

Avis sur la notification d'un contrôle préalable reçue du DPD de la Banque Européenne d'investissement à propos du dossier enregistrement des communications téléphoniques dans les salles de marchés

Bruxelles, le 8 mai 2006 (Dossier 2006-102)

1. Procédure

- 1.1. Le 20 juillet 2004 le Contrôleur européen de la protection des données (CEPD) a envoyé une lettre aux délégués à la protection des données (DPD) leur demandant d'établir l'inventaire des traitements de données susceptibles de faire l'objet d'un contrôle préalable par le CEPD tel que prévu par l'article 27 du Règlement (CE) 45/2001 (ci après "le règlement"). Le CEPD a demandé la communication de tous les traitements sujets au contrôle préalable y compris ceux ayant débuté avant la nomination du contrôleur et pour lesquels le contrôle ne pourrait jamais être considéré comme étant préalable mais qui seraient soumis à un contrôle "ex-post".
- 1.2. A partir des inventaires reçus des délégués à la protection des données, le CEPD a identifié des thèmes prioritaires.
- 1.3. Le 10 novembre 2005, le CEPD a demandé une mise à jour de l'inventaire et la notification des traitements tombant dans le champ des thèmes prioritaires. Le CEPD a également élargi le champ des thèmes prioritaires notamment aux traitements de données liés aux communications électroniques et téléphoniques.
- 1.4. Le 2 mars 2006, le CEPD a reçu la notification pour contrôle préalable le traitement des données dans le cadre du dossier "Enregistrement des communications téléphoniques dans les salles de marchés" de la BEI.
- 1.5. Une demande d'information a été envoyée au DPD le 16 mars 2006. Une première réponse a été fournie le 21 mars 2006 par le DPD, et la suite des réponses ont été fournies par téléphone par Monsieur LEMAIRE le 24 mars 2006.
- 1.6. Une demande de précisions supplémentaires a été faite le 5 avril 2006. Une réponse a été fournie le 6 avril 2006.

2. Examen de l'affaire

2.1. Les faits

Toutes les opérations financières lancées par les "front offices" des départements "Marchés des capitaux" (FICAP) et du département "Trésorerie" (FITRE) et relatives aux opérations d'emprunts, de négoce en devises, en titres et en dépôts sont négociées et conclues par téléphone. Afin d'éviter que les termes d'un accord soient mal interprétés par l'une ou l'autre

partie, toutes les communications téléphoniques faites au sein de ces services sont enregistrées. Seuls sont exclus du système d'enregistrement les postes téléphoniques sur lesquels aucune opération de négoce n'est autorisée, à savoir les postes utilisés par les différents secrétariats, ceux des cinq bureaux et de la salle de réunion périphériques à la salle des marchés. Le cas échéant ces postes peuvent être utilisés par le personnel de la salle des marchés pour leurs appels privés. Par contre aucune possibilité n'est offerte de limiter l'enregistrement des communications en salle de marchés aux opérations de négoce seules; les conversations privées sur ces téléphones sont dès lors d'office enregistrées.

Les données relatives à la communication sont enregistrées sur un CD-ROM. Il s'agit non seulement du contenu de la communication en elle-même mais également les données entourant celle-ci telles que la date et l'heure. Ces données sont également notées dans le dossier opérationnel du dealer dans le cadre de son travail.

Un accès au système est autorisé à des fins de maintenance à la firme chargée de celle-ci. Tout accès au système d'enregistrement est notifié de manière complète dans le livre de rapport qui reste en permanence à côté de l'appareillage. La notification reprend la date de l'intervention, le motif de l'intervention, l'heure de début et fin des travaux, le nom de la (les) personne(s) intervenante(s). En principe l'accès aux pistes enregistrées n'est pas nécessaire à des fins de maintenance. Si l'accès s'avère toutefois indispensable, la présence du "Manager"¹ et du "dealer"² concerné est exigée pendant toute la durée des opérations. Si le "dealer" ne souhaite pas être présent pendant toute la durée, notification lui en sera faite.

Les enregistrements et les CD-ROM d'enregistrement sont consultés uniquement pour les besoins de vérification des opérations effectués par téléphone. Cette vérification s'effectuera en cas de litige sur opération ou de nécessité de contrôle opérationnel par la direction. Toute consultation se fera soit à la demande du "dealer" concerné, soit à celle de son chef de division, soit celle de son directeur de département. Le "dealer" ne pourra en aucun cas opposer un refus à sa hiérarchie qui lui demanderait la vérification d'une opération.

