Avis relatif à la notification en vue d'un contrôle préalable reçue du délégué à la protection des données de la Banque européenne d'investissement concernant l'enregistrement des conversations téléphoniques dans les salles de sécurité et au standard téléphonique

1. Procédure

Le 15 mars 2013, le contrôleur européen de la protection des données (**CEPD**) a reçu du délégué à la protection des données (**DPD**) de la Banque européenne d'investissement (**BEI**) une notification en vue d'un contrôle préalable concernant le traitement de données à caractère personnel dans le cadre de «l'enregistrement des conversations téléphoniques dans les salles de sécurité et au standard téléphonique», accompagnée des documents justificatifs.

Il a soumis des questions le 21 mars et le 5 avril 2013, auxquelles la BEI a fourni des réponses le 17 avril 2013, de même que des documents supplémentaires. Le projet d'avis a été transmis au DPD le 7 juin 2013 afin qu'il puisse formuler des commentaires et celui-ci a confirmé le 19 juin 2013 qu'il n'avait aucun commentaire à soumettre.

2. Les faits

Lorsque la BEI estime que son niveau d'alerte est «jaune»[1] ou plus élevé, elle peut décider d'enregistrer les appels entrants et sortants des salles de sécurité et du standard téléphonique. Cette décision est prise par son comité de crise[2] sur recommandation du responsable de la sécurité de la BEI. Elle est par la suite réévaluée chaque semaine. L'enregistrement est désactivé dès que possible par décision formelle du comité de crise.

Si la procédure est engagée, les appels seront enregistrés comme suit:

- les appels entrants du standard reçus durant les heures de bureau seront enregistrés jusqu'à leur transfert vers leur destinataire final;
- en dehors des heures de bureau, les appels entrants du standard seront transférés vers les salles de sécurité et enregistrés jusqu'à leur transfert vers leur destinataire final;
- les appels sortants directement effectués depuis le standard ou les salles de sécurité (uniquement en dehors des heures de bureau pour ces dernières) seront enregistrés dans leur intégralité.

[1] Les niveaux d'alerte sont les suivants:
a) blanc - niveau normal, aucun danger spécifique détecté;
b) jaune - réponse à des tensions ou à un sentiment de danger, préparation à une situation anormale;
c) orange - danger annoncé ou constaté;
d) rouge - informations spécifiques reçues concernant une forte probabilité de menace terroriste imminente.
En 2011 et 2012, le niveau d'alerte est constamment demeuré «blanc».

[2] Présidé par le directeur général de la direction Information et soutien à l'environnement de travail; le secrétaire général et les directeurs généraux concernés en sont membres.

En outre, l'heure, la date et la durée de l'appel, de même que les numéros de téléphone (si disponibles), seront sauvegardés. Les appelants ne sont pas avertis du fait que leur appel peut être enregistré.

Les enregistrements audio des appels et les données associées à ces derniers seront conservés pendant 30 jours, après quoi ils seront automatiquement supprimés, à moins qu'une prolongation de ce délai ne soit justifiée pour les besoins d'une enquête en cours. Pour ce type d'enquêtes, le réseau téléphonique est équipé d'une fonction qui permet l'exportation des enregistrements.

D'après la BEI, ceux-ci ne seront utilisés que pour analyser les menaces terroristes susceptibles de survenir, par exemple les menaces téléphoniques. Seul le responsable de la sécurité (ou son adjoint) peut obtenir les codes d'accès (à utilisation unique) auprès du département informatique, qui gère le réseau téléphonique de la BEI. Les données obtenues peuvent ensuite être transférées au comité de crise et, après accord de ce dernier et information du DPD, aux forces de police du Luxembourg.

Les personnes concernées seront informées de ces manipulations par un avis publié tant sur l'intranet que sur le site web de la BEI. Cet avis informe les personnes concernées qu'«en raison de menaces spécifiques pour la sécurité», les appels peuvent être enregistrés sans l'émission préalable d'un avertissement sonore; il contient les numéros de téléphone du bureau des services généraux et du responsable de la sécurité, qui peuvent être contactés pour plus de renseignements.

