Avis sur la notification d'un contrôle préalable reçue du DPD (délégué à la protection des données) de la Banque européenne d'investissement à propos du dossier "Register of telephone calls (téléphonie mobile)"

Bruxelles, le 15 mai 2012 (Dossier 2009-0704)

1. Procédure

Par lettre en date du 11 octobre 2006, le Délégué à la protection des données (DPD) de la Banque européenne d'investissement (BEI) a envoyé au Contrôleur européen de la protection des données (CEPD) une notification de contrôle préalable dans le sens de l'article 27.3 du règlement (CE) n°45/2001 (le règlement) concernant le dossier "recording of telephone calls, téléphonie mobile (2006-462)". Des informations sont demandées par courrier électronique en date du 27 octobre 2006. Une réponse est apportée par courrier le 28 novembre 2006. Une nouvelle demande d'information est adressée le 11 décembre 2006. La Banque a ensuite informé le CEPD que la politique pour l'utilisation des téléphones mobiles allait être modifiée. Le dossier est resté suspendu le temps de l'adoption des nouvelles règles transmises au CEPD par courrier électronique le 22 octobre 2009. Au vu des modifications et du temps écoulé depuis la première notification, le CEPD a décidé d'ouvrir un nouveau dossier (2009-704) remplaçant la notification 2006-462. Ce dossier a été suspendu pour informations complémentaires du 18 novembre au 9 décembre 2009 et ensuite du 11 décembre 2009 au 20 septembre 2011. Une réunion a également eu lieu le 16 septembre 2011 avec le DPD de la banque pour clarifier certains faits. Une seconde réunion s'est tenue le 26 avril 2012 afin de clarifier certains nouveaux éléments apparus dans le dossier.

2. Les faits

La BEI a mis en place un système de prêt de téléphones mobiles destiné au personnel pour lequel la nécessité de cet outil a été établie par la Banque qui, en sa qualité de responsable du traitement, est représentée par le département des Ressources humaines (l'entité organisationnelle responsable de la téléphonie mobile).

Le système de téléphonie mobile ne dispose pas de fonctionnalité permettant de distinguer à priori les appels privés des appels professionnels. La BEI a donc établi un dispositif permettant de faire le distinguo à posteriori et, de là, débiter les frais des appels privés des bulletins de salaires du personnel. De cette façon la Banque peut aussi disposer d'informations pertinentes sur les coûts téléphoniques professionnels mensuels.

La distinction des appels privés/professionnels est faite par "auto-déclarations" du personnel concerné. La Banque a édicté des règles d'utilisation des téléphones mobiles et développé les

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

contrôles appropriés pour leur respect, parmi lesquels la vérification de l'exactitude des auto-déclarations (note datée du 20 janvier 2009 au personnel titulaire d'un téléphone portable).
La BEI a délégué la gestion de la téléphonie mobile à la société LUXGSM S.A. Les données des appels téléphoniques sortants et entrants effectués ou reçus par l'ensemble des postes de téléphones mobiles munis d'abonnements au réseau LUXGSM sont collectées et stockées par la société LUXGSM. Ces données sont ensuite transférées à la BEI. Au sein de la BEI, le traitement des données est effectué par les gestionnaires de l'application PeopleSoft (dans laquelle les données sont traitées) dans le département Ressources Humaines. La maintenance technique de cette base de données est assurée par le département IT de la Banque.

Toute personne en possession d'un téléphone portable ou abonnement LUXGSM, attribué pour des raisons de service en prêt temporaire par la Banque, est donc concernée par le traitement.

Le traitement est automatisé.

Les données traitées par la BEI pour les appels entrant et sortant, professionnels et privés (Voice et Data, c'est à dire autant les données des appels que les données relatives à l'accès e-mail ou Internet par téléphone mobile) des téléphones mobiles sont celles nécessaires à la facturation (numéro identifiant, nom de l'agent, prénom de l'agent, code comptable, mois de facturation, prix, pays appelé, numéro appelant, date de l'appel, heure de l'appel, durée de l'appel, numéro appelé, connexion internet le cas échéant). L'opérateur LUXGSM maintient une liste des utilisateurs de téléphone mobile incluant les informations suivantes : numéro de téléphone, nom, prénom, numéro personnel, direction, centre de dépense, mot de passe, pukcode (le code nécessaire lorsque le pincode est oublié). Les données qui peuvent révéler du contenu (sites web visités, quantités de données transférées, durée moyenne des connexions, utilisation du Wifi, sms) sont traitées de façon agrégée. C'est à dire que l'utilisateur n'est identifié que dans le cas de suspicions d'utilisation contraire aux règles établies.

