué à la protection des données du Conseil de l'Union européenne (DPD). Cette notification concerne l'enregistrement des communications effectuées sur les lignes téléphoniques du Centre de Sécurité (CdS), les interphones du bâtiment et les radios utilisées par les services du Secrétariat Général du Conseil (SGC) Sécurité, Prévention et Médical.

1.2. Cette notification fait suite à une consultation du DPD par téléphone et par courrier électronique sur la nécessité d'un contrôle préalable auprès du CEPD.

1.3. La notification est accompagnée de la Décision 198/03 du Secrétaire Général concernant les tâches du Centre de Sécurité; d'une note au personnel du 18.11.2005 (195/05) sur les appels d'urgence au Centre de Sécurité et des consignes sur l'enregistrement des communications effectuées sur les lignes de communication du Centre de Sécurité.

1.4. Le 14 décembre 2005, le CEPD a fait une demande d'information auprès du responsable du traitement. Cette information a été fournie le jour même. Des informations supplémentaires ont également été demandées le 16 janvier 2006 avec réponse le jour même.

2. Examen de l'affaire

2.1. Les faits

Tous les appels vers le numéro XXXX, aux numéros du dispatching du Centre de sécurité (CDS) (XX, XX, XX et XX XX XX) et via interphone sont enregistrés par le CDS qui opère 24 heures sur 24, 7 jours sur 7 en tant que mission du Bureau de la Sécurité (BdS) telle qu'établi par la Décision 198/03 du Secrétaire Général/Haut Représentant. Il en va de même pour toutes les liaisons radios propres aux services SGC chargés de la sécurité, de la prévention et de l'assistance.

Toute personne témoin d'un accident ou incident qui présente un danger pour des personnes ou des biens, doit le notifier immédiatement en appelant un numéro de téléphone unique (le XX), ou dans les ascenseurs ou parkings, en se servant de l'interphone d'urgence.

Il ne peut être exclus que des personnes externes au personnel du SGC utilisent les numéros mis à disposition ou les moyens disponibles à des fins d'urgence (l'interphone, par exemple).

Lors de l'appel, les personnes doivent mentionner leur nom, leur situation (bâtiment, étage, ascenseur, salle...), et le motif de leur appel. Selon la nature de l'incident, le responsable de la sécurité notifie immédiatement le service d'urgence adéquat (par exemple, le service médical, l'ambulance, les pompiers, la police) et envoi une équipe de première urgence sur place.

Les fonctionnaires de rang A* ou B* de permanence dans le service de sécurité interne ainsi que le directeur du service de sécurité peuvent écouter les communications enregistrées lorsque cela s'avère nécessaire afin de

- déterminer le cours exact des faits et de conversations en cas de contestation sur la nature et le contenu d'un appel;
- permettre l'analyse des appels prévenant de menaces;
- vérifier que les règles internes du Bureau de Sécurité sont respectées ("vérifier la correcte application des instructions"). Ces règles/consignes/instructions gèrent l'activité des agents du Bureau de Sécurité et des gardiens qui les supportent dans leur tâche.

En cas d'extrême urgence suite à un danger immédiat ou à la demande des services de police[1], c'est la personne de garde du service de sécurité qui avise le responsable A* ou B* de garde. En attente de l'arrivée du responsable précité, il écoutera la bande et le texte intégral de l'enregistrement concerné sera transcrit immédiatement. Toute intervention fera l'objet d'une inscription dans le logbook CDS.

A ces fins les bandes magnétiques contenant les enregistrements sont conservées pendant six mois.

Lorsque l'immunité est levé dans le cadre d'une enquête judiciaire ou un flagrant délit le Secrétaire Général Adjoint peut donner son accord à ce que les données soient être partagées avec les autorités judiciaires belges.

Toute personne concernée par ces traitements de données (fonctionnaire, agent ou autre) dispose d'un droit d'accès aux données qui la concerne. Ces droits peuvent être exercés en présentant une demande écrite au responsable du BdS.

