

Avis sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Banque européenne d'investissement au sujet du traitement des données LBC-FT

Bruxelles, le 7 février 2013 (2012-0326)

1. PROCÉDURE

Le 3 avril 2012, 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 d'un contrôle préalable concernant le traitement des données à caractère personnel «traitement des données LBC-FT».

Les documents suivants étaient joints à la notification à titre de documents justificatifs:

- le projet de politique de conformité en matière d'acceptation et de surveillance des contreparties couvrant l'intégrité, le blanchiment des capitaux et le financement du terrorisme (la politique intégrité et LBC-FT) [et documents connexes];
- [...]
- le code de bonne conduite administrative du personnel de la Banque européenne d'investissement dans ses relations avec le public.

Des questions ont été posées le 13 avril 2012, questions auxquelles le DPD de la BEI a répondu le 23 mai 2012, en joignant les documents complémentaires suivants:

- la charte d'intégrité de la BEI;
- le document *Compliance and the Compliance Function in Banks* (la conformité et la fonction «conformité» dans les banques) du Comité de Bâle sur le contrôle bancaire;
- les statuts de la BEI;
- un extrait du rapport au conseil des gouverneurs concernant l'exercice financier 2009 rédigé par le comité de vérification;
- un extrait du rapport au conseil des gouverneurs concernant l'exercice financier 2010 rédigé par le comité de vérification;
- []
- le questionnaire LBC-FT;
- la procédure de conformité en matière d'acceptation et de surveillance des contreparties couvrant l'intégrité, le blanchiment des capitaux et le financement du terrorisme (la procédure intégrité et LBC-FT) [et documents connexes];
- [...]

Des questions complémentaires ont été transmises les 26 juin 2012, 6 août 2012 et 8 octobre 2012; les réponses ont été reçues les 30 juillet 2012, 1^{er} octobre 2012 et 5 décembre 2012. Le projet d'avis a été envoyé au DPD pour observations le 6 décembre 2012. Le CEPD a reçu une réponse le 15 janvier 2013, suite à laquelle un rendez-vous entre la BEI et le CEPD a été fixé au 4 février 2013.

2. FAITS

Afin de mettre en œuvre les meilleures pratiques bancaires dans les domaines de la lutte contre le blanchiment des capitaux (LBC) et contre le financement du terrorisme (FT, conjointement: LBC-FT), et de minimiser les autres risques en matière d'intégrité et de réputation, le groupe BEI (constitué de la Banque européenne d'investissement et du Fonds européen d'investissement) entreprend une due diligence des contreparties (DDC) portant sur ses partenaires commerciaux (potentiels).

Avant d'entamer une nouvelle relation d'affaires, la BEI réalise une «procédure d'acceptation de la contrepartie» afin de déterminer si une telle relation entraînerait de quelconques risques parmi ceux susmentionnés. Les contreparties qui, a priori, ne suscitent pas d'inquiétudes particulières en termes d'intégrité font l'objet d'une DDC simplifiée. Tel est le cas par exemple des contreparties telles que les établissements de crédit ou financiers de l'espace des meilleures pratiques¹, les sociétés cotées en bourse de l'espace des meilleures pratiques ou les pouvoirs publics. À l'inverse, les opérations ou les relations d'affaires comportant des risques importants, au vu des résultats de l'évaluation des risques entreprise par le bureau de conformité du groupe BEI (**OCCO** - *Office of the Chief Compliance Officer*) et des principes définis dans les directives de l'Union européenne relatives à la LBC-FT², appellent une due diligence renforcée. Si tel est le cas, des compléments d'information pourraient être demandés. Cela peut notamment être le cas si des personnes politiquement exposées (PPE), des associations caritatives ou des opérations de conformité à hauts risques sont concernées.

Les résultats de ce processus sont utilisés dans le cadre du contrôle de la conformité des nouveaux projets et peuvent conduire au refus de la validation des contreparties ou à l'imposition d'exigences de conformité supplémentaires dans les contrats à signer. Le traitement débute dès lors qu'un agent de la BEI envisage d'entamer une relation d'affaires avec une nouvelle contrepartie.

Une fois la relation d'affaires établie, la surveillance des contreparties se poursuit afin de déterminer s'il est nécessaire de revoir l'évaluation initiale («surveillance continue de la relation avec la contrepartie»).

Le **responsable du traitement** est la Banque européenne d'investissement, l'OCCO étant un interlocuteur indiqué.

Les **personnes concernées** sont les personnes qui sont directement ou indirectement bénéficiaires³ des entités juridiques avec lesquelles la BEI entretient ou envisage d'entamer des relations d'affaires dans le cadre de projets de financement, ainsi que les personnes auxquelles ont été confiés des postes de direction au sein de ces entités juridiques (les «personnes clés de la contrepartie»). Il s'agit de personnes occupant des postes clés (tels que celui de président ou de directeur général) ainsi que des personnes siégeant au sein des organes directeurs (conseil d'administration, comité de direction, conseil de surveillance, conseil des collectivités locales ou équivalent) de la contrepartie.

¹ [...]

² [...]

³ Ce terme doit être considéré comme identique à la définition de «bénéficiaire effectif» à l'article 3, paragraphe 6, de la directive 2005/60/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, JO L 309 du 25.11.2005, p. 15 à 36.

Si une personne de l'une des catégories susmentionnées se trouve également être une PPE, cela est perçu comme un signe d'un risque accru. Les PPE sont définies à l'article 3, paragraphe 8, de la directive 2005/60/CE⁴ comme étant des «*personnes physiques qui occupent ou se sont vu confier une fonction publique importante ainsi que les membres directs de leur famille ou des personnes connues pour leur être étroitement associées*». Cette définition est explicitée plus avant à l'article 2 de la directive 2006/70/CE de la Commission⁵. Selon cet article, l'expression «fonction publique importante» fait référence aux actuels et anciens (sans limite temporelle) chefs d'État, chefs de gouvernement, ministres, ministres délégués et secrétaires d'État, parlementaires, membres des cours suprêmes, des cours constitutionnelles ou d'autres hautes juridictions dont les décisions ne sont pas susceptibles de recours, sauf circonstances exceptionnelles, membres des cours des comptes ou des conseils des banques centrales, ambassadeurs, chargés d'affaires, officiers supérieurs des forces armées et membres des organes d'administration, de direction ou de surveillance des entreprises publiques. Les «*membres de la famille*» sont définis comme étant les parents, le conjoint (ou équivalent), les enfants et leurs partenaires. Les «*personnes étroitement associées*» sont définies comme étant les bénéficiaires effectifs d'une personne morale ou d'une construction juridique conjointement avec une PPE ou les propriétaires d'une personne morale ou d'une construction juridique qui a été établie au profit *de facto* de la PPE. Ces dispositions visent également les situations équivalentes au niveau de l'UE ou à l'échelle internationale.

D'après le formulaire de notification, les **catégories de données** collectées dans le cadre de la procédure d'acceptation de la contrepartie sont les suivantes:

- les données d'identification;
- les données relatives aux délits, aux enquêtes et aux poursuites les concernant, ainsi qu'aux casiers judiciaires publics;
- les relations d'affaires.