L'opérateur LUXGSM conserve la totalité des données relatives à la facturation pendant une période de 6 mois[1]. La BEI stocke les informations concernant les frais privés et professionnels des utilisateurs GSM dans le logiciel Peoplesoft et au Département IT depuis le mois d'avril 2004. La BEI est cependant en train de modifier les durées de conservation des données. Elle prévoit de stocker les informations concernant les frais privés et professionnels des utilisateurs GSM pour une durée de six mois seulement :

- dans le logiciel PeopleSoft, à partir de leur injection dans ce logiciel par le Département RH ;
- par le service Telecom du Département IT, à partir de leur réception à la Banque.
-

Certaines données de contenu sont conservées sous forme agrégée pour des finalités statistiques (quantités de données transférées, durée moyenne des connexions, etc.).

En cas de suspicion d'infraction aux règles d'utilisation, le délégué à la protection des données et l'inspection générale de la Banque peuvent être destinataires des données. Le service juridique en cas de litige peut également être destinataire.

La personne concernée est informée des règles d'utilisation des téléphones lors de sa demande d'attribution d'un téléphone portable par une déclaration relative à son utilisation (la

[1] La BEI a signé un avenant au contrat signé avec la société LUXGSM afin de modifier la durée de conservation des données. D'une année, la durée de conservation est passée à six mois, le 1er février 2010.

note du 20 janvier 2009 est annexée à la déclaration). La demande de téléphone mobile est assortie d'une déclaration ("application for a mobile phone and declaration regarding its use") qui doit être signée par le demandeur et remise au Service Telecom du Département IT, elle contient une série de règles sur l'utilisation du téléphone portable auxquelles l'utilisateur doit donc souscrire.

L'accès à la base de données PeopleSoft est sécurisé par mot de passe pour le personnel de la BEI. Le nombre de personnes ayant accès aux données est limité aux gestionnaires de l'application PeopleSoft du département RH et à certains gestionnaires du département IT.

La réalisation du traitement en sous-traitance par LUXGSM est régie par un contrat.

Procédure :

Plusieurs fois par mois, le Service Telecom du Département IT envoie à l'opérateur LUXGSM des versions actualisées de la liste nominative des personnes concernées ainsi que de la liste des téléphones prêtés avec les informations des utilisateurs (en fichiers Excel) afin que LUXGSM mette à jour sa propre base de données et puisse établir ses factures mensuelles. Au début du mois suivant, LUXGSM renvoie au gestionnaire du contrat un fichier complet contenant les montants totaux des appels par utilisateurs. Le gestionnaire du contrat vérifie le fichier qui est ensuite transmis au Service Gestion du Département RH pour l'injection dans le système PeopleSoft, accessible par les utilisateurs via My/HR pour leur permettre de valider le montant de leurs frais privés.

L'utilisateur concerné est chargé de vérifier et éventuellement de contester sa facture dans les deux mois, directement par e-mail auprès de l'opérateur. Communications privées et professionnelles sont cumulées sur la facture. Après vérification, l'utilisateur valide le montant total de ses frais privés de téléphone par intranet via l'application PeopleSoft. L'accès à cette information dans PeopleSoft est confidentielle et uniquement accessible par l'utilisateur moyennant son mot de passe. Si après 3 mois, l'utilisateur n'a pas approuvé ses communications, l'ensemble des frais seront considérés comme privés et imputés comme tels à l'utilisateur.

La possibilité d'effectuer des contrôles ex-post ponctuels est prévue si la facture mensuelle dite professionnelle d'un téléphone mobile dépasse 200 €. Dans un tel cas, le système envoie un message à l'utilisateur ainsi qu'à son supérieur hiérarchique direct, lequel peut décider d'interroger l'utilisateur sur les communications passées. Les personnes concernées par ces contrôles ainsi que leur supérieur hiérarchique direct sont informées sans délai des vérifications effectuées, des résultats ainsi que de leur utilisation éventuelle. Un représentant du personnel et le délégué à la protection des données sont également informés confidentiellement et sans délai de toute exploitation individuelle des relevés des numéros appelés sur la ligne professionnelle. Les cas d'utilisation considérés comme abusifs ou illicites peuvent faire l'objet d'une investigation technique par le Département IT après approbation du Département RH et après que la personne concernée ait eu la possibilité de s'exprimer à ce sujet et que sa hiérarchie ait informé le département des Ressources Humaines. L'article 1.5 du Code de conduite de la BEI s'applique si un membre du personnel a sciemment violé les obligations établies et dès lors des mesures disciplinaires peuvent être prises par la Banque. Cette partie de la procédure ne fait pas partie de cette analyse; les traitements de données dans le cadre des procédures disciplinaires ayant été analysés dans l'avis 2005-0102 du CEPD.

