Avis sur la notification d'un contrôle préalable reçue à propos du dossier "Manager Desktop" de la Banque européenne d'investissement.

Bruxelles le XXX 2005 (Dossier 2004-307)

Procédure

Le 20 juillet 2004 le Contrôleur européen à la protection des données (CEPD) a envoyé une lettre aux délégués à la protection des données leur demandant de contribuer à l'établissement de 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. Le CEPD a demandé la notification 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".

Le 13 septembre 2004, le délégué à la Protection des données de la Banque européenne d'investissement a présenté la liste des cas devant être soumis à un contrôle préalable ex-post et notamment ceux concernant l'accès aux données à caractère professionnel, dans la mesure où ceux-ci pouvaient contenir des données relatives à l'évaluation des aspects de la personne concernée (compétence, rendement, comportement). (article 27.2.b).

Le Contrôleur européen de la protection des données a identifié certains thèmes prioritaires et a choisi un nombre de traitements sujets au contrôle préalable ex-post devant être notifiés. L'évaluation du personnel figure parmi ceux-ci.

Par courrier en date du 21 avril 2005 une notification dans le sens de l'article 27 (3) du règlement (CE) 45/2001 a été effectuée par Monsieur Jean-Philippe MINNAERT, Délégué à la Protection des données de la Banque Européenne d'Investissement (ci-après BEI).

Des informations ont été demandées par e-mails en date du 2 et du 11 mai 2005. En date du 20 mai 2005, la démonstration de la base de données Manager Desktop s'effectue au sein de la BEI dans son bureau de Bruxelles.

Faits

Le programme Manager Desktop permet aux responsables hiérarchiques d'accéder en-ligne aux données à caractère professionnel qu'ils ont besoin de connaître pour gérer les agents placés sous leur responsabilité, à l'exclusion de toutes données à caractère privé, telles que l'adresse, le lieu de naissance, la situation de famille ou les données relatives aux ayants-droit.

Chaque responsable hiérarchique (directeur général, directeur, chef de division, chef de bureau extérieur, chef d'unité ou délégués par eux) peut consulter uniquement les données relatives aux agents placés sous sa responsabilité.

Les données suivantes sont accessibles :

- les connaissances linguistiques,
- l'historique de carrière à la banque, (les raisons de changement de grade ou d'échelon sont indiquées : mérite, promotion, nouvelle affectation, reclassement, réorganisation)
- les diplômes,
- la base salariale
- le résumé des formations suivies depuis l'embauche,
- les appels téléphoniques professionnels

En outre, dans l'écran *Job History Summary*, figurent également :

- la date de naissance,
- la nationalité,
- la nature du contrat de travail (à durée indéterminée ou déterminée, avec, dans ce dernier cas, la mention de la date d'expiration du contrat).
- la base salariale

La base de données permet aussi de voir les données contenues dans l'onglet REVIEW ALL APPLICANTS. Cette rubrique permet au Manager de voir les candidats à un poste; les données indiquées après sélection de cette rubrique sont les qualifications professionnelles, l'expérience, à l'intérieur et à l'extérieur de la BEI, les langues étrangères, la formation continue suivie et la motivation du candidat".

L'information des personnes concernées s'effectue comme suit :

L'information des personnes concernées a été effectuée au moment de la collecte des données, lors de l'embauche, avec l'accord de l'agent concerné afin de permettre à la BEI d'analyser les candidatures.

L'information initiale sur le fonctionnement du système a été faite par des présentations orales de la fonctionnalité, en février 2002, ainsi que par une note explicative de la Direction RH du 27 février 2002 (en annexe).

Depuis lors, une présentation du système est faite systématiquement aux nouveaux collègues dans le cadre des sessions d'information lors de l'entrée en service. Les notes et documents de référence concernant le manager desktop sont accessibles à tout le personnel à travers l'intranet.

Un avertissement explicite quant au caractère confidentiel des données accessibles dans le cadre du manager desktop ainsi qu'un renvoi sous forme d'hyperlien au Règlement (CE) N° 45/2001 du 18 décembre 2000 figure sur la page d'accès à l'application PSFT RH.

Enfin, les membres du personnel ont accès, chacun pour ce qui le concerne au travers du libre service PSFT « My HR », à l'ensemble de leurs données personnelles reprises dans le manager desktop (en plus des données à caractère privé, évoquées à la rubrique 4 ci-dessus, qui ne sont pas reprises dans le manager desktop).

L'accès aux données

Le nombre de personnes ayant accès aux informations est très limité. Les responsables hiérarchiques peuvent consulter uniquement les données des agents placés sous leur responsabilité.