Une partie de ces données est collectée directement auprès des personnes concernées, l'autre partie étant collectée à partir d'autres sources d'informations telles que les journaux, les bases de données spécialisées gérées par le secteur privé et les sites web. Ces deux dernières sources d'informations peuvent comprendre des bulletins d'information révélant des comportements (prétendument) illicites.

Suit une **description plus détaillée de l'opération de traitement**: les données collectées pendant la **procédure d'acceptation de la contrepartie** sont utilisées par la personne chargée du dossier s'occupant de l'opération de la BEI en question afin [d'évaluer la contrepartie à des fins de conformité]. [Les personnes chargées du dossier devront se pencher sur des éléments tels que] l'identité et les antécédents de la contrepartie et l'opération en question. [Il faudra évaluer] notamment si la contrepartie ou les personnes clés de la contrepartie ont fait l'objet d'allégations d'activités illégales ou préjudiciables/peu scrupuleuses ou de pratiques douteuses⁶, si leur fortune provient prétendument d'activités illégales, ou si elles affichent un comportement commercial inapproprié.

[Une évaluation plus poussée devra établir] si elles figurent sur de quelconques listes de sanctions pertinentes, si elles font l'objet d'une enquête pénale et/ou administrative menée par des autorités pertinentes, si elles ont des casiers judiciaires ou des condamnations pénales, si des sanctions leur ont été imposées ou si elles sont partie à d'importantes affaires au civil, et si elles suscitent d'autres inquiétudes concernant leur intégrité susceptibles de porter atteinte à la réputation de la BEI. L'objet de cette [évaluation] est d'aider à évaluer le risque de

⁴ Citée plus haut.

⁵ JO L 214 du 4.8.2006, p. 29 à 34.

⁶ [...]

blanchiment des capitaux, de financement du terrorisme ou tout autre risque de conformité aux termes de la charte d'intégrité⁷ de la BEI et du document portant sur la conformité et la fonction «conformité» dans les banques⁸, rédigé par le Comité de Bâle sur le contrôle bancaire.

En cas de réponse affirmative à l'une de ces questions, l'OCCO doit être consulté. L'OCCO émet alors un avis évaluant le risque que présente la contrepartie, avis qui devra être inclus dans le rapport soumis au conseil d'administration en vue de l'approbation de la relation d'affaires, ou être joint à celui-ci. Ces rapports peuvent comprendre des recommandations, telles que celles d'ajouter au contrat des clauses relatives à l'intégrité, d'exiger le renvoi des directeurs ou employés sanctionnés et/ou reconnus coupables ou d'exiger la transmission du résultat des enquêtes et de se conformer aux jugements des autorités compétentes.

Certaines contreparties⁹ remplissent les critères leur permettant de bénéficier d'une due diligence simplifiée («DDS») à condition qu'il n'y ait aucune inquiétude particulière quant à leur intégrité. Si tel est le cas, les exigences en matière de documentation sont assouplies¹⁰. Les opérations dites à haut risque donnent lieu à une due diligence renforcée («DDR»). Tel peut être notamment le cas lorsque des PPE sont concernées. Cela signifie que les vérifications supplémentaires que recommande l'OCCO viennent s'ajouter aux vérifications susvisées. Ces vérifications supplémentaires peuvent consister à obtenir des pièces d'identité des personnes clés de la contrepartie, des preuves documentaires des sources de richesse des bénéficiaires effectifs et/ou des PPE ainsi qu'un curriculum vitae ou une déclaration d'intérêt du bénéficiaire effectif et/ou de la PPE.

Si une relation d'affaires est conclue, les contreparties restent assujetties à une **surveillance continue**. Ce processus consiste entre autres à tenir à jour, au moyen d'examens périodiques, les informations collectées dans le cadre de la procédure d'acceptation de la contrepartie. De tels examens doivent être entrepris avant le premier versement, avant les versements si le dernier versement date de plus d'un an, puis, en règle générale, tous les ans. Par ailleurs, les agents de la BEI en contact avec les contreparties doivent rester vigilants afin de relever tout éventuel problème ou toute éventuelle rumeur ainsi que certains signes d'alerte relatifs aux contreparties. Outre les questions telles que celles consistant à déterminer si les transactions dévient du scénario habituel ou s'il y a récemment eu un changement de propriétaire, il peut également s'agir de déterminer si les contreparties (ou les personnes publiquement associées à celles-ci) ont un passé douteux ou font l'objet de bulletins d'information révélant de possibles violations d'ordre pénal, civil ou réglementaire. Dès qu'un signe d'alerte est identifié, l'OCCO est informé. Si des PPE sont concernées, un examen annuel¹¹ permet d'établir si elles se sont vu confier des fonctions publiques supplémentaires susceptibles de susciter des inquiétudes en termes d'intégrité et si elles ont fait l'objet de poursuites ou d'enquêtes pour activités illégales. De même, les personnes clés de la contrepartie font l'objet d'un suivi afin de vérifier si elles sont devenues PPE ou, si elles l'étaient déjà, si leurs fonctions au sein de la contrepartie ont changé.

⁷ Disponible à: http://www.eib.org/attachments/general/occo_charter_fr.pdf.

⁸ Disponible à: <http://www.bis.org/publ/bcbs113.pdf>.

⁹ Les établissements financiers ou de crédit de l'espace de meilleures pratiques [], les sociétés cotées dont les valeurs sont admises à la négociation sur un marché réglementé au sein de l'espace des meilleures pratiques, les autorités publiques ou autres contreparties qui satisfont aux critères techniques établis conformément à l'article 40, paragraphe 1, point b), de la directive 2005/60/CE.

¹⁰ Cela fait essentiellement référence aux exigences en matière de documentation concernant les personnes morales.

¹¹ Ou plus fréquent, si l'OCCO le recommande.

Les données collectées aussi bien dans le cadre de la procédure d'acceptation de la contrepartie que dans le cadre de sa surveillance peuvent être **transmises** aux membres des organes directeurs de la BEI, aux services internes de la BEI, aux institutions et organes de l'UE (notamment à l'OLAF) et aux cellules de renseignement financier (CRF) nationales. Les transferts à des entités externes seront entrepris soit sur demande du destinataire, soit de la propre initiative de la BEI s'agissant des transferts à des CRF nationales en cas de suspicion de blanchiment de capitaux ou de financement du terrorisme. Les transferts à des pays tiers ne sont pas prévus.

Les personnes concernées sont **informées** de l'opération de traitement dans une section de multiples façons. La procédure intégrité et LBC-FT dispose que *«les données à caractère personnel fournies à la banque [dans ce contexte] seront traitées conformément au règlement (CE) n° 45/2001»* et qu'elles seront *«traitées sous la supervision du chef du bureau de conformité du groupe BEI (GCCO - EIB Group Chief Compliance Officer) et utilisées exclusivement aux fins des activités de LBC-FT de la BEI»*. D'après la procédure, les personnes concernées ont le droit *«d'accès, de rectification et de verrouillage»* de ces données et *«peuvent exercer leurs droits en contactant à tout moment l'OCCO et/ou le contrôleur européen de la protection des données»*. Cette procédure s'accompagne également d'une description générale des mesures que la BEI prendra dans le cadre de la procédure d'acceptation de la contrepartie. D'après la notification, le responsable du traitement traitera les demandes d'effacement et de verrouillage dans les 30 jours ouvrables. La procédure intégrité et LBC-FT sera mise à la disposition du public sur le site de la BEI. Par ailleurs, les contrats de financement comprendront une clause relative à l'applicabilité du règlement¹². La BEI a également annoncé qu'elle publierait un «avis ad hoc» sur le respect du règlement (CE) n° 45/2001.