Les personnes sont informées de la procédure de manière générale dans une communication au personnel du 18.11.2005 (195/05). En cas d'écoute des enregistrements, les parties en cause seront avisées dès que possible afin de garantir leurs droits et libertés.

Les bandes magnétiques sont stockées dans un coffre fort dans un local sécurisé situé dans une zone sécurisée. Un registre dans lequel sont répertoriés les changements de bande se trouve dans ce même coffre.

[1] Les services de police peuvent avoir accès qux données lorsque le Secrétaire Général Adjoint leur en autorise dans le cadre d'une enquête judiciaire du pays hôte ou un flagrant délit.

2.2. Les aspects légaux

2.2.1. Contrôle préalable

Le règlement 45/2001 s'applique au traitement de données à caractère personnel par toutes les institutions et organes communautaires, dans la mesure où le traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire. Nous sommes ici en présence d'un traitement de données par le Secrétariat Général du Conseil, à savoir une institution communautaire, et d'un traitement dans le cadre d'activités qui relèvent d'activités du premier pilier et donc du champ d'application communautaire.

Le règlement 45/2001 s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

Nous sommes en présence ici d'un traitement de données personnelles puisqu'il s'agit de l'enregistrement de communications entre deux personnes identifiées ou identifiables[2]. L'enregistrement est automatisé. En cas de mise en œuvre de la procédure d'urgence ou de vérification, une partie des communications est transcrite ce qui équivaut à un traitement manuel puisque les données seront reprises dans un fichier.

L'article 27 §1 du règlement (CE) 45/2001 soumet au 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 confidentialité des communications est tellement sensible, qu'elle fait l'objet d'une disposition spécifique dans le règlement (article 36). A ce titre, l'on peut considérer qu'il existe un risque tel que visé à l'article 27 §1 du règlement.

Par ailleurs, l'article 27§2 du règlement contient une liste des traitements susceptibles de présenter de tels risques. L'article 27§2 sous b) prévoit que sont soumis à un contrôle préalable les traitements destinés à évaluer des aspects de la personnalité des personnes concernées tels que leur compétence, leur rendement ou leur comportement. Une des finalités identifiées en ce qui concerne l'enregistrement des conversations est de vérifier que les règles internes du Bureau de Sécurité sont respectées plus précisément de vérifier que les personnes chargées de la sécurité ont œuvré selon les règles. Le traitement est donc destiné, ne fût-ce que partiellement, à évaluer la conduite de certaines personnes. Il pourrait également conduire à l'adoption de mesures disciplinaires. Pour ces raisons le traitement doit faire l'objet d'un contrôle préalable.

En principe, le contrôle effectué par le Contrôleur européen de la protection des données est préalable à la mise en place du traitement. Dans ce cas, en raison de la nomination du Contrôleur européen à la protection des données, qui est postérieure à la mise en place du système, le contrôle devient par la force des choses ex-post. Ceci n'enlève rien à la mise en place souhaitable des recommandations présentées par le Contrôleur européen à la protection des données.

Comme il a été mentionné, toute intervention fera l'objet d'une inscription dans le logbook CDS. Le présent contrôle préalable ne vise pas l'analyse du traitement des données dans le cadre de ce logbook mais seulement en ce qui concerne ce traitement particulier.

[2] La personne appelante est censée s'identifier au début de l'appel. La personne recevant l'appel est identifiée comme étant la personne de service au moment de l'appel.

La notification du DPD a été reçue le 23 novembre 2005. Conformément à l'article 27(4), le présent avis doit être rendu dans les deux mois qui suivent. Le contrôleur rendra donc son avis au plus tard le 24 janvier 2005.