L'accès à ces données est sécurisé par un mot de passe strictement personnel et chaque membre du personnel a un droit d'accès et, le cas échéant, de rectification à l'égard de ses données personnelles. La rectification s'effectue soit par "Self-service Employee" ou moyennant une demande à RH assortie d'un justificatif (ex. données carrière antérieures à l'entrée en service, diplômes).

Les managers ont accès aux données des membres de leur équipe aussi longtemps qu'ils sont titulaires de leur poste (sauf suspension de l'accès par RH).

Les managers qui changent de poste n'ont plus accès aux données correspondant à leur ancienne fonction, sauf cas de promotion au sein du même service.

Concernant les appels téléphoniques professionnels

Les appels téléphoniques peuvent être effectués à la BEI en faisant le préfixe 0 ou le préfixe 10. Les appels avec le préfixe 0 sont professionnels, c'est à dire que c'est la BEI qui les paye.

Les appels avec le 10 sont privés, c'est à dire que ce sont les Agents qui les payent et ces appels ne sont pas connus par les Managers.

Les données indiquées sur les listes des téléphoniques professionnels sont les suivantes : date, heure, numéro appelé, durée, coût, coût total des appels par mois.

A la fin de chaque mois est mentionnée une case "approved" qui permet à l'agent d'approuver que les appels sont bien professionnels et non pas privés.

La liste des appels téléphoniques professionnels figurant dans le "Manager Desktop" permet donc aux Managers de voir le coût des appels téléphoniques effectués par leur personnel pour des raisons professionnelles. La base de données des appels téléphoniques est mise à jour une fois par mois. Elle sert au manager afin qu'il puisse voir ce qui est imputé au budget de sa direction. Les données téléphoniques sont effacées mois par mois, à l'occasion de la mise à jour de la liste.

Toujours dans l'attente d'une autre version que le power-point pour consulter la note sur la gestion des appels téléphoniques. Doit on poursuivre la demande de cette note, doit-on suspendre le délai ?

Aspects légaux

1. contrôle préalable

La notification reçue par e-mail le 21 avril 2005 représente un traitement de données à caractère personnel ("toute information concernant une personne identifiée ou identifiable" - article 2.a) et tombe dès lors sous le champ d'application du Règlement (CE) 45/2001.

L'article 27.1 du Règlement 45/2001 soumet au contrôle préalable du Contrôleur européen de la protection des données tout "traitement susceptible 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", ce qui est le cas en l'espèce, en raison du contrôle des appels téléphoniques professionnels.

La traitement rencontre par ailleurs les dispositions de l'article 27.2.b : "les traitements susceptibles de présenter de tels risques sont les suivants : les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur compétence, leur rendement ou leur comportement", ce qui est le cas en l'espèce. En effet la base de données peut comprendre les résultats d'une procédure d'évaluation ou des données relatives à l'évaluation, à leur compétence, mais n'est pas en tant que telle une opération de traitement dans le but d'évaluer la personne concernée.

La base de données Manager Desktop peut être comprise comme un outil de collecte de données, donnés qui serviront, notamment, à déterminer quelles personnes correspondent à un profil recherché ou quelles personnes choisir en fonction de leur compétence dans l'attribution d'un projet ou d'un dossier. De même dans l'historique de la carrière, les raisons de changement de grade ou d'échelon sont indiquées et montrent donc bien que ceci est utilisé dans le cadre d'une évaluation. A ces divers titres, Manager Desktop tombe sous le champ d'application de l'article 27.2.b du règlement (CE) 45/2001.

Par ailleurs, la mention des appels téléphoniques professionnels soulève le problème de la protection des données dans le cadre des réseaux internes de télécommunications. Le traitement des données relatives au trafic pose des problèmes particuliers d'une importance telle que le chapitre IV du règlement prévoit une disposition spécifique et des garanties spéciales (articles 34 à 40 du règlement 45/2001). Le contrôle des appels téléphoniques peut par ailleurs signifier une forme d'évaluation de l'usage professionnel du téléphone, de la proportionnalité de l'usage. Ce qui a une conséquence directe tant sur la gestion du budget des télécommunications (article 37.2 du règlement) que sur l'évaluation de la personne (article 27.2.b du règlement).

La notification du Délégué à la protection des données de la BEI a été reçue le 21 avril 2005. Des informations ont été fournies par e-mails datés du 2 et du 11 mai 2005.