Les données sont **conservées** pendant dix ans à l'issue de la relation d'affaires. Aucun traitement supplémentaire à des fins scientifiques ou statistiques n'est envisagé.

Les données sont stockées sous forme électronique dans une zone d'accès restreint des serveurs de la BEI soumise aux **règles de sécurité** générales de la BEI (telles que le code de conduite du personnel, les normes informatiques et les règles relatives aux mots de passe). Les copies papier sont conservées sous clé dans des cabinets de l'OCCO prévus à cet effet auxquels seuls les agents de l'OCCO dûment habilités peuvent accéder.

3. ANALYSE JURIDIQUE

3.1. Contrôle préalable

Les opérations notifiées constituent un traitement des données à caractère personnel [*«toute information concernant une personne physique identifiée ou identifiable»* - article 2, point a), du règlement n° 45/2001 («le règlement»)]. Le traitement est effectué par un organe de l'UE dans le cadre d'activités qui relèvent du champ d'application des traités. Le traitement des données est effectué, du moins en partie, de manière automatique. Le règlement est donc applicable.

¹² Le libellé de la clause est le suivant: *«[l]e traitement des données à caractère personnel sera réalisé par la banque conformément à la législation en vigueur de l'Union européenne relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel effectués par les institutions et organes de la CE et à la libre circulation de ces données»*.

Aux termes de l'article 27, paragraphe 1, du règlement, 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» sont soumis au contrôle préalable du CEPD. L'article 27, paragraphe 2, du règlement dresse une liste non exhaustive de traitements susceptibles de présenter de tels risques. Le point a) mentionne entre autres les traitements de données relatives à des suspicions, infractions et condamnations pénales. Le point b) mentionne les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur comportement. Le point c) fait référence aux traitements permettant des interconnexions non prévues en vertu de la législation nationale ou communautaire entre des données traitées initialement pour des finalités différentes. Enfin, le point d) soumet à un contrôle préalable les traitements visant à exclure des personnes d'un contrat. Dans la notification, tous ces points ont été cités comme raisons à l'origine d'un contrôle préalable.

Comme décrit ci-dessus au chapitre 2, les données relatives à des infractions (ou suspicions) peuvent être traitées [article 27, point a)]. La procédure d'acceptation de la contrepartie a pour objet d'évaluer les aspects de la personnalité des personnes concernées [article 27, point b)], à savoir leur comportement, afin d'évaluer si elles présentent des risques au niveau de la LCB-FT ou de l'intégrité/la réputation. Il ne saurait non plus être exclu que les vérifications effectuées par les agents de la BEI avant de conclure un contrat entraînent des interconnexions entre des données à caractère personnel traitées initialement pour des finalités différentes [article 27, point c)]. Enfin, le traitement peut tout à fait conduire à l'exclusion de personnes du bénéfice d'un droit, d'une prestation ou d'un contrat [article 27, point d)]. Pour toutes ces raisons, le traitement fait l'objet d'un contrôle préalable.

Le contrôle préalable en vertu de l'article 27 du règlement devrait en principe avoir lieu avant le début du traitement. Lors d'échanges ultérieurs avec le CEPD, il a été clarifié que la procédure notifiée «réorganise, complète, modernise et vise à rendre plus cohérentes et efficaces les activités de conformité de la BEI, dont certaines étaient déjà en place auparavant». Il a également été déclaré que cela avait déjà été indiqué au CEPD dans une notification antérieure datant de 2007. Indépendamment du fait que la BEI ait fait part de l'existence de ce traitement ou non, il n'en demeure pas moins que l'activité de traitement notifiée était en place à la BEI avant la notification, bien que sous une forme différente et moins structurée. Le contrôle préalable actuel ne saurait donc avoir valeur de véritable contrôle préalable, mais plutôt de contrôle ex post. Le CEPD regrette que dans le cadre du présent dossier, la notification ne lui ait pas été soumise en temps opportun, à savoir avant le début des traitements. Il n'en reste pas moins que le responsable du traitement devrait dûment mettre en œuvre toute recommandation faite dans le cadre du présent avis.

La notification du DPD a été reçue le 3 avril 2012. Des questions supplémentaires ont été envoyées les 13 avril, 26 juin, 6 août et 8 octobre 2012; les réponses ont été reçues les 23 mai, 30 juillet, 1^{er} octobre et 5 décembre 2012. Le projet d'avis a été envoyé pour commentaires au DPD le 6 décembre 2012. Le CEPD a reçu une réponse le 15 janvier 2012. Suite à ces réponses, une réunion a été fixée au 4 février 2013. Conformément à l'article 27, paragraphe 4, du règlement, le présent avis doit être rendu dans un délai de deux mois. La procédure a été suspendue pendant une durée totale de 248 jours. Compte tenu de toutes les périodes de suspension, l'avis doit être rendu au plus tard le 11 février 2013.

3.2. Licéité du traitement

D'après la notification, l'article 5, points a) et b), du règlement établit les bases de licéité. En vertu de l'article 5, point a), un test en deux étapes doit être effectué afin de déterminer: 1) si soit le traité, soit d'autres actes législatifs prévoient une mission d'intérêt public sur la base de laquelle le traitement de données est effectué (*base juridique*), 2) si les traitements sont effectivement nécessaires à l'exécution de cette mission¹³. En vertu de l'article 5, point b), il doit être établi que le responsable du traitement est soumis à une obligation légale de collecte et de traitement des données qui ne lui laisse aucune marge de discrétion¹⁴. L'exigence de l'existence d'une obligation légale en vertu de l'article 5, point b) est notablement plus stricte que l'exigence de base juridique en vertu de l'article 5, point a), dans la mesure où une obligation spécifique ne laissant au responsable du traitement aucun autre choix que celui du traitement est normalement nécessaire.

3.2.1. Article 5, point a)

3.2.1.2. Les bases juridiques avancées par la BEI

Dans la notification, le responsable du traitement a avancé un certain nombre de bases juridiques possibles sans préciser celles qui étaient considérées comme des motifs de licéité aux termes de l'article 5, point a) ou de l'article 5, point b). Ces dispositions sont, respectivement, l'article 67, paragraphe 3, l'article 75, l'article 215 et l'article 325 du traité sur le fonctionnement de l'Union européenne (TFUE), le protocole n° 5 des traités (statuts de la BEI), notamment ses articles 16 et 18, paragraphe 1, les directives 2005/60/CE et 2006/70/CE, ainsi que les «*décisions et règlements du Conseil adoptés dans le cadre de la politique étrangère et de sécurité commune de l'UE*». Plusieurs de ces dispositions ne sauraient constituer une base juridique appropriée du traitement notifié, comme cela sera expliqué ci-après.

