Avis sur la notification d'un contrôle préalable reçue du DPD de la Banque Européenne d'Investissement (BEI) à propos du dossier Gestion du Temps (GDT)

Bruxelles, le 26 juin 2006 (Dossier 2004-306)

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 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".

1.2. A partir des inventaires reçus des délégués à la protection des données, le CEPD a identifié des thèmes prioritaires parmi lesquels les dossiers contenant des données relatives a la santé.

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.

1.4. Le 2 février 2006, le CEPD a reçu la notification pour contrôle préalable le traitement des données dans le cadre du dossier "Gestion du Temps" de la BEI.

1.5. Le 3 février 2006, une demande d'informations supplémentaires à été adressée au DPD de la BEI. Une réponse a été fournie par le DPD le 16 février 2006.

1.6. Le 10 mars 2006 le CEPD a demandé une réunion d'information sur l'application "Gestion du Temps". Cette réunion a eu lieu le 18 mai 2006 en présence de Monsieur Burré de la BEI et de Madame Louveaux du CEPD.

1.7. Le 20 juin 2006 le CEPD a suspendu le délai pour rendre son avis pour 10 jours afin de permettre au responsable du traitement de d'apporter des informations complémentaires et au CEPD de les intégrer.

2. Examen de l'affaire

2.1. Les faits

En vertu du Règlement du personnel de la BEI, le total hebdomadaire des heures de travail est fixé à 40 heures pour les membres du personnel travaillant à temps plein basé sur une

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

moyenne d'heures de 8 heures par jour ouvrable. Des dispositions relatives aux temps partiels adaptent ces heures en fonction. Des mesures de récupération des heures supplémentaires sont prévues.

Afin de permettre à la banque et à son personnel de gérer de façon semi-automatisée les présences/absences, incluant les heures supplémentaires, congés et maladies et autres absences, la BEI a mis en place un système "Gestion du temps" (GDT).

Tous les membres du personnel de la BEI, à l'exception des membres du Comité de direction, enregistrent leurs entrées et sorties dans un système électronique (pointeuse) au moyen de leurs cartes de services. Tout enregistrement est respectivement qualifié d'"entrée" ou de "sortie". En cas d'oubli d'un pointage, les heures seront inversées et les heures prestées ne seront pas exactes. Ce type d'erreur sera automatiquement reconnu par le système et nécessitera une correction manuelle de la part de la personne concernée à partir de l'application GDT sur son PC. En cas de correction, le système ajuste automatiquement les heures de présence en fonction. L'application permet également d'insérer les heures de travail pendant lesquelles les membres du personnel ont du effectuer d'autres missions pour la BEI et pendant lesquelles elles étaient absentes du bureau (TEX: travail à l'extérieur).

Les membres du personnel peuvent également introduire des demandes de congé, des absences pour maladie (sans certificat) et des absences pour récupération d'heures supplémentaires. Les demandes de congé et de récupération d'heures supplémentaires doivent être validées par un supérieur hiérarchique. Dès qu'une demande est formulée elle apparaît sur l'écran du supérieur. Si la demande est validée, un "ok" s'affichera, sinon un "no" apparaît à côté de la demande. Une absence pour maladie sans certificat médical ne nécessite pas de validation par la hiérarchie.

L'application GDT permet à chaque agent d'avoir un listing mensuel concernant ses propres présences/absences: les heures à faire pendant le mois concerné, le nombre d'heures reportées du/des mois précédents, le total des heures prestées par jour, le total des heures faites pendant le mois affiché, l'excédent/déficit à la fin du mois. L'écran indiquera les jours de congé de base, le report de l'année précédente, les congés supplémentaires (par exemple en vertu de l'âge, pour missions, en vertu du centre d'intérêt).

Une option de GDT permet d'informer la personne concernée, ainsi que la hiérarchie, de la moyenne d'heures de travail en excès par rapport à la durée standard, pendant une période de 4 mois. Une durée maximale d'heures supplémentaires pendant une période de 20% est permise. Au-delà de ces 20% la personne sera avertie. Il en va de même pour sa hiérarchie. Cette option vise inciter les supérieurs hiérarchiques à être vigilants par rapport aux heures excédentaires dépassant un certain plafond afin de promouvoir le bien être au travail et la conciliation entre la vie professionnelle et familiale.