3. Les aspects légaux

3.1. Contrôle préalable

La notification reçue le 22 octobre 2009 représente un traitement de données à caractère personnel au sens du règlement - toute information concernant une personne identifiée ou identifiable - (article 2.a). Les données des utilisateurs de téléphones mobiles prêtés par la Banque sont traitées par LUXGSM pour le compte de la Banque ainsi que par la Banque elle-même dans l'application PeopleSoft.

Le traitement est effectué par un organe européen et est mis en œuvre pour l'exercice d'activités relevant du champ d'application du droit européen (article 3.1). Le traitement est automatisé en tout (article 3.2). Dès lors, le traitement tombe sous le champ d'application du règlement.

L'article 27.1. du 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 traitement de données relatives au trafic et à la facturation dans le cadre des réseaux internes de télécommunication pose des problèmes particuliers d'une importance telle que le chapitre IV du règlement prévoit une disposition spécifique et des garanties spéciales. Pour le motif qui précède, le traitement en question fait l'objet d'un contrôle préalable du CEPD.

En principe, le contrôle effectué par le CEPD est préalable à la mise en place du traitement. Dans ce cas, le contrôle préalable est postérieur à la mise en place du traitement. Ceci n'enlève rien à la mise en place des recommandations présentées par le CEPD.

La téléphonie mobile permet aussi un accès à Internet. La politique générale de vérification de l'utilisation d'Internet n'est pas analysée dans cet avis.

La notification du DPD a été reçue le 22 octobre 2009. Conformément à l'article 27(4) du règlement, le présent avis doit être rendu dans les deux mois qui suivent. Une demande d'information a suspendu le délai dans lequel l'avis doit être rendu de 877 jours. Le CEPD rendra donc son avis pour le 18 mai Octobre 2012.

3.2. Licéité du traitement

Conformément au règlement (article 5.a)), la licéité du traitement est liée à l'exécution d'une mission effectuée dans l'intérêt public sur la base d'actes législatifs adoptés sur la base des traités instituant l'Union européenne.

Deux éléments doivent donc être considérés: d'une part si le traité ou d'autres instruments juridiques prévoit la mission d'intérêt public endossée par le traitement (la base juridique), d'autre part si le traitement mis en place est effectivement nécessaire à la réalisation de cette mission d'intérêt public (la nécessité).

Dans le présent dossier, le CEPD note que la BEI a adopté des règles d'utilisation des postes de téléphones portables. Ces règles prévoient que les téléphones sont a priori réservés aux besoins professionnels mais peuvent, dans une mesure raisonnable être utilisé à usage privé pour autant que cet usage soit déclaré car il sera déduit du salaire de la personne concernées. Des vérifications peuvent être conduites par la Banque. L'adoption de cette note et sa

communication à chaque utilisateur de téléphone portable est un élément pertinent pour déterminer que la base juridique est adéquate au regard de l'article 5.a).

La base juridique du traitement a toute son importance car les données traitées peuvent être sensibles et les risques au regard des droits et libertés des personnes concernées importants. Elle se fonde en l'espèce sur des communications au personnel (26 avril et 15 mai 2004) et notes Coordinations (20 janvier 2009), concernant les nouvelles procédures pour les frais privés de téléphone ainsi que sur la déclaration que la personne concernée doit signer lorsqu'elle souhaite utiliser un téléphone mobile fourni par la Banque. Le CEPD a interprété la notion d'actes législatifs au sens large, comme des actes de portée normative. Une décision administrative de la Banque peut donc être considérée comme suffisante pour être conforme à l'article 5.a).