Si les personnes concernées sollicitent l'accès à leurs données à caractère personnel, cet accès peut leur être accordé sur autorisation du responsable de la sécurité, lequel devrait consulter le DPD avant de prendre sa décision. Les personnes concernées auront le droit de verrouiller l'accès aux enregistrements (à des fins de preuves) et d'obtenir leur effacement s'ils sont illicites. Les limitations définies à l'article 20 du règlement (CE) n° 45/2001 (ci-après le «règlement») peuvent s'appliquer.

Le responsable du traitement est la BEI; l'unité chargée du traitement est l'unité «Sécurité et services» au sein du département «Bâtiments et logistique» relevant de la direction «Information et soutien à l'environnement de travail».

3. Analyse juridique

3.1. Contrôle préalable

Le traitement de données à l'examen constitue un traitement de données à caractère personnel réalisé par un organe de l'Union dans le cadre de l'exercice d'activités qui relèvent du champ d'application du droit de l'Union. Il est automatisé. Dès lors, le règlement (CE) n° 45/2001 s'applique.

L'article 27, paragraphe 1, dudit règlement soumet au contrôle préalable du CEPD 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». Le paragraphe 2 contient une liste non exhaustive des traitements susceptibles de présenter de tels risques.

Le traitement de données à caractère personnel par des moyens de communication électronique suscite certaines préoccupations spécifiques; l'intégralité du chapitre IV du règlement est consacrée à la protection des données à caractère personnel dans ce contexte. L'article 36 établit le principe général de confidentialité des communications.

Le traitement à l'examen a pour finalité d'enregistrer le contenu des appels, et constitue dès lors un traitement susceptible de présenter des risques particuliers au regard des droits et libertés des personnes concernées.[3]
La notification mentionne également le traitement de données relatives à des «mesures de sûreté», qui sont l'une des catégories particulières de données nécessitant un contrôle préalable (article 27, paragraphe 2, point a)). Plus spécifiquement, il indique la raison pour laquelle le traitement doit être soumis au contrôle préalable, à savoir que les données collectées seront utilisées pour l'évaluation des menaces terroristes. Il convient de souligner que les «mesures de sûreté» définies à l'article 10, paragraphe 5, du règlement englobent la détention préventive, le gel des actifs ou des mesures similaires; cet article ne concerne pas toutes les collectes de données à des fins de sécurité. Il va sans dire que la grande majorité des appelants ne sera pas concernée par ce type de mesure.

Bien que l'article 27, paragraphe 2, point a), ne s'applique pas en l'espèce, le traitement est soumis au contrôle préalable prévu à l'article 27, paragraphe 1, susmentionné.

Étant donné que le contrôle préalable est destiné à évaluer des situations susceptibles de présenter certains risques, l'avis du CEPD doit être rendu avant le début du traitement.

Dans le présent cas, le CEPD a été informé de l'existence d'un traitement antérieur plus intrusif que le traitement notifié. Il a vivement enjoint la BEI de notifier ce traitement sans délai, et au plus tard le 15 mars 2013. La notification soumise présente d'importantes modifications par rapport au traitement précédent.

Elle a été reçue du DPD le 15 mars 2013. Conformément à l'article 27, paragraphe 4, le présent avis doit être rendu dans les deux mois qui suivent la réception de la notification. Lorsque le CEPD demande des informations supplémentaires au responsable du traitement, ce délai est suspendu jusqu'à la réception des réponses. Le présent dossier a été suspendu du 21 mars au 17 avril 2013 et du 7 au 19 juin 2013. Au total, il a été suspendu pendant 39 jours. Le CEPD rendra donc son avis au plus tard le 24 juin 2013.

3.2. Licéité du traitement

Le traitement de données à caractère personnel n'est autorisé que s'il est justifié au titre de l'article 5 du règlement. L'article 5, point a), concerne les traitements qui sont «nécessaire[s] 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». Le considérant 27 du règlement précise que «[l]e traitement de données à caractère personnel effectué pour l'exécution de missions d'intérêt public [...] comprend le traitement de données

[3] Voir par exemple les avis suivants relatifs au contrôle préalable par le CEPD: «Enregistrement de la ligne réservée aux appels relatifs aux urgences et à la sécurité à Bruxelles (n° 88888)», publié le 22 mai 2006; «recording of emergency phone calls at the JRC Ispra site» (enregistrement des appels téléphoniques d'urgence sur le site du Centre commun de recherche d'Ispra), publié le 13 octobre 2008; «Enregistrement de la ligne réservée aux appels au dispatching technique relatifs aux interventions dans les immeubles de la CE à Bruxelles (n° 55555)», publié le 19 novembre 2008.