L'option "Présent/absent" permet de vérifier si une autre personne est présente ou non au bureau à une heure précise ou un jour particulier et s'il est possible de la joindre par téléphone. Chaque agent aura accès aux données "Présent/absent" des personnes dans sa propre division. L'application indiquera par un code couleur la raison de l'absence (congé annuel, congé, maladie, maternité, mission, autres).

L'option "délégation d'accès" permet à tout membre du personnel de déléguer l'accès personnel à ses données à une personne de son choix. Cette option permet de modifier les données mais ne donne pas accès aux données des personnes sous la hiérarchie de la personne délégant.

Les directeurs auront accès non seulement aux demandes de validation de congés ou de récupérations d'heures mais peuvent également visualiser les comptes individuels d'heures du personnel sous leur autorité. Ils peuvent visualiser le calendrier indiquant la disponibilité du personnel sous leur responsabilité. Les directeurs ont la possibilité de déléguer le devoir d'autorisation/validation de demandes de congé, de visualisation de comptes individuels ou de calendriers (par exemple à leurs Chefs de division).

Le gestionnaire du système a accès à l'ensemble des données auxquelles l'intéressé n'a pas accès lui-même à savoir l'ajustement des droits annuels de congé (par exemple, congé spécial) et l'introduction des dates de données sans solde, congé parental, maladie avec certificat, congé de maternité.

En cas de données incomplètes ou inexactes, la personne concernée peut demander la rectification de son décompte d'heures soit directement par son accès via son PC individuel, soit en adressant un e-mail au gestionnaire du système, soit en envoyant un courrier interne au gestionnaire, soit en déléguant un accès à une autre personne de confiance.

GDT ne concerne que l'application pour gérer les présences et absences des membres du personnel :

- collectées par la pointeuse,
- corrigées par la personne concernée le cas échéant,
- validées par les directeurs.

L'application ne concerne que les heures de présence, demandes de récupérations d'heures supplémentaires et introduction des jours de congé pour maladie de moins de trois jours sans certificat médical.
D'autres informations sont importées dans GDT à partir d'autres bases de données. Il s'agit de données relatives aux missions, aux congés spéciaux, et aux congés maladie avec certificat médical. L'application GDT ne communique pas de données à d'autres bases de données.

Les données sont conservées 13 mois par l'application GDT sur chaque PC individuel. Elles sont conservées pendant 10 ans par le gestionnaire du système à des fins statistiques.

Tous les enregistrements dans GDT se font par voie du numéro personnel de l'agent.

Lors de son entrée en fonction, tout agent de la BEI reçoit un document explicatif sur l'application GDT. Ce document explique le fonctionnement du système. Il mentionne entre autres, les données reprises dans le système, les modes d'introduction de données par les agents et les possibilités d'accès pour d'autres personnes dans le système.

L’accès aux applications informatiques est sécurisé via l’accès au PC individuel de chaque agent.
La maintenance de GDT est sous-traitée à une firme de consultants qui agit au sein même de la BEI. Cette maintenance porte uniquement sur les aspects techniques. La sous-traitance est régie par un contrat entre la BEI et la firme de consultants.

2.2. Les aspects légaux

2.2.1. Contrôle préalable

La notification reçue le 2 février 2006 représente un traitement de données à caractère personnel ("toute information concernant une personne identifiée ou identifiable") selon l'article 2 sous a) du règlement. Le traitement de données dans le cadre de la gestion du temps (GDT) est effectué par une institution et est mis en œuvre pour l'exercice d'activités relevant du champ d'application du droit communautaire (article 3§1).

Par ailleurs, le traitement des données automatisé en tout ou en partie, est sujet au règlement en vertu de l'article 3 §2, ce qui est le cas du traitement présent dans la mesure où la plupart des opérations portant sur les données sont automatisées.

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. L'article 27 §2 sous b) présente comme traitements susceptibles de présenter de tels risques, "les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur compétence, leur rendement ou leur comportement". Le traitement des données personnelles dans le cadre de la Gestion du temps tombe sous le coup de l'article 27§2 sous b) dans la mesure où l'information sur les absences ou présences permet d'évaluer le comportement de la personne concernée en tant qu'heures passées au bureau. En effet, l'outil en calculant les heures prestées permet l'évaluation éventuelle de la personne concernée.