L'article 67, paragraphe 3, du TFUE est une disposition générale relative à l'espace de liberté, de sécurité et de justice (ELSJ), disposant que l'Union «*œuvre pour [...] la prévention de la criminalité [...] ainsi que [...] la lutte contre celle-ci*». Cette disposition est trop générale pour servir de base directe aux activités de traitement entreprises par la BEI en vertu de l'article 5, point a) - à partir de ce texte seul, le comportement de la BEI ne serait pas prévisible. Par exemple, les personnes concernées ne seraient pas en mesure de comprendre la mesure dans laquelle des données à caractère personnel les concernant pourraient être collectées et traitées plus avant. En outre, les traitements notifiés concernent également l'évaluation des personnes concernées quant aux «risques de réputation» qu'ils présentent, lesquels ne sont pas équivalents à la «criminalité».

L'article 325, paragraphe 1, du TFUE dispose que «*[l]Union et les États membres combattent la fraude et toute autre activité illégale portant atteinte aux intérêts financiers de l'Union par des mesures prises conformément au présent article [...]*». La suite de cet article définit des missions qui incombent à la Commission et aux États membres et autorise les colégislateurs de l'Union à prendre les mesures nécessaires à cette fin. Outre la disposition générale du premier paragraphe, aucune indication n'est fournie quant aux démarches spécifiques à effectuer. Comme pour l'article 67, paragraphe 3, du TFUE, cette disposition est trop générale

¹³ L'article 5, point a), du règlement autorise un traitement qui 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*».

¹⁴ L'article 5, point b) autorise un traitement qui est «*nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis*».

pour servir à elle seule de base juridique directe aux traitements de la BEI dans le cadre de la LBC-FT aux termes de l'article 5, point a).

Le responsable du traitement cite également les articles 75 et 215 du TFUE. Si ces deux dispositions autorisent l'Union à adopter une législation relative au gel des avoirs, elles ne sauraient autoriser un gel d'avoir ni exiger la vérification des listes de sanctions afin de déterminer si les clients y figurent. Les traitements de la BEI ne sauraient donc être directement fondés sur ces dispositions du traité. Par contre, les règlements et décisions adoptés sur la base de ces dispositions peuvent constituer la base juridique d'une partie du traitement notifié, à savoir les vérifications effectuées par la BEI afin de s'assurer que la contrepartie ne figure sur aucune liste de sanctions pertinente¹⁵. Ils ne couvrent toutefois pas les autres parties du traitement qui sont relatives à la LBC-FT et aux risques de réputation. Dès lors, la référence à une telle disposition ne saurait être considérée comme suffisante que pour justifier une partie du traitement, et non l'intégralité de celui-ci.

En ce qui concerne le contexte plus large de la législation européenne de LBC-FT, le responsable du traitement fait référence dans la notification aux directives 2005/60/CE et 2006/70/CE comme bases juridiques possibles. Ces directives établissent le cadre législatif relatif à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme (ci-après: «les directives LBC-FT»). Comme toute directive, elles s'adressent aux États membres, et ce faisant, ne sauraient s'appliquer directement à la BEI. Par ailleurs, les directives ne sont pas directement applicables en elles-mêmes dans la mesure où elles doivent être mises en œuvre au niveau national au moyen de dispositions législatives nationales. Le CEPD réfute donc le fait que les directives LBC-FT puissent constituer *directement* la base juridique des présents traitements.

En conclusion, la plupart des bases juridiques citées par le responsable du traitement dans la notification ne semblent pas appropriées aux fins de l'article 5, point a), du règlement. Le CEPD examinera ci-dessous les éventuelles bases juridiques qui pourraient légitimer le traitement.

3.2.1.3. Bases juridiques possibles

Le CEPD estime que la base juridique aux fins de l'article 5, point a) doit se trouver dans les dispositions légales qui s'appliquent directement à la BEI, telles que ses statuts et les dispositions adoptées par les organes de la BEI sur la base de ceux-ci. En particulier, l'article 18, paragraphe 1, des statuts de la BEI dispose que la BEI «*veille à ce que ses fonds soient utilisés de la façon la plus rationnelle dans l'intérêt de l'Union*». Cette obligation essentielle implique que la BEI a le devoir de s'assurer, entre autres, que ses ressources ne soient pas utilisées à des fins de blanchiment des capitaux ni de financement du terrorisme. Dans la même mesure, l'utilisation de fonds à destination de contreparties présentant des risques d'intégrité ou de réputation serait contraire à l'objectif d'utilisation rationnelle des

¹⁵ Il existe au total une vingtaine de règlements en vigueur imposant des mesures restrictives, telles que le gel des avoirs, fondés sur l'article 215 du TFUE ou d'autres bases juridiques antérieures. Bien que les dispositions y contenues soient légèrement différentes, tous les actes fondés sur ces articles comprennent des dispositions essentiellement équivalentes à l'article 2 du règlement (CE) n° 881/2002, qui dispose que «[t]ous les fonds et ressources économiques appartenant à, en possession de ou détenus par une personne physique ou morale, un groupe ou une entité désignés [...] sont gelés» et que «[a]ucun fonds ou ressource économique ne doit être mis, directement ou indirectement, à la disposition [...], ni utilisé au bénéfice» des personnes et des entités énumérées. Si des fonds sont néanmoins mis à la disposition de ces personnes ou entités, les personnes qui ce font sont passibles de sanctions telles que des amendes (article 10 du règlement n° 881/2002) sauf si elles «ne savaient pas ni ne pouvaient raisonnablement savoir» que leurs actions enfreindraient ces dispositions (article 2, paragraphe 2, du règlement n° 881/2002).

fonds dans l'intérêt de l'Union. De telles opérations nuiraient à l'image de la BEI en tant qu'institution publique chargée de gérer les fonds de l'UE et compromettraient la réputation de la Banque elle-même.

Qui plus est, l'article 12 des statuts de la BEI charge le comité de vérification de vérifier «*que les activités de la Banque sont conformes aux meilleures pratiques bancaires*». Les vérifications s'inscrivant dans le cadre de la LBC-FT (à savoir la DDC) font indéniablement partie des meilleures pratiques bancaires en Europe et au-delà, comme l'ont reconnu les recommandations du GAFI¹⁶ à ce sujet. Dans un certain sens, les mesures visant à éviter les relations d'affaires avec les contreparties présentant des risques d'intégrité et de réputation peuvent également être considérées comme des meilleures pratiques bancaires¹⁷. Les risques d'intégrité/de réputation revêtent encore plus d'importance pour les institutions financières internationales publiques telles que la BEI que pour les banques commerciales nationales. Une vigilance particulière est donc nécessaire pour éviter que la réputation de la BEI ne soit mise en danger du fait d'opérations conclues avec des personnes de mauvaise réputation.

Bien que les dispositions susmentionnées puissent, en théorie, servir de bases juridiques, le CEPD estime qu'elles sont trop générales et trop vagues pour constituer en soi un fondement suffisant du traitement dont il est question. En d'autres termes, les obligations générales découlant de l'article 12 et de l'article 18, paragraphe 1, des statuts de la BEI doivent être mises en œuvre et rendues plus concrètes et spécifiques. Il est en particulier indispensable que la BEI détermine et définisse précisément ce qui constitue les «meilleures pratiques bancaires» aux termes de l'article 12 aux fins du traitement LBC-FT.