à caractère personnel nécessaires pour la gestion et le fonctionnement de ces institutions et organes».

Dans certaines situations de crise ou à haut risque, il peut être nécessaire de prendre des précautions supplémentaires pour assurer le bon fonctionnement de la BEI. Les principales caractéristiques du traitement sont établies dans un document interne qui a été approuvé par le comité de direction de la BEI. Ce document énonce les finalités du traitement ainsi que les critères pour l'activation de l'enregistrement. Il ne contient aucune information sur les délais de conservation ni sur les destinataires externes potentiels.

Compte tenu du fait que l'enregistrement des appels constitue un acte portant atteinte à la vie privée, les règles devraient être clairement définies dans une base juridique. Il convient notamment d'établir clairement les responsabilités des différents acteurs, les délais de conservation et les destinataires (modifiés conformément à la recommandation formulée dans le présent avis). Le document présenté en tant que base juridique ne couvre pas tous ces aspects et devrait être modifié.

Recommandation: adopter une base juridique claire et complète pour l'enregistrement de ces appels.

3.3. Qualité des données

L'article 4, paragraphe 1, point c), du règlement établit le principe selon lequel 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.

La finalité du traitement est l'analyse des menaces terroristes susceptibles de survenir, notamment les menaces téléphoniques, qui sont explicitement mentionnées dans la notification.

Étant donné que la grande majorité des appels entrants et sortants ne seront pas concernés, un enregistrement général de tous les appels serait assurément disproportionné. L'approche choisie, à savoir n'enregistrer les appels que lorsque le niveau d'alerte est «jaune» ou plus élevé et que le comité de crise a pris la décision formelle de procéder à l'enregistrement, permet de restreindre le caractère intrusif du traitement ainsi que tout traitement inutile de données à caractère personnel. C'est un réel progrès par rapport à la pratique antérieure qui consistait à enregistrer systématiquement ces appels.

La notification fait spécifiquement référence aux menaces terroristes reçues par téléphone, qui, selon toute vraisemblance, devraient davantage concerner les appels entrants que les appels sortants.[4] Il en résulte que l'établissement d'une distinction entre les appels entrants et les appels sortants pourrait contribuer à réduire encore davantage toute collecte et conservation inutiles de données à caractère personnel.

Recommandation: déterminer si la finalité du traitement peut également être réalisée si seuls les appels entrants sont enregistrés.

[4] De plus, pour les appels sortants, le numéro composé serait de toute façon connu.

3.4. Conservation des données

Les enregistrements des appels entrants et sortants sont conservés pendant 30 jours si le système est activé. La finalité déclarée de ce délai est l'analyse des menaces terroristes potentielles.

L'article 4 du règlement énonce le principe selon lequel les données à caractère personnel doivent être conservées 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.

Pour évaluer la pertinence de ce délai de conservation, il peut être utile de la comparer avec les délais prévus pour les autres mesures de sûreté. Pour la surveillance par télévision en circuit fermé (CCTV) sur les sites des institutions et organes de l'Union européenne, le CEPD recommande un délai de conservation maximal de sept jours (à moins qu'une enquête ne soit ouverte).[5] Dans le cas à l'examen, ce délai semble suffisant pour évaluer la nécessité de transférer des enregistrements de menaces aux forces de police du Luxembourg.

Recommandation: réduire le délai de conservation à sept jours ou justifier le choix d'un délai plus long.

3.5. Transferts de données

Les enregistrements de données peuvent être transférés au comité de crise et, après accord de ce dernier et information du DPD, aux forces de police du Luxembourg.