2.2.2. Base légale et licéité du traitement

La Décision du Conseil du 22 Mars 2004 portant adoption de son règlement intérieur prévoit en son article 23 que le Conseil décide de l'organisation de son secrétariat général. Sur cette base, le Secrétaire Général du Conseil a adopté une décision concernant les tâches du Bureau de Sécurité (décision 198/03). Le préambule de cette décision mentionne: "Il est nécessaire d'assurer efficacement la sécurité du Conseil et de ses instances, de leurs activités, du personnel et des visiteurs du Conseil, de ses bâtiments et des biens et ressources qu'ils renferment, ainsi que des informations confidentielles, sensibles et classifiées qui circulent en son sein, conformément aux dispositions du Statut et autres règles de droit applicables". Cette décision prévoit qu'il appartient au Bureau de Sécurité d'assurer cette protection (article 2§1). A ce titre le Bureau de Sécurité peut, avec l'autorisation du Secrétaire Général ou du Secrétaire Général adjoint, en cas d'extrême urgence, avoir accès à tous les documents et informations nécessaires dans le cadre de l'enquête (article 6§1). Par ailleurs le Bureau de Sécurité est chargé de gérer un Centre de Sécurité et de faire face aux urgences en cas d'alerte, d'incident ou d'accident (article 9§1).

L'analyse de la base légale s'accompagne de l'analyse de la licéité du traitement telle que définie à l'article 5 du règlement (CE) 45/2001. L'article 5(a) prévoit que le traitement de données à caractère personnel ne peut que être effectué si le traitement est "nécessaire à l'exécution d'une mission relevant 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". La base légale relevant des dispositions ci-dessus mentionnées, vient à l'appui de la licéité du traitement.

2.2.3. Traitement portant sur des catégories particulières de données

Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé ou à la vie sexuelle sont interdits à moins que des bases soient trouvées au sein de l'articles 10§2.

Des informations relatives à l'état de santé d'une personne peuvent figurer dans l'enregistrement d'appels d'urgence dans la mesure où certains appels portent précisément sur des appels pour urgence médicale. Dans ce cas, le traitement peut être considéré comme étant autorisé par l'article 10§2 sous b) qui permet le traitement de données sensibles lorsque le traitement est nécessaire afin de respecter les obligations et droits spécifiques du responsable du traitement en matière de droit du travail dans la mesure où il est autorisé par les traités instituant les Communautés européennes ou d'autres actes législatifs adoptées sur la base des traités.

Par ailleurs, l'article 10§2 sous c) permet également le traitement de ces données lorsque nécessaire à la sauvegarde d'intérêts vitaux de la personne concernée ou d'une autre personne lorsque celle-ci est dans l'incapacité de donner son consentement. Cette disposition sert à justifier le traitement des données sensibles relatives à des personnes externes au Conseil mais dont l'intérêt vital est en jeu.

2.2.4. Qualité des données

En vertu de l'article 4(1) sous c) du règlement "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". Par ailleurs elles doivent être "exactes et, si nécessaire, mises à jour" (article 4(1) sous d).

Les données, objet du présent contrôle préalable concernent l'entièreté des conversations vers le numéro XXXX, aux numéros du dispatching du Centre de sécurité (CDS), par liaisons radios propres aux services du SGC et via interphone sont enregistrés par le CdS. Il n'est pas raisonnable de procéder à une sélection des données au sein même de la conversation puisqu'à priori toutes les données sont pertinentes en vue des finalités poursuivies.

2.2.5. Conservation des données

Les données relatives aux conversations téléphoniques sont conservées pendant 6 mois.

En cas de traitement de ces données nécessaires pour une enquête de sécurité/administrative, elles seraient gardées jusqu'à aboutissement final de l'enquête et les possibles recours en justice.

Le règlement prévoit que les données sont "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§1 sous e)).

Par ailleurs, en vertu de l'article 37§1, les données de trafic, à savoir les données qui sont nécessaires afin d'établir les communications sont effacées ou rendues anonymes à la fin de la communication. Toutefois des exceptions à ce principe sont prévues par l'article 20 notamment lorsque cette exemption est nécessaire pour "assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales", "garantir la protection de la personne concernée" ou "assurer la sécurité nationale, la sécurité publique et la défense des Etats membres". Le CEPD interprète la disposition "assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales" à la lumière de sa *ratio legis* et dès lors comme s'appliquant également aux enquêtes disciplinaires[3]. Autant d'exceptions qui justifient dans le cas présent une conservation des données au-delà de la fin de la communication pendant une période de 6 mois ou au-delà en cas d'enquête.