À cet égard, le CEPD prend acte des travaux entrepris par la BEI afin d'établir un cadre pour l'identification des meilleures pratiques bancaires au sens de l'article 12 des statuts. En particulier, la charte d'intégrité de la BEI adoptée par le comité de direction définit le principe selon lequel le groupe BEI doit exécuter ses missions «*en conformité avec les normes généralement reconnues de bonnes pratiques financières et administratives [...]*». Elle stipule de même que l'OCCO doit contribuer à «*faire en sorte que le groupe BEI observe les lois, règles et règlements en vigueur, de même que les pratiques et normes professionnelles généralement admises [...]*». Elle précise en outre que «*l'objectif [est] [...] de prévenir le blanchiment d'argent, la corruption, et l'utilisation de fonds à des fins terroristes [...]*».

Par ailleurs, le comité de direction de la BEI a déclaré que la BEI «*se soumet en permanence et volontairement aux principales obligations imposées par la législation de l'UE et aux normes applicables au secteur bancaire*» (soulignement ajouté)¹⁸, à savoir notamment les directives LBC-FT et les recommandations du GAFI. À cette fin, le comité de direction et le conseil d'administration ont adopté un cadre de conformité aux meilleures pratiques bancaires (le «cadre»), reposant sur les directives susmentionnées et plusieurs autres textes. Le Comité de vérification a pris la décision selon laquelle les meilleures pratiques au sein de la BEI devaient être «*basées sur les principes prévus*» dans ceux-ci. Le comité de vérification a

¹⁶ Groupe d'action financière, Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération - Les Recommandations du GAFI.

¹⁷ Voir, par exemple, Comité de Bâle sur le contrôle bancaire: *Compliance and the Compliance Function in Banks*, avril 2005: «*L'expression "risque de conformité" est définie dans le présent document comme étant le risque de sanctions légales ou réglementaires, le risque de perte financière et le risque d'atteinte à la notoriété qui pourraient découler pour une banque du non-respect de lois, règlements, règles, normes d'un organisme d'autorégulation connexes, et codes de conduite s'appliquant à ses activités bancaires*» (soulignement ajouté), voir p. 7.

¹⁸ Réponse du comité de direction aux rapports annuels du comité de vérification concernant l'exercice financier 2010, p. 1 (jointe au rapport annuel au Conseil des gouverneurs concernant l'exercice financier 2010, du Comité de vérification).

également publié un document définissant la procédure que les agents de la BEI doivent suivre dans le cadre de la réalisation des vérifications LBC-FT (la «procédure»). Cette procédure est en outre complétée par [...] de plus amples précisions concernant ces vérifications. Le cadre est essentiellement basé sur la procédure intégrité et LBC-FT ainsi que sur les [documents connexes] correspondants. Le cadre a ensuite été notifié au Conseil des gouverneurs.

Les traitements notifiés semblent également en principe nécessaires aux fins d'une telle mission. Si elle ne réalisait ni les vérifications relatives à l'identité et aux antécédents du client avant d'entamer une relation d'affaires avec celui-ci, ni de surveillance continue, la BEI ne serait pas en mesure de détecter ni d'empêcher les situations où ses fonds seraient utilisés à des fins de blanchiment des capitaux ou de financement du terrorisme ou celles où la contrepartie présenterait des risques de réputation pour la BEI. Il convient toutefois de ne pas perdre de vue le fait que la notion de nécessité est une question de degré, et qu'il appartient au responsable du traitement de s'assurer qu'une telle surveillance ne dépasse pas les limites de ce qui est approprié et proportionné au but poursuivi. Ces aspects seront analysés dans la section 3.4 ci-dessous.

Compte tenu de ce qui précède, le CEPD estime que la combinaison des statuts de la BEI et des dispositions d'application y relatives (à savoir, la charte d'intégrité, le cadre, la procédure et les [documents connexes]) pourrait constituer, en théorie, une base juridique suffisante aux fins de l'article 5, point a), du règlement. Toutefois, tous ces documents ne sont pas publiés puisque seules la charte d'intégrité et la procédure le sont. De plus, les informations figurant dans les documents qui sont publiés (la charte et la procédure) ne sont pas exhaustives. Par souci de clarté et de transparence, le CEPD recommande que la procédure soit complétée par des informations supplémentaires quant au type de vérifications entreprises concernant les personnes physiques, telles que précisées dans les directives pertinentes et/ou les [documents connexes] (voir, par exemple, les informations portant sur les personnes clés de la contrepartie, la due diligence simplifiée ou renforcée des contreparties, les PPE, etc.). Le CEPD n'est pas sans ignorer l'argument selon lequel la fourniture de trop de détails dans les documents publiés pourrait faciliter les tentatives visant à contourner les mesures LBC-FT. Toutefois, pour des raisons de sécurité juridique, il convient de rendre les pratiques de la BEI plus transparentes. Quant au niveau de détail, les 40 recommandations du GAFI et les notes interprétatives y afférentes¹⁹ définissent la norme quant aux informations qui peuvent être divulguées sans compromettre l'efficacité des mesures LBC-FT.

3.2.2. Article 5, point b)

Pour que l'article 5, point b) soit applicable, il doit être établi que le responsable du traitement est soumis à une obligation légale de collecte et de traitement des données qui ne lui laisse aucune marge de discrétion. Pour les raisons en partie déjà exposées ci-dessus, le CEPD estime que les dispositions indiquées par la BEI ne peuvent être prises en compte aux fins de l'article 5, point b).

Si l'article 67, paragraphe 3, du TFUE prévoit que l'Union œuvre à la prévention de la criminalité et à la lutte contre celle-ci, il ne contient aucune obligation spécifique chargeant la BEI d'établir un programme de LBC-FT. La même remarque vaut pour l'article 325 du TFUE qui se contente d'énoncer le principe général selon lequel l'Union et les États membres combattent la fraude et toute autre activité illégale portant atteinte aux intérêts financiers de

¹⁹ <http://www.fatf-gafi.org/documents/internationalstandardscombatingmoneylaunderingandthefinancingofterrorismroliferation-thefatfrecommendations.html>

l'Union par des mesures spécifiques que devront adopter la Commission et les États membres. Les articles 75 et 215 du TFUE ne sont pas directement pertinents s'agissant de la BEI pour les motifs expliqués ci-dessus à la section 3.2.1. Il en va de même des directives LBC-FT dans la mesure où elles ne s'appliquent pas à la BEI.

L'article 12 et l'article 18, paragraphe 1, des statuts, imposent à la BEI des obligations générales consistant i) à utiliser ses fonds de la façon la plus rationnelle dans l'intérêt de l'Union et ii) à se conformer aux meilleures pratiques bancaires. Comme cela a déjà été souligné, pour que l'article 5, point b), soit applicable, il doit être établi que le responsable du traitement est soumis à une obligation légale de collecte et de traitement des données qui ne lui laisse aucune marge de discrétion. Les traitements spécifiques doivent être directement imposés par le traité ou un acte juridique adopté sur la base de celui-ci. Les dispositions susmentionnées n'établissent directement aucune obligation précise concernant le traitement LBC-FT. Le CEPD n'est dès lors pas convaincu que l'article 5, point b), soit applicable en l'espèce.

3.3. Traitement de catégories particulières de données

En vertu de l'article 10, paragraphe 1, 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 est interdit. Le traitement de ces catégories particulières de données est interdit à moins que l'une des exceptions aux termes de l'article 10, paragraphe 2, soit applicable. Il convient également de tenir compte de l'article 10, paragraphe 4, du règlement, qui dispose que *«[s]ous réserve de garanties appropriées, et pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2 peuvent être prévues par les [traités de l'UE] ou d'autres actes législatifs adoptés sur la base de ces traités ou, si cela s'avère nécessaire, sur décision du contrôleur européen de la protection des données»*.