La consultation se fera en présence simultanée de l'agent impliquée et de son directeur de département ou de son remplaçant. La présence du chef de division pourra être requise. Si nécessaire, l'Inspection Générale, les services juridiques, le directeur des ressources humaines ou le Chief Compliance Officer (CCO) pourront être invités à y assister. Après l'introduction du code d'accès, l'agent directement impliqué dans la transaction litigieuse localisera au préalable, sur son canal d'écoute, la partie incriminée. Si l'écoute d'une opération litigieuse doit impérativement intervenir pendant l'absence, plus ou moins longue, de l'agent concerné (congé, mission, maladie...), son directeur de département tentera de le joindre pour lui signifier la nécessité de l'écoute de son canal. Dans ce cas le Délégué à la protection des données (DPC) sera également informé. En cas d'impossibilité de joindre l'agent concerné, l'écoute se fera d'office après en avoir averti le Directeur des Ressources Humaines et le DPC. Le directeur de département (ou son remplaçant) utilisera le code personnel d'accès dont l'agent concerné lui avait remis copie sous enveloppe scellée. Un procès verbal sera établi et signé par toutes les personnes en présence; copie sera remise à l'agent concerné dès son retour.

En cas de litige, les données peuvent être communiquées à la contrepartie (banque ou organisme directement concerné). En général la contrepartie aura elle-même un enregistrement de la transaction et ne devra dès lors pas recourir à une demande de

¹ Le Directeur Général FI, les directeurs des départements FITRE et FICAP, le membre de la division Coordination et Politiques Financières de FI chargé des questions techniques et conjointement.

² C'est à dire chaque agent dont les communications sont enregistrées.

transmission des données. Toutefois, si elle le demandait, la contrepartie ne pourra prendre connaissance de l'enregistrement que sur les lieux de la BEI et en présence du dealer. Si nécessaire, elles peuvent également être communiquées à l'Inspecteur Général, au service juridique ou Directeur Ressources Humaines et aux Chief Compliance Officer (CCO).

Toutes les personnes concernées au sein de la BEI ont été informées des détails de la procédure en elle-même au début de la procédure par leur hiérarchie. La procédure fait l'objet du "Finance Directorate Front Office Manuel" dont un exemplaire est remis à chaque nouveau membre de la Direction. Ce manuel contient une information sur le champ d'application du système d'enregistrement, les relations avec les contreparties, l'accès au local sécurisé, la procédure de maintenance du système, la conservation des CD-ROM d'enregistrement, la consultation des enregistrements, et le système de sauvegarde. Les directeurs de la Trésorerie et des Marchés des Capitaux veillent à ce que chaque contrepartie, soit avertie par le moyen qu'ils jugeront le plus approprié de l'existence d'un tel système d'enregistrement à la BEI au niveau des "front offices". Par ailleurs, l'enregistrement de telles conversations se fait en conformité au code d'éthique professionnel du milieu financier.

Des mesures de sécurité sont adoptées. [...]

2.2. Les aspects légaux

2.2.1. Contrôle préalable

L'enregistrement des communications téléphoniques relatives aux opérations d'emprunts, de négoce en devises, en titres et en dépôts faits dans les départements des marchés des capitaux (FICAP) et de la trésorerie (FITRE), constitue un traitement de données. Par ailleurs il s'agit d'un traitement de données personnelles puisqu'il s'agit de l'enregistrement de communications entre deux personnes dont au moins l'une d'entre elle est identifiée ou au moins "identifiable". En effet, est réputée "identifiable" au sens de l'article 2.a du règlement "une personne qui peut être identifiée directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale". Puisque l'enregistrement s'effectue sur un canal qui est propre à chaque "dealer", cette personne est identifiée. Par ailleurs, souvent au début de la communication la personne dans l'institution contrepartie va également s'identifier.

Le traitement de données présenté est effectué par une Institution, est mis en œuvre pour l'exercice d'activités relevant du champ d'application du droit communautaire.

Ces enregistrements se font à l'aide de moyens automatisés (article 3§2 du règlement) et font l'objet de traitements manuels puisque les données sont notées dans un dossier opérationnel du dealer constitutif d'un fichier au sens de l'article 2 du règlement.

Dès lors, ce traitement tombe sous le champ d'application du règlement (CE) 45/2001.