En date du 12 mai 2005 (22è jour), rendez vous a été pris pour une démonstration de la base de données Manager Desktop au sein de la BEI. Conformément à l'article 27.4 du règlement (CE) 45/2001, le délai des deux mois au sein duquel le contrôleur

européen de la protection des données doit rendre son avis est suspendu, le temps que cette démonstration puisse se dérouler.

En date du 20 mai 2005, la démonstration de la base de données Manager Desktop s'effectue au sein de la BEI dans son bureau de Bruxelles. Par e-mail en date du 20 mai 2005 et à la suite du rendez-vous à la BEI, de nombreuses questions sont posées. Dès lors le délai reste suspendu. Les réponses ont été fournies par e-mail daté du 26 mai 2005.

Le Contrôleur européen de la protection des données rendra donc son avis pour le 4 juillet 2005 au plus tard, tel que prévu à l'article 27.4 du Règlement.

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.

2. base légale et licéité du traitement

La banque européenne d'investissement bénéficie, en application de ses Statuts, de l'autonomie de décision au sein du système institutionnel communautaire. Conformément à l'article 29 du règlement intérieur de la banque, le Conseil d'administration arrête les règlements relatifs au personnel. Le règlement du personnel fixe les conditions générales d'emploi du personnel.

La base légale de ce traitement repose sur les règlements régissant les relations de l'institution avec son personnel ainsi que les dispositions administratives et notes d'informations destinées à l'ensemble du personnel. La base légale est donc recevable en ce sens puisque la base de donnée est nécessaire pour une meilleure gestion du personnel.

L'analyse de la base légale par rapport au Règlement (CE) 45/2001 s'accompagne de l'analyse de la licéité du traitement. L'article 5.a du Règlement (CE) 45/2001 prévoit que "*le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités instituant les Communautés européennes ... ou relevant de l'exercice légitime de l'autorité publique dont est investi l'institution*". Les gestion des données professionnelles de la Banque européenne d'investissement concernant le personnel de la banque rentre dans le cadre de l'exercice légitime de l'autorité publique dont est investie l'institution, et est utile à la gestion des services du personnel, c'est pourquoi le traitement est licite.

Par ailleurs, les données contenues dans la rubrique "Review All Applicants" sert pour le Manager à voir les candidats à un poste; elles permettent donc bien une évaluation de la personne et sont donc soumises au contrôle préalable (article 27.2.b du règlement).

La référence à l'article 5.c dans la communication au personnel ("le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernées est partie ou à

l'exécution de mesures précontractuelles prises à la demande de celle-ci") ne semble pas pertinente dans la mesure où ce qui est inhérent au processus, ce n'est pas l'exécution du contrat mais l'exercice légitime de l'autorité publique dont est investie l'institution.

La mention des appels téléphoniques professionnels soulève le problème de la base légale de façon plus vaste. La conservation de données relatives au trafic et l'établissement des coûts moyens relèvent manifestement de la définition du "traitement" énoncée à l'article 2, point b), du règlement. Le système permet d'associer les différents numéros de postes aux informations sur l'utilisateur. Dans le cas précis, le montant total imputé à un numéro de poste est associé à un utilisateur. Les données doivent donc être qualifiées de "données à caractère personnel" au sens de l'article 2, point a).

Un objectif a été identifié dans les informations fournies ultérieurement : servir au manager afin de voir ce qui est imputé au budget de sa direction. Par ailleurs, in nous est précisé que "cette modalité se trouve dans le "Manager Desktop" parce que d'après nous elle a une finalité professionnelle et que cela évite d'avoir à créer un autre outil informatique uniquement pour cette modalité". Ceci n'est acceptable que dans le cadre de l'efficacité des perspectives informatiques, mais à l'unique condition que le personnel en soit informé (voir supra point 8).

La licéité du traitement de ces données est couverte par l'exercice légitime de l'autorité publique dont est investi la BEI en sa qualité d'institution, en vertu de laquelle elle doit gérer efficacement l'utilisation des outils de télécommunication au sein de ses bureaux (article 5.a). Ce premier point est étayé par les dispositions de l'article 37, paragraphe 2, qui impliquent que ce traitement est licite s'il a lieu "aux fins de la gestion du budget des télécommunications et du trafic ...".

3. Qualité des données

Les données doivent être "*adéquates, pertinentes et non excessives*" (article 4.1.c du règlement (CE) 45/2001) au regard des finalités pour lesquelles elles sont collectées, à savoir la gestion des données professionnelles. Les données traitées, décrites au début de cette opinion, doivent être considérées comme remplissant ces qualifications par rapport au traitement.