Par ailleurs, l'article 37§2 permet la conservation des données aux fins de gestion du budget et du trafic, y compris la vérification de l'usage autorisé des systèmes de télécommunications, pendant un délai de maximum 6 mois après la collecte à moins que la conservation soit nécessaire à la constatation, à l'exercice ou à la défense d'un droit dans le cadre d'une action en justice en instance devant un tribunal. Cette disposition sert dès lors à couvrir la conservation au-delà des six mois en cas de recours en justice.

2.2.6. Transfert des données

En cas d'incident, les données enregistrées seront communiquées aux fonctionnaires de rang A* ou B* de permanence dans le service de sécurité interne ainsi qu'au directeur du service de sécurité.

[3] Voir l'avis du CEPD 2004-198 du 21 mars 2004.

En vertu de l'article 7 du règlement 45/2001, les données à caractère personnel ne peuvent faire l'objet d'un transfert au sein d'une institution que si elles sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire. Ceci est le cas puisque la consigne prise en matière d'écoute d'enregistrement CdS prise sur base de la décision 198/03 prévoit que c'est le responsable A* ou B* qui écoute la bande et qui, en cas d'urgence avise le directeur du DdS. Ces personnes devront dès lors avoir les moyens techniques de prendre connaissance des communications.

Lorsque l'immunité est levé dans le cadre d'une enquête judiciaire ou un flagrant délit le Secrétaire Général Adjoint peut donner son accord à ce que les données soient être partagées avec les autorités judiciaires belges. Dans ce cas l'article 8 est d'application puisqu'il s'applique aux transferts de données à caractère personnel à des destinataires autres que les institutions et organes communautaires et relevant de la directive 95/46/EC.

La directive 95/46/EC ne vise pas les activités judicaires. Toutefois, la loi belge du 8 décembre 1992 relative à la protection des données à caractère personnel, hormis l'exception de certains articles, est applicable aux autorités publiques en vue de l'exécution de leurs missions de police judiciaire (article 3§5 de la loi). L'article 8 du règlement est dès lors applicable. Il précise que le transfert ne peut avoir lieu que si le destinataire démontre que les données sont nécessaires à l'exécution d'une mission effectuée dans l'intérêt public ou relevant de l'exercice de l'autorité publique ce qui est le cas ici.

2.2.7. Confidentialité des données

En vertu de 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 de droit communautaire.

Cette obligation de confidentialité s'applique au contenu même d'une communication. Il interdit, en principe, toute interception ou enregistrement des communications. Toute restriction à ce principe devra se faire dans le respect des principes généraux de droit communautaire. Ce dernier concept se réfère à la notion de droits fondamentaux, tels qu'établis par la Convention Européenne des Droits de l'Homme.

En pratique cela implique que toute restriction à la confidentialité des données doit se faire en respectant les droits fondamentaux tels qu'établis dans la Convention. Toute restriction ne peut être faite que si elle est prévue par la loi et est nécessaire dans une société démocratique, notamment à des fins de sécurité nationale, sûreté publique, à la défense de l'ordre et à la prévention des infractions pénales ou à la protection des droits et libertés d'autrui.

Toute restriction au principe de confidentialité devra donc être examinée à la lumière de critères stricts et notamment de proportionnalité par rapport à des finalités précises.

Dans le cas présent, l'enregistrement des communications se faisant non pas à l'insu des personnes concernées et à des fins de sécurité nationale, sûreté publique, de défense de l'ordre ou à la prévention des infractions pénales, le CEPD estime qu'il n'y a pas de violation du principe de confidentialité pour autant que les données soient limitées à ce qui est strictement nécessaire.

L'on ne peut par ailleurs exclure que les enregistrements soient utilisés à des fins d'enquête disciplinaire. La référence dans l'article 36 au respect des principes généraux du droit communautaire, n'exclut pas cette utilisation pour autant que le principe de proportionnalité soit

respecté. Toute utilisation des enregistrements pour l'évaluation du personnel de sécurité de manière plus générale (en vue de la promotion, par exemple) irait au-delà de ce qui est permis.