Dans la notification, le responsable du traitement n'a pas identifié de catégorie particulière de données mentionnée à l'article 10, paragraphe 1. En tout état de cause, même si le traitement de catégories particulières de données n'est pas le but premier du traitement, la possibilité du traitement de telles données ne saurait être exclue. Par exemple, les vérifications entreprises à des fins de lutte contre le terrorisme pourraient tout à fait révéler des opinions politiques ou des convictions religieuses ou philosophiques. Le CEPD rappelle que, si tel est le cas, il convient de respecter l'interdiction en vertu de l'article 10, paragraphe 1, ou d'examiner de façon restrictive s'il est nécessaire d'appliquer une exception. Quoi qu'il en soit, le personnel de la BEI chargé des dossiers doit être informé de cette règle et éviter le traitement des catégories particulières de données à moins que les exceptions prévues à l'article 10, paragraphe 2 ou à l'article 10, paragraphe 4, ne soient applicables. Ce principe peut revêtir la forme d'une disposition générale à inclure dans les notes explicatives relatives à la LBC-FT.

L'article 10, paragraphe 5, ne permet *«le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté [...] que s'il est autorisé par les traités [...] ou d'autres actes législatifs adoptés sur la base de ces traités ou, si cela s'avère nécessaire, par le contrôleur européen de la protection des données, sous réserve des garanties spécifiques et appropriées»*. D'après la notification, les données relatives aux infractions (ou aux suspicions) peuvent être traitées dans le cadre de la procédure d'acceptation de la contrepartie et, par la suite, de la surveillance de la contrepartie. Le cadre relatif à la LBC-FT ne semble contenir aucune référence spécifique au fait que la BEI collecterait et traiterait des données relatives à des infractions aux termes de l'article 10, paragraphe 5.

Le CEPD recommande dès lors que la BEI adopte une base juridique spécifique (une décision prise au niveau administratif approprié) l'autorisant à traiter des données aux termes de l'article 10, paragraphe 5, en application des dispositions pertinentes du traité ou des statuts. Le traitement de catégories particulières de données devrait, en tout état de cause, être limité à la mesure nécessaire au respect des obligations légales relatives à la LBC-FT. Des garanties appropriées pour veiller au respect des principes de nécessité, de proportionnalité et de qualité des données devraient être mises en place à cet égard (voir également le point 3.4 ci-dessous).

3.4. Qualité des données

L'article 4, paragraphe 1, point c), du règlement dispose que 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. Cela comprend le fait que les données doivent être exactes et à jour; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes soient effacées ou rectifiées [article 4, paragraphe 1, point d)].

Concernant les critères de pertinence et d'adéquation, le traitement devrait être limité aux catégories de données qui sont directement liées à la garantie du respect de la législation bancaire applicable. Cela signifie notamment que les références aux «*enquêtes pénales et/ou administratives*», «*casiers judiciaires, condamnations pénales ou importantes affaires au civil*» et autres doivent être lues comme des références à de telles données dans la mesure où elles ont trait au respect des obligations relevant de la LBC-FT. Par ailleurs, le lien entre certaines des questions posées et les finalités de la LBC-FT n'est pas toujours clair. C'est le cas par exemple des allégations de «*pratiques douteuses*» ou «*autres risques d'intégrité*». Le CEPD recommande à la BEI d'examiner pour chacune des questions posées s'il existe un lien clair et direct entre celles-ci et les finalités de la LBC-FT ainsi que d'expliquer et de justifier ces liens au CEPD. Les questions pour lesquelles il n'existe aucun lien de ce type devront être supprimées. Par ailleurs, les dispositions imposant certaines vérifications devraient être interprétées de manière équilibrée conformément aux exigences de proportionnalité et aux autres exigences relatives à la protection des données.

Il est raisonnable de présumer que certaines des catégories de données sont de qualité suffisante, telles que les données d'identification fournies par les personnes concernées elles-mêmes ou les extraits de casiers judiciaires publics. Pour d'autres catégories de données, telles que les allégations d'activités illégales ou peu scrupuleuses, qui pourraient être fondées sur des articles de presse, cela ne peut être affirmé avec la même certitude. En l'espèce, la BEI doit prendre les mesures nécessaires pour garantir un niveau de précision élevé. De telles mesures pourraient entre autres consister à ne pas utiliser les articles de presse qui ne sont pas fiables, à recouper les informations tirées des articles de presse avec des sources d'information indépendantes ou à donner aux personnes concernées la possibilité de faire valoir leurs arguments. La BEI devrait mettre en place des procédures permettant de garantir que les données soient actualisées lorsque cela s'avère nécessaire et que les allégations qui s'avèrent infondées soient effacées dès que possible. Une attention particulière devra être portée aux homonymes afin d'éviter toute éventuelle confusion.

D'autre part, le CEPD suggère à la BEI de mettre en place des mesures efficaces pour garantir un niveau élevé de qualité des données. Ces mesures devraient par exemple couvrir les domaines clés suivants²⁰:

²⁰ Voir, à cet égard, l'avis 14/2011 du groupe de travail «article 29» sur les questions de protection des données relatives à la prévention du blanchiment de capitaux et du financement du terrorisme, pages 15 et 16.

- les personnes chargées du dossier qui entreprennent la DDC devraient recevoir une formation quant à la façon de ce faire tout en respectant les exigences en matière de protection des données;
- l'identification des bonnes et mauvaises pratiques de LBC-FT, notamment en ce qui concerne le principe KYC (*Know Your Client*), les pratiques de DDC, la façon de remplir le questionnaire, la notification (*reporting*) et le suivi continu.
- la nécessité d'éviter le recours à des techniques de profilage;
- les procédures d'inscription et de radiation des listes, ainsi que les mécanismes de réévaluation et de réexamen périodique;
- le principe de vérification de l'exactitude des sources d'informations publiques;
- une description expliquant si et comment l'entité fait la distinction entre les données factuelles, les données subjectives, les informations des services de renseignement et les données collectées au sujet de différentes catégories de personnes concernées;
- le respect strict et clair du principe de limitation de la finalité, notamment en ce qui concerne les transferts.

Le CEPD recommande à la BEI d'élaborer et de mettre en œuvre des mesures efficaces pour garantir un niveau de qualité des données élevé, tel que décrit ci-dessus.

3.5. Conservation des données

Les données à caractère personnel ne seront pas conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement [article 4, paragraphe 1, point e)].

Comme cela a été expliqué dans la partie descriptive du présent avis, les données sont conservées pendant dix ans. Aucun traitement supplémentaire à des fins scientifiques ou statistiques n'est envisagé.