Concernant les appels téléphoniques professionnels, les données les concernant doivent être examinées à la lumière de la règle de la proportionnalité contenue dans le règlement (CE) 45/2001. Certaines données semblent excessives au regard de cette proportionnalité, et il semble qu'il soit suffisant de ne mentionner que le numéro et le coût. Les autres ne sont pas nécessaires.

Concernant la case "approved", étant donné que nous n'effectuons pas un contrôle préalable du système qui gère les appels téléphoniques et que par ailleurs, il est établi que ce ne sont que appels professionnels, le Contrôleur européen de la protection des données n'a pas à se prononcer sur l'utilité d'une telle case.

L'indication de la base salariale ne semble avoir aucune utilité, c'est pourquoi le Contrôleur européen de la protection des données recommande son retrait.

Par ailleurs les données doivent être *traitées loyalement et licitement* (article 4.1.a du Règlement (CE) 45/2001). La licéité a déjà fait l'objet d'une analyse. Quant à la loyauté, dans le cadre d'un sujet aussi sensible, elle doit faire l'objet de beaucoup d'attention. Elle est liée aux informations qui doivent être transmises à la personne concernée (voir infra, point 8).

Enfin les données doivent être "*exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables sont prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées*". (article 4.1.d du règlement). La fiche d'informations sur le processus Manager Desktop mentionne clairement le droit de rectification ouvert au personnel et le moyen de l'effectuer. L'article 4.1.d du règlement est en l'espèce bien respecté.

4. rétention des données

L'article 4.1.e du Règlement (CE) 45/2001 pose le principe que les données doivent 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*".

Concernant la rétention des données elles mêmes, il n'y a pas d'indication, ce ne peut être que sur le très long terme. Au-delà de la base de données elle-même, ces données sont certainement conservées sur le long terme puisqu'elles retracent toute la carrière de la personne. Quid des garanties appropriées ? La conservation des données sur le long terme devrait néanmoins être accompagnée de garanties appropriées. ? Le Contrôleur européen recommande la mise en oeuvre de garanties appropriées pour l'utilisation de ces données après la fin du contrat à la Banque européenne d'investissement.

Accès des managers, le temps qu'ils sont managers. Doit-on développer ?

La perspective que les données soient conservées pour des raisons historiques, statistiques ou scientifiques est exclue dans la notification.

Concernant la rétention des données sur les appels téléphoniques, l'information nous est donnée que les données sont effacées mois par mois, après la mise à jour de la liste (une fois par mois). Les conditions de l'article 37.2 sont respectées (6 mois). Par ailleurs, sachant qu'il ne s'agit pas ici d'effectuer le contrôle préalable du système qui gère la liste des appels professionnels et que les données sont effacées rapidement, l'ensemble est conforme aux dispositions du règlement (CE) 45/2001.

5. Changement de finalité, usage compatible

L'utilisation du numéro personnel de l'agent permet de dire que la plupart des données sont extraites des bases de données du personnel. Le traitement analysé n'implique pas un changement général de la finalité prévue pour les bases de données relatives au

personnel et n'est pas non plus incompatible avec cette finalité. Ceci implique que l'article 6.1 du Règlement (CE) 45/2001 n'est pas d'application en l'espèce et que l'article 4.1.b du Règlement est respecté.

6. transfert des données

Il n'y a pas de transfert dans le sens où Manager Desktop est en quelque sorte une consultation électronique du dossier personnel. Et certaines parties de ce dossier sont l'objet d'un contrôle préalable. Par contre des données relatives au trafic sont transférées par les personnes responsables de la gestion de la facturation, du trafic ou du budget (demander à M. Minnaert par qui est géré cette liste des appels ?) vers cette base de données. Est-il nécessaire de l'étudier ?

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

La Banque européenne d'investissement utilise le numéro de personnel. L'utilisation d'un identifiant n'est, en soi, qu'un moyen -légitime, en l'espèce- de faciliter le travail du responsable du traitement des données à caractère personnel; toutefois, cette utilisation peut avoir des conséquences importantes. C'est d'ailleurs ce qui a poussé le législateur européen à encadrer l'utilisation de numéros identifiants par l'article 10§6 du Règlement, qui prévoit l'intervention du contrôleur européen. En l'espèce, l'utilisation du numéro de personnel peut avoir pour conséquence de permettre l'interconnexion de données traitées dans des contextes différents. Il ne s'agit pas ici d'établir les conditions dans lesquelles la Banque européenne d'investissement peut traiter le numéro personnel, mais de souligner l'attention qui doit être portée à ce point du Règlement. En l'espèce, l'utilisation du Numéro Personnel par la Banque européenne d'investissement est raisonnable car l'utilisation de ce numéro est un moyen de faciliter le travail du traitement.