L'article 27§1 du règlement (CE) 45/2001 soumet au contrôle préalable du CEPD tous "les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités". L'article 27§2 du règlement contient une liste des traitements susceptibles de présenter de tels risques.

Le traitement de données dans le cadre des réseaux internes de communication présente des aspects particuliers en matière de protection des données, qui ont conduit à la rédaction d'un

chapitre spécialement dédié à ses aspects (Chapitre IV). Notamment, l'article 36 prévoit le principe fondamental de la confidentialité des données qui sera examiné ci-après. Au regard de ces risques particuliers, l'enregistrement des communications en salle des marchés peut entraîner une application de l'article 27 §1.

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

La notification du DPD a été reçue le 2 mars 2006. Conformément à l'article 27(4), le présent avis doit être rendu dans les deux mois qui suivent. Le délai a été suspendu pour une durée de 9 jours. Le contrôleur rendra donc son avis au plus tard le 11 mai 2006.

2.2.2. Base légale et licéité du traitement

Selon la notification reçue du DPD, le traitement des données collectées lors de l'enregistrement des communications des départements des marchés des capitaux (FICAP) et de la trésorerie (FITRE) se base sur le règlement du personnel et le FI Front Office Manual/Annexe 4 qui décrit la procédure. Le CEPD considère ce Manuel comme servant de base au traitement des données collectées dans les enregistrements pour des besoins de vérification des opérations effectuées par téléphone. "Cette vérification s'effectuera en cas de litige sur opération ou de nécessité de contrôle opérationnel par la direction" (Manuel, Partie IV). La vérification porte dès lors sur le contenu de la transaction. Le traitement ne peut dès lors servir à d'autres finalités que celles susmentionnées.

L'analyse de la base légale s'accompagne de l'analyse de la licéité du traitement telle que définie à l'article 5 du règlement (CE) 45/2001. L'article 5(a) prévoit que le traitement de données à caractère personnel ne peut que être effectué si le traitement est "nécessaire à l'exécution d'une mission relevant effectuée dans l'intérêt public sur la base des traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités". Le préambule du règlement (§27) prévoit que le traitement de données à caractère personnel effectué pour des raisons 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. L'enregistrement des communications en salle des marchés visant à assurer la validité des transactions peut dès lors être considéré comme étant nécessaire à l'exécution des missions de la BEI.

2.2.3. Qualité des données

En vertu de l'article 4§1 sous c) "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". Afin d'éviter que les termes d'un accord soient mal interprétés par l'une ou l'autre partie, toutes les communications téléphoniques faites au sein de ces services sont enregistrées. Par contre aucune possibilité n'est offerte de limiter l'enregistrement des communications en salle de marchés aux opérations de négoce seules. Les données concernées sont donc l'ensemble des données présentes dans les enregistrements de communications. Puisqu'il n'y a pas de possibilités de limiter les enregistrements il se peut que des conversations privées sur ces téléphones soient enregistrées le cas échéant.

La finalité du traitement étant la vérification des transactions passées sur les lignes des salles de marché et de la trésorerie, il est difficile, voir même non souhaitable de ne pas enregistrer tous les appels depuis ces départements puisqu'il est difficile a priori de faire la distinction entre des appels entrants à des fins privées sur des postes destinés aux opérations transactionnelles et des appels entrants professionnels. L'enregistrement de l'ensemble des communications est donc pertinent et non excessif par rapport à la finalité poursuivie. Par ailleurs il faut souligner que les membres des départements concernés sont invités dans le manuel de procédure, d'effectuer leurs appels privés à partir de certains postes précis non soumis aux enregistrements.

En ce qui concerne les données qui entourent la communication sans faire partie du contenu en lui-même, de telles données sont nécessaires dans le cas présent afin, par exemple, de pouvoir relier le contenu de la communication à un destinataire déterminé ou de pouvoir donner une date et une heure à la communication. Cela contribue à assurer l'exactitude des données.

L'article 4§1 sous d) prévoit par ailleurs que les données doivent être "exactes et, si nécessaire, mises à jour". L'enregistrement en direct des conversations garanti le respect de ce principe. D'autant qu'en cas de défaillance du système, un signal d'alarme est envoyé conjointement aux services techniques de la division FM ainsi que vers la salle des marchés.