Ensuite, le règlement précise dans son article 37(2) que les données de trafic peuvent être traitées aux fins de la gestion du budget des télécommunications et du trafic, y compris la vérification de l'usage autorisé des systèmes de télécommunication. La BEI a développé ce traitement pour d'une part la gestion efficace de son budget -via les auto-déclarations concernant les appels privés et professionnels- et d'autre part pour vérifier le respect des règles d'utilisation des postes de téléphones portables (note au personnel titulaire d'un téléphone d'un téléphone portable, 20 janvier 2009) qu'elle a adopté.

En outre, le considérant 27 du règlement dispose que "*le traitement de données à caractère personnel effectué pour l'exécution de missions d'intérêt public par les institutions et organes communautaires comprend le traitement de données à caractère personnel nécessaires pour la gestion et le fonctionnement de ces institutions et organes*". Le traitement en question a entre autre pour finalité la gestion efficace du budget de l'institution concernant la téléphonie mobile.

La nécessité du traitement doit être évaluée à la lumière des finalités du traitement. Le traitement doit en effet être nécessaire pour atteindre les finalités présentées. Nécessité et finalité sont donc directement liées.

En l'espèce, comme expliqué plus haut, la finalité du traitement est de s'assurer pour la Banque que l'usage privé des téléphones portables soit imputé en termes de coûts aux employés et soit raisonnable en termes de temps.

3.3. Qualité des données

Les données traitées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées (article 4.1.c)), à savoir la gestion du budget des communications téléphoniques et la vérification des règles d'utilisation du téléphone mobile. Il convient d'établir si les données sont nécessaires à la réalisation des finalités pour lesquelles elles sont collectées. Dans le cas sous analyse, le traitement de données ne concerne que les données relatives à la facturation et au trafic et ne concerne aucune donnée relative au contenu des communications. Les données décrites semblent, en l'espèce, nécessaires au regard de la finalité pour laquelle elles ont été collectées. Il est cependant nécessaire de déterminer quelles données relatives au trafic sont nécessaires aux finalités déclarées - voir le point 4 concernant les numéros composés - et quelles données peuvent être communiquées aux différentes parties impliquées dans la procédure.

Par ailleurs les données doivent être traitées loyalement et licitement (article 4.1.a. du règlement. La licéité a déjà fait l'objet d'une analyse (voir point 3.2). Quant à la loyauté, dans le cadre d'un sujet aussi sensible, elle doit faire l'objet de beaucoup d'attention. Dans le cas sous analyse elle est liée aux informations qui doivent être transmises à la personne concernée. Ces informations doivent être claires pour les personnes concernées - c'est à dire faire partie d'un cadre informatif transparent et complet - et être disponibles dans un document unique (voir ci-dessous point 3.8).

Enfin les données doivent être "exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables sont prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées" (article 4.1.d) du règlement). Le système en lui-même semble garantir la qualité des données. Les droits d'accès et de rectification à la disposition de la personne concernée représentent le deuxième moyen permettant de s'assurer de la qualité des données (voir point 3.7). De plus, la liste des appels envoyée à la personne concernée et la possibilité qu'à cette dernière de contester cette liste, constitue un moyen supplémentaire de garantir l'exactitude des données.

3.4. Conservation des données

Le principe général du règlement veut que les données à caractère personnel ne puissent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement" (article 4.1.e) du règlement).

L'article 37 du règlement prévoit des règles spécifiques concernant la conservation des données relatives au trafic et à la facturation dans le cadre des réseaux internes de télécommunication. Ces réseaux sont définis par l'article 34 comme étant "les réseaux de télécommunications ou des équipements de terminaux fonctionnant sous le contrôle d'une institution ou d'un organe communautaire".

Les données relatives au trafic qui concernent les utilisateurs et qui sont traitées et mises en mémoire afin d'établir les communications sont effacées ou rendues anonymes dès que la communication ou la connexion concernée est terminées (article 37.1). Le principe général est donc l'effacement des données dès qu'elles ne sont plus nécessaires à l'établissement de la communication ou de la connexion.

L'article 37.2 du règlement établit cependant que les données relatives au trafic conservées aux fins de la gestion du budget des télécommunications et du trafic, y compris la vérification de l'usage autorisé des systèmes de communication, doivent être effacées ou rendues anonymes dès que possible et au plus tard 6 mois après leur collecte, à moins que leur conservation ultérieure ne 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.

La Société LUXGSM conserve à présent[2] les données de téléphonie mobile du personnel de la BEI pour une durée de 6 mois.