Bien qu'elles ne soient pas directement applicables, les durées de conservation prévues dans la directive 2005/60/CE et la législation nationale qui l'applique peuvent servir de référence aux durées de conservation appropriées. Selon l'article 30 de cette directive, de telles données doivent être conservées pendant «*au moins cinq ans*». La vaste majorité des États membres appliquent une durée de conservation de cinq ans²¹. Le CEPD n'a reçu aucune justification probante démontrant les raisons pour lesquelles la BEI nécessiterait une durée de conservation considérablement plus longue, alors qu'il ressort très clairement de la pratique qu'une durée de conservation de cinq ans est suffisante. Le responsable du traitement a toutefois exprimé ses préoccupations quant au fait qu'une durée de conservation de 5 ans ne serait pas suffisante si une documentation était demandée une fois cette durée expirée, par exemple dans le contexte de poursuites judiciaires, notamment dans des pays tiers. La BEI a également affirmé qu'elle n'avait à ce jour qu'une expérience limitée en matière de LBC-FT et qu'elle n'était donc pas en mesure d'évaluer si une durée de conservation de 10 ans était suffisante ou excessive. L'expérience pourrait donc révéler qu'il faut modifier une telle durée. Pour ces motifs, le CEPD suggère à la BEI d'évaluer, dès lors qu'elle disposera de 10 années d'expérience dans le domaine de la LBC-FT, si une durée de 10 ans est nécessaire. En s'appuyant sur cette évaluation, la BEI devrait être en mesure de démontrer si une telle durée de conservation plus longue est effectivement nécessaire.

²¹ 25 des 27 États membres ont adopté une durée de conservation de 5 ans; seules l'Espagne et la Slovénie ont adopté une durée de conservation de 6 ans. Voir le document de travail des services de la Commission: *Compliance with the anti-money laundering directive by cross-border banking groups at group level*, SEC (2009) 939 final, pages 50-51.

3.6. Transfert de données

Les transferts de données à des destinataires qui sont soumis au règlement sont régis par l'article 7 de ce dernier; les transferts à des destinataires qui sont soumis aux législations nationales mettant en œuvre la directive 95/46/CE sont régis par l'article 8 du règlement, les transferts à des destinataires qui ne sont pas soumis à ces lois devant quant à eux respecter les règles définies à l'article 9 du règlement.

L'article 7, paragraphe 1, dispose que les données ne peuvent faire l'objet de transferts entre institutions ou organes de l'Union ou en leur sein que si elles sont «nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire». Les transferts visés à l'article 7 interviennent aussi bien au sein de la BEI qu'à destination d'autres institutions ou organes de l'Union. Les transferts internes peuvent survenir dans la mesure nécessaire pour prendre des décisions de financement et pour les fonctions de contrôle interne. D'après les informations fournies par la BEI, les transferts vers d'autres institutions et organes de l'UE sont essentiellement les transferts à OLAF, la Cour des comptes pouvant également recevoir des données. Dans la mesure où ces transferts concernent les enquêtes réalisées au sujet de dossiers spécifiques, ils relèvent en principe de l'article 7, paragraphe 1, du règlement. Une analyse au cas par cas doit cependant être réalisée afin d'apprécier in concreto si les conditions nécessaires au transfert sont effectivement remplies.

Les transferts à des CRF des États membres seront soumis soit à l'article 8, soit à l'article 9 du règlement, selon les modalités d'application de la directive 95/46/CE dans l'État membre en question: bien que le champ d'application de la directive à proprement parler exclue les activités répressives, de nombreux États membres ont choisi d'appliquer la directive sur une base horizontale, une loi couvrant ainsi tous les secteurs. S'agissant de ces États membres, les transferts à leurs CRF nationaux relèvent de l'article 8. L'article 8, point a), permet que les données à caractère personnel soient transférées à de tels destinataires «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».

De l'avis du CEPD, cette disposition doit être interprétée en ce sens que si les informations ne sont pas envoyées sur demande du destinataire, il appartient à l'émetteur de s'assurer que le transfert est nécessaire. Ce faisant, lorsque la BEI envoie des données à caractère personnel à des organes d'enquête d'un État membre, elle devrait démontrer que ces données sont nécessaires à l'exécution d'une mission effectuée dans l'intérêt public. Cette disposition s'applique aux transferts aux CRF s'il existe des motifs raisonnables de soupçonner des activités de blanchiment des capitaux ou de financement du terrorisme conformément au principe énoncé à l'article 22 de la directive 2005/60/CE. Une analyse au cas par cas est cependant nécessaire afin de démontrer la nécessité in concreto.

Concernant les États membres qui ont exclu de telles activités du champ d'application de leur législation mettant en œuvre la directive 95/46/CE, l'article 9 s'applique. L'article 9, paragraphe 1, n'autorise de tels transferts que pour autant qu'un niveau de protection adéquat soit assuré dans le pays destinataire. Dans la mesure où ces destinataires sont à la fois des États membres de l'UE et des signataires de la convention 108 du Conseil de l'Europe²², il est, en théorie, présumé que le niveau de protection est adéquat. Par ailleurs, la dérogation prévue à l'article 9, paragraphe 6, point d) («nécessaire [...] pour des motifs d'intérêt public

²² Conseil de l'Europe: convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STE n° 108.

importants») pourrait être invoquée dans des cas particuliers. Toutefois, cette exception devrait être interprétée de manière restrictive et faire l'objet d'une analyse au cas par cas.

D'après la notification, aucun autre transfert visé à l'article 9, par exemple vers des pays tiers, n'est prévu.

3.7. Droits d'accès et de rectification

Les articles 13 et 14 du règlement disposent que les personnes concernées doivent avoir le droit, à tout moment, d'accéder aux données enregistrées qui les concernent et de rectifier ces dernières. Des limitations sont possibles en vertu de l'article 20. Dans la notification, la BEI a indiqué que ces droits pourraient être limités conformément à l'article 20, paragraphe 1, points a), b) et c) du règlement.

D'après la BEI, la situation visée à l'article 20, paragraphe 1, point a) (la prévention, la recherche, la détection et la poursuite d'infractions pénales) serait le motif de refus d'accès le plus courant. The CEPD souligne que toute limitation des droits d'accès et de rectification ne peut être opérée qu'au cas par cas et uniquement dans la mesure où elle est *nécessaire* à cette fin. Des procédures appropriées devraient être mises en place afin de permettre l'exercice de ces droits dans de tels cas de figure.

En tout état de cause, l'article 20, paragraphe 3, doit être pris en compte et respecté par la BEI: *«[s]i une limitation prévue au paragraphe 1 est imposée, la personne concernée est informée conformément au droit communautaire des principales raisons qui motivent cette limitation et de son droit de saisir le contrôleur européen de la protection des données»*. En ce qui concerne le droit d'information, cette disposition doit être lue conjointement avec les articles 11, 12 et 20 du règlement (voir le point 2.2.9 ci-dessous).

En outre, il y a également lieu de tenir compte de l'article 20, paragraphe 4: *«Si une limitation prévue au paragraphe 1 est invoquée pour refuser l'accès à la personne concernée, le contrôleur européen de la protection des données lui fait uniquement savoir, lorsqu'il examine la réclamation, si les données ont été traitées correctement et, dans la négative, si toutes les corrections nécessaires ont été apportées»*. Le droit d'accès indirect devra alors être garanti. En effet, cette disposition interviendra, par exemple, dans les cas où la personne concernée a été informée de l'existence du traitement, ou en a connaissance, mais où son droit d'accès reste limité en application de l'article 20.

L'article 20, paragraphe 5, dispose que *«[l]'information visée aux paragraphes 3 et 4 peut être reportée aussi longtemps qu'elle prive d'effet la limitation imposée sur la base du paragraphe 1»*. Il peut être nécessaire que la BEI reporte cette information conformément à cette disposition, afin de protéger l'enquête. La nécessité d'un tel report doit être appréciée au cas par cas.