Par ailleurs, l'article 27 §2 sous a) présente comme présentant un tel risque, "les traitements de données relatives à la santé". Puisque les données concernant les absences pour maladie de moins de trois jours peuvent être introduites dans le système de gestion du temps l'article 27§2 sous a) s'applique également. De plus, des informations relatives à des congés maladie sur base de certificat médical sont également introduites et peuvent dès lors être visualisées à partir de l'écran GDT.

Gestion du temps est dès lors soumis au contrôle préalable par le CEPD.

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 février 2006. Conformément à l'article 27(4), le présent avis doit être rendu dans les deux mois qui suivent. Le délai ayant été suspendu 13 + 69 + 10 jours pour demande d'information supplémentaire, le contrôleur rendra donc son avis au plus tard le 3 juillet 2006.

2.2.2. Base légale et licéité du traitement

La base légale sur laquelle repose le traitement de données en question repose sur les articles 25 à 28, 30, 31 et 33 du Règlement du personnel de la BEI et dans les dispositions administratives n° 3 et 5 ainsi que son annexe VI sur le travail a temps partiel.

L'article 25 du règlement du personnel fixe la durée du temps de travail à 40 heures semaine et prévoit que les heures de travail seront déterminées en fonction.

En vertu de l'article 27 du règlement du personnel, tout membre du personnel doit faire connaître au service du personnel toute absence ainsi que les raisons de son absence. Par ailleurs, tout membre du personnel absent pour plus de trois jours consécutifs, doit fournir un certificat médical à partir du 4ième jour.

Le Règlement du personnel prévoit également que les membres du personnel ont droit à 24 jours de congés payés et des congés spécifiques pour des occasions particulières en vertu des dispositions particulières. Les membres du personnel peuvent faire une demande de congés non payés pour des raisons particulières pour une période de trois mois renouvelable (article 31).

En cas d'absence prolongée ou répétée non due à une maladie professionnelle ou un accident du travail, la rémunération de l'employé sera diminuée en vertu de critères établis à l'article 33 du règlement du personnel.

L'application GDT permet de gérer non seulement les horaires de travail mais également de gérer les absences et les congés en récupération. Il est également utilisé pour le comptage et le transfert des données relatives aux heures supplémentaires pouvant être récupérées.

L'analyse de la base légale s'accompagne de l'analyse de la licéité du traitement. L'article 5 sous a) du règlement 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 d'autres actes législatifs adoptés sur la base de ces traités ou relevant de l'exercice légitime de l'autorité publique dont est investie l'institution*".

La BEI exerce son droit d'organiser les heures de travail et la gestion des congés et à ce titre procède à l'exécution de missions effectuées dans l'intérêt public et sur la base d'actes adoptés sur base des traités. Les dispositions du règlement du personnel et les dispositions administratives confirment que le traitement est licite.

2.2.3. Traitement portant sur des catégories particulières de données

Le traitement des données à caractère personnel relatives à la santé est interdit à moins que des bases soient trouvées dans les articles 10§2 et/ou 10§3.

Bien que l'information reprise dans le système GDT soit enregistrée comme congés "maladie" et ne révèle pas d'informations médicales en soi, il s'agit de données "relatives à la santé" dans la mesure où elles révèlent des informations sur l'état de santé des personnes concernées.

L'article 10§2 sous b) prévoit que l'interdiction de traitement des données, ne s'applique pas lorsque le traitement est nécessaire afin de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par les traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités. Puisque la base pour le traitement des données dans le cadre de la Gestion du temps repose sur l'article 27 du règlement du personnel, ce traitement peut être considéré comme étant nécessaire afin de respecter les droits et obligations du responsable du traitement en matière de droit du travail.

2.2.4. Qualité des données

L'article 4 du règlement énonce certaines obligations en ce qui concerne la qualité des données à caractère personnel. 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" (article 4 §1 sous c).

Il ressort de la présentation faite lors de la réunion avec le gestionnaire du système ainsi que des informations reçues telles que mentionnées dans les faits, que les données sont adéquates et pertinentes au regard de la finalité déclarée.

Les données doivent être traitées loyalement et licitement (article 4 §1 sous a). La licéité a déjà été examinée et la loyauté est liée à la transparence due à l'information donnée aux personnes concernées (voir infra).