8. Information des personnes concernées

Il est indiqué dans la notification que les personnes concernées, en l'occurrence le personnel de la Banque européenne d'investissement, sont informées par le biais des dispositions administratives, de la page Ressources Humaines d'Intranet et les notes de services.

Les dispositions de l'article 11 sur l'information de la personne concernée sont applicables en l'espèce. Les dispositions mentionnées aux points a) (identité du responsable du traitement), b) (finalités du traitement) c) (destinataires ou catégories de destinataires des données) d) (caractère obligatoire ou facultatif de la réponse aux questions ainsi que les conséquences éventuelles d'un défaut de réponse) (est -ce applicable ?) et paragraphe e) ("*l'existence d'un droit d'accès aux données le concernant et de rectification de ces données*") sont bien respectées.

La mention des données sur les appels téléphoniques professionnels est manquante. La note d'information et la communication au personnel doivent être modifiées en ce sens. Il en est de même concernant l'absence de la mention de la base salariale. Elles

ne sont pas mentionnées non plus dans la notification au contrôleur. La licéité du traitement doit être reflétée dans la note d'information et la communication au personnel. C'est pourquoi le Contrôleur européen de la protection des données demande à ce que les deux notes soient rectifiées en conséquence.

Néanmoins, à aucun moment n'est indiqué dans la notification ou dans ses annexes les possibilités suivantes : le paragraphe f) de ce même article qui fait part des informations non obligatoires (*base juridique du traitement, délais de conservation des données, droit de saisir à tout moment le contrôleur européen de la protection des données*). Ceci permet de garantir la loyauté du traitement. Ces éléments devraient être indiquées à la personne devant être informée.

Au regard de ces différentes considérations, le Contrôleur européen de la protection des données souhaite que les informations mentionnées au point f de l'article 11 du règlement et ce à tous les niveaux d'information (communications au personnel, notes d'informations, page Ressources Humaines intranet, ...) ainsi que tout autre moyen approprié.

9. Droits d'accès et de rectification

L'article 13 du règlement (CE) 45/2001 dispose du droit à l'information - et de ses modalités - à la demande de la personne concernée par le traitement. Dans la notification la mention est faite à la possibilité d'accès par un membre du personnel à son dossier, ainsi que dans la note d'information.

En l'espèce, l'article 13 du règlement (CE) 45/2001 est bien respecté.

10. Sécurité

Conformément à l'article 22 du Règlement (CE) 45/2001 relatif à la sécurité des traitements, *"le responsable du traitement met en oeuvre les mesures techniques et organisationnelles appropriées pour 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"*.

L'unique mesure de sécurité est l'existence d'un simple mot de passe du manager pour consulter cette base de données. Si ce dernier donne ou se fait dérober son mot de passe, toutes les possibilités de consultation deviennent possibles. Ceci semble relativement insuffisant au regard du traitement de données sensibles. Des mesures adéquates doivent être envisagées.

Le Contrôleur européen de la protection des données recommande la mise en place de mesures de sécurité plus strictes pour la consultation de cette base de données par les managers.

Conclusion

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

- ne mentionne que les données nécessaires au regard de la proportionnalité mentionnée à l'article 4.1.c. Il semble qu'il soit suffisant de ne mentionner que le numéro et le coût. Les autres ne sont pas nécessaires.

- retire la mention de la base salariale. Cette indication ne semblant avoir aucune utilité.

- mentionne dans la note d'information et dans la communication au personnel le fait que les appels téléphoniques professionnels ainsi que la base salariale (le temps que cette dernière soit effacée des données) sont des données apparaissant dans la base Manager Desktop. La licéité du traitement doit être reflétée dans la note d'information et la communication au personnel. La note d'information et la communication au personnel doivent être modifiées en conséquence.

- mentionne les informations citées au point f de l'article 11 (*base juridique du traitement, délais de conservation des données, droit de saisir à tout moment le contrôleur européen de la protection des données*) du règlement et ce à tous les niveaux d'information (communications au personnel, notes d'informations, page Ressources Humaines intranet, ...) ainsi que tout autre moyen approprié.

- mette en place de mesures de sécurité plus strictes pour la consultation de cette base de données par les managers.

Bruxelles, le XXX 2005

Peter HUSTINX