L'article 14 du règlement accorde à la personne concernée le droit à la rectification des données inexactes ou incomplètes. Compte tenu de la sensibilité de ces dossiers dans la plupart des cas, ce droit revêt une importance cruciale pour garantir la qualité des données utilisées, laquelle est, en l'espèce, liée au droit de défense. Toute limitation au titre de l'article 20 du règlement doit être appliquée à la lumière de ce qui a été dit aux paragraphes précédents concernant le droit d'accès.

3.8. Information de la personne concernée

Les informations à fournir aux personnes concernées doivent comprendre au minimum les éléments suivants (voir les articles 11 and 12 du règlement):

- l'identité du responsable du traitement;
- les finalités du traitement;
- les destinataires ou les catégories de destinataires;
- les catégories de données collectées;
- l'existence d'un droit d'accès et de rectification;
- la base juridique du traitement;
- les durées de conservation;
- le droit de saisir le CEPD;
- lorsque les données sont collectées auprès de la personne concernée, le caractère obligatoire ou facultatif de la réponse ainsi que les conséquences éventuelles d'un défaut de réponse;
- lorsque les données ne sont pas collectées auprès de la personne concernée, l'origine des données, sauf si le responsable du traitement ne peut divulguer cette information pour des raisons de secret professionnel.

La BEI publiera les règles et procédures relatives à la LBC-FT (c'est-à-dire la procédure intégrité et LBC-FT) sur son site Internet et inclura un avis quant à l'applicabilité du règlement n° 45/2001 dans ses contrats de financement. Bien que ce dernier avis pourrait contribuer à mieux faire connaître la législation applicable concernant la protection des données, il ne saurait à lui seul être suffisant, notamment parce qu'il parviendrait aux personnes concernées à un stade trop avancé (bien après le début du traitement).

En ce qui concerne les moyens de communication des informations, le CEPD estime que la publication de la procédure sur le site web ne suffit pas à elle seule à garantir que les personnes concernées recevront les informations de manière efficace. De fait, toutes les éventuelles personnes concernées ne liraient pas les informations publiées sur le site web. Le CEPD estime donc que cette publication doit être complétée, dans la mesure du possible, par une certaine forme d'informations individuelles contenant les informations nécessaires en vertu des articles 11 et 12 du règlement. Le CEPD recommande notamment de fournir ces informations à la contrepartie dès la première occasion appropriée (à savoir, après que le contact initial mettant la procédure en route a été établi), en lui demandant de les transmettre aux personnes identifiées ou identifiables concernées (par exemple au sein de l'organisation).

Sur le fond de la procédure, le CEPD remarque que, dans son état actuel, la procédure intégrité et LBC-FT n'informe pas les personnes concernées des (catégories de) destinataires des données, ne cite aucune base juridique claire du traitement et ne fournit pas de liste exhaustive des catégories de données. Elle ne les informe pas non plus des conséquences éventuelles d'un refus de fourniture d'informations (lorsqu'elles sont collectées directement auprès des personnes concernées) ni des sources de données collectées auprès d'autres sources.

Par ailleurs, la référence à l'exercice des droits des personnes concernées «*en contactant l'OCCO et/ou le contrôleur européen de la protection des données*» devrait être remplacée par une référence du type «*les personnes concernées peuvent exercer leurs droits en contactant le responsable du traitement; elles ont le droit de saisir à tout moment le contrôleur européen de la protection des données*», clarifiant ainsi la distinction entre leurs fonctions

respectives. Elle devrait également comprendre les coordonnées du responsable du traitement. Toutes les lacunes mentionnées dans cette rubrique doivent être rectifiées.

3.9. Décisions individuelles automatisées

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

Le CEPD rappelle à la BEI que tous les systèmes experts doivent être utilisés comme élément d'information et d'avertissement à l'appui de la prise de décisions opérée par le conseil d'administration et qu'ils ne sauraient remplacer la décision définitive qui doit être prise après analyse humaine.

3.10 Mesures de sécurité

Après l'examen minutieux des mesures de sécurité adoptées, le CEPD estime que ces mesures sont appropriées au regard de l'article 22 du règlement (CE) n° 45/2001.

4. CONCLUSION

Il n'y a aucune raison de penser qu'il existe une violation des dispositions du règlement n° 45/2001 pour autant qu'il soit pleinement tenu compte des observations apportées dans le présent avis. En particulier, la BEI devrait:

- s'assurer que le personnel de la BEI chargé des dossiers soit informé des règles concernant les catégories particulières de données en vertu de l'article 10 du règlement et éviter le traitement des catégories particulières de données à moins que l'une des exceptions prévues à l'article 10, paragraphe 2, ou à l'article 10, paragraphe 4, soit applicable. Ce principe peut revêtir la forme d'une disposition générale à inclure dans [les documents relatifs à] la LBC-FT;
- compléter la procédure par des informations supplémentaires quant au type de vérifications entreprises sur les personnes physiques, telles que précisées dans les directives pertinentes de l'UE et/ou les [documents connexes] (voir, par exemple, les informations relatives aux personnes clés de la contrepartie, due diligence simplifiée et renforcée des contreparties, PPE, etc.);
- établir une base juridique spécifique l'autorisant à traiter des données aux termes de l'article 10, paragraphe 5, au moyen d'une décision prise au niveau administratif approprié. Le traitement de catégories particulières de données devrait, en tout état de cause, être limité à la mesure nécessaire au respect des obligations légales relatives à la LBC-FT;
- examiner pour chacune des questions posées [...] s'il existe un lien clair et direct entre celles-ci et les finalités de la LBC-FT, expliquer et justifier ces liens au CEPD [et éviter] les questions pour lesquelles il n'existe aucun lien de ce type;

- élaborer et mettre en œuvre des mesures efficaces pour garantir un niveau de qualité des données élevé tel que décrit au point 3.4;
- évaluer, dès lors qu'elle disposera de 10 années d'expérience dans le domaine de la LBC-FT, si une durée de conservation de 10 ans est nécessaire et faire rapport au CEPD de la nécessité ou non de celle-ci;
- opérer des limitations des droits d'accès et de rectification au cas par cas uniquement et uniquement dans la mesure où elles sont *nécessaires*; des procédures appropriées devraient être mises en place afin de permettre l'exercice ultérieur de ces droits dans de tels cas de figure;
- remplacer la référence à l'exercice des droits des personnes concernées «*en contactant l'OCCO et/ou le contrôleur européen de la protection des données*» par une référence du type «les personnes concernées peuvent exercer leurs droits en contactant le responsable du traitement; elles ont le droit de saisir à tout moment le contrôleur européen de la protection des données»;
- rectifier les lacunes actuelles relatives aux informations fournies aux personnes concernées tel que décrit au point 3.8;
- fournir des informations aux personnes concernées dans un avis de confidentialité séparé qui devra être publié sur le site web de la BEI et qui sera envoyé aux nouvelles contreparties au début de la procédure d'acceptation de la contrepartie, en leur demandant de les transmettre aux personnes identifiées ou identifiables concernées (par exemple au sein de l'organisation).

Fait à Bruxelles, le 7 février 2013.

(signé)

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données