Par ailleurs, puisque nous sommes ici en présence d'une exception au principe de confidentialité des données, il est important de souligner que la finalité de vérification que les règles internes du Bureau de Sécurité sont respectés, doit être interprété de manière stricte et ne peut servir pour vérifier la conduite des agents en général. Il doit s'agir d'une vérification par rapport aux consignes, règles écrites établies par le Bureau de Sécurité et accessibles au personnel de service.

2.2.8. Droit d'accès et de rectification

En vertu des articles 13 et 14 du règlement (CE) 45/2001, les personnes concernées disposent d'un droit d'accès et de rectification des données personnelles les concernant.

La décision du Conseil du 13 septembre 2004 portant adoption de dispositions d'application en ce qui concerne le règlement 45/2001 prévoit, en sa section 5, les modalités d'exercice des droits de la personne concernée. Par ailleurs, la consigne interne au service de sécurité pour les agents du Centre de Sécurité, prévoit que toute personne concernée par ces traitements de données (fonctionnaire, agent ou autre) dispose d'un droit d'accès aux données en présentant une demande écrite auprès du Responsable de Sécurité.

L'article 20 du règlement 45/2001 prévoit des restrictions au droit d'accès notamment si une telle mesure constitue une mesure nécessaire pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales. Cet article a été interprété par le CEPD comme permettant également des limitations dans le cadre d'enquêtes disciplinaires (voir l'avis 2004-0198). Il semble que l'usage de cette limitation pourrait être exercé dans certains cas en cas d'enquête sur base d'enregistrements CdS. Le CEPD souhaite souligner qu'une telle restriction doit être limitée aux fins de l'enquête et au temps nécessaire pour l'enquête.

2.2.9. Information des personnes concernées

En vertu de l'article 11 du règlement, tout traitement de données à caractère personnel implique que les personnes concernées soient suffisamment informées de ce traitement. Cette information doit normalement se faire au plus tard au moment de la collecte des données auprès de la personne concernée sauf si la personne concernée a déjà été informée.

La communication au personnel du 18/11/2005 (195/05) informe la personne sur l'identité du responsable du traitement; les finalités poursuivies; les personnes auxquels les données sont communiquées; les droits d'accès; la possibilité de saisir le Contrôleur européen de la protection des données; la durée de conservation des données.

Il ne peut être exclu que des personnes externes au personnel du SGC utilisent les numéros mis à disposition ou les moyens disponibles à des fins d'urgence tels que l'interphone. Dans le cas où ces communications seraient enregistrées, des moyens appropriés d'information des personnes externes doivent être mis en place.

2.2.10. Sécurité

L'article 22 du règlement prévoit que des mesures techniques et organisationnelles doivent être prises afin d'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.

Après une analyse attentive par le CEPD des mesures de sécurités adoptées, le CEPD considère que ces mesures sont adéquates à la lumière de l'article 22 du règlement (CE) 45/2001.

Conclusion

Le traitement proposé ne paraît pas entraîner de violations des dispositions du règlement (CE) 45/2001 pour autant qu'il soit tenu compte des observations faites ci-dessus. Cela implique, en particulier, que :

- la finalité de vérification de respect des règles internes du Bureau de Sécurité, doit être interprété de manière stricte et ne peut servir pour vérifier la conduite des agents en général. Il doit s'agir d'une vérification par rapport aux consignes, règles écrites établies par le Bureau de Sécurité et accessibles au personnel de service.

- la restriction éventuelle au droit d'accès soit limitée aux fins de l'enquête et au temps nécessaire pour l'enquête;

- dans le cas où les communications de personnes extérieures seraient enregistrées, des moyens appropriés d'information doivent être mis en place.

Fait à Bruxelles, le 23 janvier 2006

Peter HUSTINX
Le Contrôleur européen de la protection des données