Les données sont conservées depuis le mois d'avril 2004. Le CEPD se réjouit que la BEI s'applique à présent à se conformer à l'article 37.2 du règlement en prévoyant une durée de

[2] La BEI a signé un avenant au contrat signé avec la société LUXGSM afin de modifier la durée de conservation des données. D'une année, la durée est passée à six mois, le 1er février 2010.

conservation plus courte et au plus tard de 6 mois après la collecte des données à moins que leur conservation ultérieure ne 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. Toutes les données de plus de 6 mois non nécessaires dans le cadre d'une action en justice doivent donc être effacées sans délais.

De plus, certaines données nécessaires à la validation des appels privés par le personnel ne sont plus nécessaires au contrôle du budget une fois la validation effectuée. C'est le cas par exemple des numéros composés. Le CEPD recommande donc que ces données, nécessaires exclusivement à la validation des appels privés, soient effacées dès que la validation a eu lieu. En effet, les données doivent être nécessaires à la finalité pour laquelle elles ont été collectées. Il n'existe pas de lien suffisant, après la validation des appels privés par la personne concernée, entre la finalité - la contrôle du budget - et les données conservées (le numéro composé par exemple).

L'article 20 du règlement prévoit que des exceptions et des limitations peuvent être apportées à l'article 37.1 pour autant qu'une telle limitation constitue une mesure nécessaire pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales; pour sauvegarder un intérêt économique ou financier important d'un État membre ou de l'Union européenne, y compris dans le domaine monétaire, budgétaire et fiscal; pour garantir la protection de la personne concernée ou des droits et libertés d'autrui. Cette disposition autorise donc la conservation des données relatives au trafic et à la facturation pour d'autres finalités que celle de la gestion du trafic et du budget des communications dans un nombre limité de cas. Le CEPD a interprété l'article 20 à la lumière de la *ratio legis*, et notamment en autorisant des exceptions pour la durée de conservation dans le cadre des enquêtes disciplinaires. Dans le cadre d'enquêtes disciplinaires, les données adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées peuvent dès lors, conformément à l'article 20 du règlement, être conservées pour une durée supérieure à 6 mois (voir à ce propos l'avis rendu par le CEPD à propos du traitement de données portant sur la procédure disciplinaire de la BEI, 2005-102).

Si une conservation plus longue des données est envisagée pour des finalités statistiques, cela doit se faire dans le respect de l'article 4.1.e, les données doivent être rendues anonymes.

3.5. Transfert des données

L'opération de traitement devrait également être examinée à la lumière de l'article 7.1. du règlement. Au titre de cet article, les données à caractère personnel ne peuvent faire l'objet d'un transfert entre institutions ou organes communautaires ou en leur sein que "si elles sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire". L'article 37.3. du règlement stipule que le traitement de données relatives au trafic et à la facturation ne peut être réalisé que par les personnes responsables de la gestion de la facturation, du trafic ou du budget. Les transferts décrits ci-dessus semblent bien répondre aux critères de ces articles.

L'article 7.3 du règlement dispose que "le destinataire traite les données uniquement aux fins qui ont motivés leur transmission". Il doit être garanti que toute personne recevant et traitant des données relatives au trafic et à la facturation au sein de la BEI ne pourra les utiliser à d'autres fins.

3.6. Traitement incluant le numéro de personnel ou le numéro identifiant

La BEI utilise le numéro de personnel. L'utilisation d'un identifiant n'est, en soi, qu'un moyen - légitime, en l'espèce - de faciliter le travail du responsable du traitement des données à caractère personnel; toutefois, cette utilisation peut avoir des conséquences importantes. C'est d'ailleurs ce qui a poussé le législateur européen à encadrer l'utilisation de numéros identifiants par l'article 10.6 du règlement, qui prévoit l'intervention du Contrôleur européen.

Il ne s'agit pas ici d'établir les conditions dans lesquelles la BEI peut traiter le numéro de personnel, mais de souligner l'attention qui doit être portée à ce point du règlement. En l'espèce, l'utilisation du numéro de personnel par la BEI est raisonnable car l'utilisation de ce numéro est uniquement un moyen de faciliter le travail du traitement, en particulier la facturation.

3.7. Droit d'accès et de rectification

L'article 13 du règlement dispose du droit d'accès -et de ses modalités- à la demande de la personne concernée par le traitement. L'article 14 du règlement dispose du droit de rectification pour la personne concernée. Dans le cas d'espèce, la personne concernée a accès à sa facture détaillée qu'elle peut vérifier et contester. Les articles 13 et 14 du règlement sont donc respectés.