Les transferts sont réglementés par les articles 7, 8 et 9 du règlement, selon que le destinataire est une institution ou un organe de l'Union européenne (article 7), relève de la législation nationale adoptée en application de la directive 95/46/CE (article 8) ou ne relève pas de la législation nationale adoptée en application de la directive 95/46/CE (article 9).

Pour les transferts au comité de crise, l'article 7 s'applique. En vertu de cet article, les données ne peuvent faire l'objet de transferts que 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 Le comité de crise est chargé d'assurer la continuité des activités de la BEI en situation de crise; les informations sur les menaces sont importantes pour la prise de décisions dans de telles situations. Ces transferts sont donc conformes à l'article 7.

Pour les transferts aux forces de police luxembourgeoises, l'article 8 s'applique. Bien que la directive 95/46/CE ne s'applique pas en tant que telle aux activités de la police, ses modalités d'application en vigueur au Luxembourg s'appliquent quant à elles aussi à ce secteur. L'article 3 de la loi luxembourgeoise du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, telle que modifiée (soulignement ajouté), dispose ce qui suit:

«Article 3. Champ d'application
(1) La présente loi s'applique:
[...]

[5] Les lignes directrices sont disponibles sur le site web du CEPD.

- au traitement de données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'État, même liées à un intérêt économique ou financier important de l'État, sans préjudice des dispositions spécifiques de droit national ou international régissant ces domaines.

(2) Est soumis à la présente loi:
(a) le traitement mis en œuvre par un responsable du traitement établi sur le territoire luxembourgeois; [...]»[6]

Lorsque les enregistrements contiennent des preuves de l'existence de menaces terroristes, les transferts de données aux forces de police luxembourgeoises peuvent être couverts par l'article 8, point a), du règlement, étant donné que ces données sont nécessaires à l'exécution de missions relevant de l'exercice de l'autorité publique, à savoir la réalisation d'enquêtes sur des actes criminels, et notamment des menaces terroristes. Ces transferts étant vraisemblablement effectués à l'initiative de la BEI, celle-ci devrait évaluer leur nécessité au cas par cas. D'après la notification, le comité de crise prend la décision de transférer ou non ces données. Il convient de s'assurer qu'il étudie chaque cas avant de prendre sa décision. L'évaluation réalisée devrait être détaillée dans un registre des transferts.

Recommandation: évaluer au cas par cas la nécessité de transférer les données aux forces de police luxembourgeoises et détailler cette évaluation dans un registre des transferts.

3.6. Droits d'accès et de rectification

Les personnes concernées ont le droit d'accéder à leurs données et d'obtenir la rectification de données inexactes (articles 13 et 14 du règlement). Ces droits peuvent être limités conformément à l'article 20; par exemple, l'article 20, paragraphe 1, point a), autorise l'application de limitations lorsqu'elles sont nécessaires pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales.

Selon la notification, *«les personnes concernées peuvent accéder aux enregistrements de leurs conversations sur autorisation du chef des services de sécurité de la Banque, lequel devrait consulter le DPD avant d'accorder une telle autorisation»*.

En tant que dérogation à la règle générale, l'article 20 devrait être lu dans un sens strict. Par conséquent, l'accès devrait être accordé de manière générale, à moins qu'il n'existe des raisons particulières d'invoquer une exception dans un cas spécifique. Le passage «sur autorisation du chef des services de sécurité de la Banque» devrait être lu dans ce sens.

3.7. Information des personnes concernées

En vertu des articles 11 et 12 du règlement, une série d'informations minimales doit être fournie aux personnes concernées, sauf si elles en sont déjà informées. L'article 11 concerne les situations dans lesquelles les données sont collectées auprès de la personne concernée, par exemple dans les formulaires de demande. L'article 12 concerne les situations dans lesquelles les données ne sont pas obtenues auprès de la personne concernée, à savoir lorsqu'il n'y a pas d'interactions entre la personne concernée et le responsable du traitement et la première n'a pas nécessairement conscience que des données la concernant sont collectées (par exemple

[6] Extrait du site web de l'Autorité pour la protection des données du Luxembourg: http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002mod_fr.pdf.

vidéosurveillance, premières phases d'enquêtes internes). Ces informations minimales comprennent dans tous les cas au moins l'identité du responsable du traitement, les finalités du traitement auquel les données sont destinées, les destinataires ou les catégories de destinataires des données, l'existence d'un droit d'accès aux données la concernant et de rectification de ces données, toute information supplémentaire nécessaire pour assurer un traitement loyal des données (par exemple la base juridique du traitement auquel les données sont destinées, les délais de conservation des données et le droit de saisir à tout moment le contrôleur européen de la protection des données). Des limitations peuvent être appliquées au titre de l'article 20 du règlement.