2.2.4. Confidentialité des données

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

Il doit être précisé à cet égard que le principe de la confidentialité des communications est inspiré de l'article 5 de la directive (CE) 97/66 qui prévoit que les Etats membres doivent interdire d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément aux principes de droit communautaire. Cette directive a été remplacée depuis par la directive (CE) 2002/58, mais le principe reste le même: si les parties à la communication donnent leur consentement, il n'y a pas de violation du principe de confidentialité des communications. Le CEPD considère que l'article 36 du règlement doit être interprété à la lumière de ces dispositions.

En ce qui concerne l'enregistrement des communications, les "dealers" sont informés de la procédure dans le manuel "Front Office Manual/Annexe 4 " dont un exemplaire est remis à chaque nouveau membre de la Direction. Quant aux personnes concernées au sein de la contrepartie, les directeurs de la Trésorerie et des Marchés des Capitaux veillent à ce que chaque contrepartie, soit avertie par le moyen qu'ils jugeront le plus approprié de l'existence d'un tel système d'enregistrement à la BEI au niveau des "front offices". Il conviendra à ce titre de vérifier non seulement que la contrepartie en tant qu'institution est avertie, mais également que les personnes dont les données sont enregistrées soient également informées.

Quant à l'écoute éventuelle des enregistrements, la consultation se fera en présence simultanée de l'agent impliqué. En cas d'absence plus ou moins longue de l'agent concerné, son directeur de département tentera de le joindre pour lui signifier la nécessité d'écoute du canal. Seulement en cas d'impossibilité de joindre l'agent, l'écoute se fera sans qu'il en soit informé. Cette écoute se fera toutefois selon des conditions strictes conformément aux principes de

droit communautaire. L'écoute au sein de la BEI suppose d'office une écoute au sein de la contrepartie à la transaction et dès lors l'information de celle-ci.

2.2.5. Conservation des données

En principe les données personnelles peuvent 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 sous e).

L'article 37 §1 prévoit des règles particulières en matière de conservation de données de trafic à savoir les données entourant une communication dont notamment les données nécessaires pour établir celle-ci. En effet, en principe ces données doivent être effacées ou rendues anonymes dès que la communication est terminée.

L'article 37 §2 permet une conservation des données relatives au trafic pendant une période n'allant pas au-delà de 6 mois à des fins de gestion du budget des télécommunications et du trafic, y compris la vérification de l'usage autorisé des systèmes de communication. Cette disposition n'est toutefois pas nécessaire afin de justifier la conservation des données après la fin de la communication puisque l'article 20 permet également des restrictions à certains principes du règlement dans certains cas précis.

En effet, l'article 20 du règlement permet des exceptions aux articles 4 §1 et 37 §1 notamment lorsque la conservation des données constitue une "mesure nécessaire pour sauvegarder un intérêt économique ou financier important d'un Etat membre ou des Communautés européennes, y compris dans les domaines monétaire, budgétaire et fiscal".

Des données de trafic sont traitées dans le cadre la procédure d'enregistrement. L'ensemble des données est conservée pour une période d'un an à moins qu'il n'y ai une contestation d'une transaction auquel cas les CD-ROM seront éventuellement conservés au-delà de la période d'un an et ce jusqu'à ce que le problème soit résolu.

Cette période de conservation se justifie pour des raisons de sécurité et de preuve des transactions et pour répondre aux pratiques en la matière des différents intervenants (contreparties) sur les marchés financiers internationaux et est spécifique de la par la nature des marchés sur lesquels opère la BEI. Elle peut se justifier sur la base de l'article 20 dans la mesure où ladite procédure peut être considérée comme étant "nécessaire pour sauvegarder un intérêt économique ou financier important d'un Etat membre ou des Communautés européennes, y compris dans les domaines monétaire, budgétaire et fiscal".

2.2.6. Transfert des données

En vertu de la notification reçue du DPD, en cas de litige, les données peuvent être communiquées à la contrepartie (banque ou organisme directement concerné) et si nécessaire, à l'Inspecteur Général, au service juridique ou Directeur Ressources Humaines et aux Chief Compliance Officer (CCO).

Les transferts de données en interne doivent répondre aux critères de l'article 7 du règlement. Celui-ci prévoit que les données ne peuvent faire l'objet d'un transfert que si elles sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire. Le CEPD soulève un doute quant à nécessité de transfert vers Directeur Ressources Humaines si

le seul objectif du traitement des données est vérification des transactions tel que cela est stipulé dans la notification et le Manuel.

En cas de litige, les données ne sont pas transférées à la contrepartie mais sont mise à la disposition de celle-ci à la BEI. Nous verrons dès lors ce point dans la partie relative au droit d'accès.