Le CEPD souligne cependant que le verrouillage des données ainsi que leur effacement doivent être assurés par la Banque dans les conditions prévues par les articles 15 et 16.

En ce qui concerne le verrouillage des données qu'il faut distinguer deux situations:
(1) lorsque la personne concernée conteste l'exactitude de ses données, les données doivent être verrouillées "pendant un délai permettant au responsable du traitement de vérifier l'exactitude, y compris l'exhaustivité des données". Ainsi, lorsque la BEI reçoit une demande de verrouillage sur cette base, il doit immédiatement verrouiller les données pendant le délai nécessaire à la vérification de l'exactitude et de l'exhaustivité des données;

(2) lorsque la personne concernée demande le verrouillage de ses données en raison d'un traitement illicite, ou lorsque les données doivent être verrouillées à des fins probatoires, la BEI aura besoin d'un certain temps afin de conduire cette évaluation pour décider de verrouiller les données. Dans ce cas, même si le verrouillage ne peut pas avoir lieu directement, la demande doit être traitée rapidement afin de préserver les droits de la personne concernée. Le CEPD a donc estimé que l'évaluation de la demande devait se faire le plus tôt possible et au plus tard dans les 15 jours ouvrables.

3.8. Information des personnes concernées

Les articles 11 et 12 du règlement 45/2001 portent sur les informations à fournir aux personnes concernées en vue de garantir un traitement transparent des données à caractère personnel. Les personnes concernées doivent bénéficier d'une information claire et proactive. L'article 11 prévoit que, lorsque les données sont collectées auprès de la personne concernée, les informations doivent être fournies au moment où elles sont recueillies. Lorsque les données n'ont pas été collectées auprès de la personne concernée, les informations doivent être fournies au moment où les données sont enregistrées ou communiquées pour la première fois, sauf si la personne en dispose déjà (article 12).

En l'espèce, les données n'ont pas été collectées auprès de la personne concernée. L'article 12 s'applique. Pour rappel, le personnel concerné dispose d'une série de documents, sous forme de communications au personnel, de règles d'utilisation et de guide des utilisateurs au moment où la Banque lui attribue un téléphone portable. Il signe également sa demande ("application for a mobile phone and declaration regarding its use") dont il reçoit une copie. Si les informations à fournir se retrouvent en filigranes des documents, le CEPD souligne que cette information manque de clarté et peut ainsi entraver un traitement loyal des données. L'information concernant les rubriques prévues par l'article 12 devrait être plus claire et préférentiellement disponible dans un document unique. Dans la même perspective, le CEPD demande que la personne concernée soit aussi informée de la durée de conservation des données ainsi que de son droit de saisir à tout moment, le Contrôleur européen de la protection des données. De plus, une référence au code de conduite et aux conséquences possibles en cas de violation des obligations établies par le code devrait figurer dans la demande signée par la personne concernée.

3.9. Traitement de données à caractère personnel pour le compte de la BEI dans sa qualité de responsable du traitement

La société LUXGSM doit être considérée comme le sous-traitant au sens de l'article 2.e): LUXGSM traite des données à caractère personnel pour le compte de la BEI.

L'article 23 prévoit que la réalisation de traitement en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que le sous-traitant n'agit que sur instruction du responsable du traitement et que les obligations visées aux articles 21 et 22 incombent également au sous-traitant. La sous-traitance est bien régie par un contrat qui précise que LUXGSM n'agira que sur instruction de la Banque et que le règlement 45/2001 s'applique au traitement de données sous traité. L'article 23 semble donc bien respecté.

3.10. Sécurité

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.

4. 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 BEI:

- se conforme rapidement à l'article 37.2 du règlement en prévoyant une durée de conservation plus courte et au plus tard de 6 mois après la collecte des données à moins que leur conservation ultérieure ne 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 et efface toutes les données de plus de 6 mois non nécessaires dans le cadre d'une action en justice.

- fournisse une information à la personne concernée claire et préférentiellement disponible dans un document unique. La personne concernée doit aussi être informée de la durée de conservation des données ainsi que de son droit de saisir à tout moment, le Contrôleur européen de la protection des données.

Fait à Bruxelles, le 15 mai 2012

(**signé**)

Giovanni BUTTARELLI
Le Contrôleur européen adjoint de la protection des données