L'avis inclus dans la notification et à publier sur le site web de la BEI ne mentionne que la finalité du traitement, les grandes catégories de données concernées et les coordonnées pour l'obtention d'informations supplémentaires.

Que la situation à l'examen soit régie par l'article 11 ou 12, ces informations ne sont pas suffisantes.[7]

Il est à noter, par ailleurs, que bien que cet avis soit en théorie mis à la disposition de toutes les personnes concernées, cela ne suffit pas pour garantir une information adéquate. À moins que l'une des exceptions de l'article 20 du règlement ne puisse être dûment invoquée (par exemple assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales), la BEI devrait faire entendre un message automatique aux appelants pendant qu'ils attendent qu'un opérateur prenne leur appel. Ce message devrait contenir des informations générales sur l'existence d'un éventuel enregistrement ainsi que ses finalités.[8] Il ne devrait se faire entendre que lorsque l'enregistrement est activé.

L'avis devrait être modifié de manière à mentionner toutes les informations visées à l'article 11 du règlement.

Si pour le grand public, une déclaration de confidentialité générale publiée sur le site web de la BEI et un message aux appelants suffisent, le personnel du standard téléphonique et des salles de sécurité devrait recevoir des informations plus ciblées, étant donné qu'il est davantage concerné par ces traitements. À cette fin, l'avis reprenant les informations minimales pourrait également être envoyé au personnel concerné par courrier électronique ou d'autres mesures pourraient être prises pour s'assurer que le personnel est informé.

Recommandations: à moins que l'une des exceptions de l'article 20 du règlement ne puisse être dûment invoquée, les appelants devraient recevoir un bref message automatique les informant du traitement. L'avis devrait être modifié de manière à mentionner les informations obligatoires en vertu de l'article 11 du règlement. Le personnel du standard téléphonique et des salles de sécurité devrait recevoir des informations plus ciblées.

3.8. Mesures de sécurité

[...]

[7] Dans des cas similaires, le CEPD a estimé que l'article 11 s'appliquait si l'enregistrement était annoncé (voir les avis mentionnés dans les notes de bas de page 3 et 8).

[8] En adéquation avec les pratiques établies pour d'autres procédures impliquant l'enregistrement d'appels; voir, par exemple, l'avis du CEPD concernant un contrôle préalable intitulé «Enregistrement de la ligne réservée aux appels au dispatching technique relatifs aux interventions dans les immeubles de la CE à Bruxelles (n° 55555)», publié le 19 novembre 2008.

4. Conclusion:

Rien ne porte à croire que les dispositions du règlement (CE) n° 45/2001 ont été violées dans la mesure où les recommandations formulées dans le présent avis sont pleinement prises en considération.

Pour rappel, les recommandations émises sont les suivantes:

- adopter une base juridique claire et complète pour l'enregistrement de ces appels;
- déterminer si la finalité du traitement peut également être réalisée si seuls les appels entrants sont enregistrés;
- évaluer au cas par cas la nécessité de transférer les données aux forces de police luxembourgeoises et détailler cette évaluation dans un registre des transferts;
- réduire le délai de conservation à sept jours ou justifier le choix d'un délai plus long;
- modifier l'avis de manière à mentionner les informations obligatoires en vertu l'article 11 du règlement;
- fournir des informations plus ciblées au personnel du standard téléphonique et des salles de sécurité;
- à moins que l'une des exceptions de l'article 20 du règlement puisse être dûment invoquée, faire entendre aux appelants un bref message automatique les informant du traitement.

Fait à Bruxelles, le 20 juin 2013

(**signé**)

Giovanni Buttarelli
Contrôleur européen adjoint de la protection des données