2.2.7. Droit d'accès et de rectification

En application de l'article 13 du règlement, la personne concernée a notamment le droit d'obtenir, sans contrainte, du responsable du traitement, la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données. L'article 14 du règlement donne à la personne concernée le droit de rectifier les données inexacts ou incomplètes.

Le "Finance Directorate Front Office Manuel" (annexe 4) prévoit un accès pour le "dealer" au système d'enregistrement. Un éventuel droit de rectification ne pourrait s'exercer que sur les données entourant la communication, le contenu de celle-ci ne pouvant être erroné puisqu'il se fait en direct.

En ce qui concerne le droit d'accès et de rectification des contreparties, les contreparties, enregistrant elles-mêmes les communications, elles n'ont, en principe, pas besoin d'exercer un droit d'accès aux enregistrements de la BEI. Ceci étant dit, si la contrepartie ne devait pas posséder chez elle un tel système ou en cas de défaillance de son système, la BEI prévoit la possibilité de consultation pour les dealers des contreparties en ce qui concerne les enregistrements les concernant, en se rendant au siège de la BEI. Les mêmes limitations au droit de rectification s'appliquent le cas échéant.

2.2.8. Information des personnes concernées

Les articles 11 et 12 portent sur les informations à fournir à la personne concernée afin de garantir un traitement transparent des données à caractère personnel. L'article 11 prévoit que, lorsque les données sont collectées auprès de la personne concernée, les informations doivent être fournies au moment de la collecte. Lorsque les données n'ont pas été collectées auprès de la personne concernée, les informations doivent être fournies dès l'enregistrement des données ou lors de leur première communication, sauf si la personne concernée en dispose déjà. Étant donné qu'en l'espèce, les informations sont collectées au départ auprès de l'intéressé l'information doit être fournie au plus tard au moment de l'enregistrement des données.

L'information à fournir aux personnes concernées selon l'article 11 porte sur l'identité du responsable du traitement; les finalités du traitement, les destinataires ou catégories de destinataires; le caractère obligatoire ou facultatif de la réponse aux questions ainsi que les conséquences éventuelles d'un défaut de réponse; ainsi que l'existence d'un droit d'accès aux données et de rectification de données inexacts ou incomplètes. Toute information supplémentaire portant notamment sur la base juridique, les délais de conservation des données et le droit de saisir à tout moment l'EDPS peut également être donnée dans la mesure où cette information supplémentaire est nécessaire pour assurer un traitement loyal à l'égard de la personne concernée.

Comme mentionné dans les faits, l'information aux personnes concernées est fournie dans le "Finance Directorate Front Office Manuel" (annexe 4) dont un exemplaire est remis à chaque nouveau membre de la Direction. Ce manuel décrit de manière détaillée la procédure

d'enregistrement mais toutes les rubriques de l'article 11 ne sont pas mentionnées. Le manuel ne détermine ni le responsable du traitement, ni la possibilité de saisir à tout moment l'EDPS.

Quant à l'information donnée aux contreparties, selon les informations reçues, les directeurs de la Trésorerie et des Marchés des Capitaux veillent à ce que chaque contrepartie, soit avertie par le moyen qu'ils jugeront le plus approprié de l'existence d'un tel système d'enregistrement à la BEI au niveau des "front offices". Il conviendra à ce titre de vérifier non seulement que la contrepartie en tant qu'institution est avertie, mais également que les personnes dont les données sont enregistrées soient également informées.

2.2.9. Sécurité

Article 22 du règlement prévoit que des mesures techniques et organisationnelles doivent être prises afin d'assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à caractère personnel à protéger.

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

Conclusion

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

- Le manuel "Front Office Manual/Annexe 4 " détermine le responsable du traitement et la possibilité de saisir à tout moment l'EDPS;
- La nécessité du transfert des données vers Directeur Ressources Humaines soit examinée à la lumière de la finalité de vérification des transactions telle qu'elle est stipulée dans la notification et le manuel "Front Office Manual/Annexe 4 ";
- Qu'il soit vérifié dans la mesure du possible que non seulement la contrepartie en tant qu'institution soit avertie des informations concernant le traitement des données, mais également que cette information soit communiquée aux personnes dont les données sont enregistrées.

Fait à Bruxelles, le 8 mai 2006

Peter HUSTINX
Le Contrôleur européen de la protection des données