Selon l'article 4 §1 sous d) les données doivent "exactes et, si nécessaire, mises à jour". L'utilisation du numéro personnel permet notamment d'assurer l'exactitude des données lors d'une importation de données à partir d'autres bases de données. Par ailleurs, les droits d'accès et de rectification de la personne concernée constituent également un moyen d'assurer l'exactitude des données et la mise à jour en cas d'erreur de pointage (voir infra "droit d'accès et de rectification").

2.2.5. Conservation des données

En vertu de l'article 4 §1 sous e) les données à caractère personnel seront 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. Si les données sont conservées à des fins historiques, statistiques ou scientifiques, les données seront rendues anonymes ou cryptées.

Les données sont conservées 13 mois par l'application GDT sur chaque PC individuel. Elles sont conservées 10 ans par le gestionnaire du système à des fins statistiques. Ces données ne sont toutefois pas rendues anonymes.

Le CEPD approuve la conservation des données par l'application GDT pendant une période de 13 mois. Toutefois, le CEPD ne peut cautionner une conservation des données par le gestionnaire pendant une période de 10 ans. En effet, en règle générale un délai de conservation pendant 5 ans peut être approprié à condition que ce délai corresponde avec le délai de contestation ou de correction des relevés relatifs aux heures de travail ou aux absences et que soient pris en compte les droits des personnes concernées découlant des relevés de l'application. Par conséquent une durée de 5 ans peut être considérée comme approprié.

Les données pourraient être conservées à fins de statistiques relatives aux heures de travail; dans ce cas elles devront être rendues anonymes.

Le CEPD recommande dès lors que le délai de conservation à long terme soit revu.

2.2.6. Transfert des données

Le traitement doit également être examiné à la lumière de l'article 7 §1 du règlement qui prévoit que les transferts de données à caractère personnel entre institutions ou organes

communautaires ou en leur sein ne peut se faire que si les données "sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire". Par ailleurs, tout destinataire des données ne peut qu'en faire usage aux fins qui ont motivé leur transmission.

Dans le système GDT différents utilisateurs bénéficient de droits d'accès différents. Ces droits sont clairement définis. En effet, les membres d'une même division ont accès au calendrier afin de pouvoir vérifier la présence/absence d'un membre de la division; les directeurs ont accès non seulement aux demandes de validation de congés ou de récupération d'heures supplémentaires mais peuvent également visualiser les comptes individuels d'heures du personnel sous leur autorité. Ils peuvent visualiser le calendrier indiquant la disponibilité de personnel sous leur responsabilité. Ces accès peuvent être considérés comme nécessaires pour l'exécution légitime de missions relevant de la compétence du destinataire.

Les directeurs ont la possibilité de déléguer le devoir d'autorisation/validation de demandes de congé, de visualisation de comptes individuels ou de calendriers (par exemple à leurs Chefs de division). Cette délégation devrait être assortie de garanties afin d'éviter notamment que les données fassent l'objet d'un traitement pour des finalités autres que la gestion des heures de récupération.

De plus, des mesures plus strictes devraient être adoptées en ce qui concerne l'accès aux données par le gestionnaire du système puisque cette accès permet de d'élaborer un tableau relativement précis des absences/présences de chaque membre du personnel, ainsi que les heures supplémentaires effectuées ainsi que d'effectuer des statistiques individuelles. Le CEPD souhaite dès lors la mise en place de garanties spécifiques en ce qui concerne cet accès.

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

Selon l'article 10 §6, le contrôleur européen de la protection des données, "détermine les conditions dans lesquelles un numéro personnel ou tout autre identifiant utilisé de manière générale peut faire l'objet d'un traitement par une institution ou un organe communautaire".

La présente décision ne vise pas à déterminer les conditions générales d'utilisation du numéro personnel identifiant mais uniquement dans le cadre de l'application GDT. En l'espèce l'utilisation du numéro personnel à des fins d'enregistrement des données dans le système est raisonnable dans la mesure où l'utilisation de ce numéro se fait à des fins d'identification de la personne dans le système et contribue dès lors à assurer l'exactitude des données.

2.2.8. Droit d'accès et de rectification

L'article 13 du règlement prévoit un droit d'accès pour les personnes concernées à leurs données. En cas de donnée incomplète ou inexacte, la personne concernée dispose d'un droit de rectification en vertu de l'article 14 du règlement.

Le système permet à la personne concernée d'accéder à ses données par l'accès au système via son PC personnel.
Comme mentionné dans les faits, en cas de données incomplètes ou inexactes, elle peut demander la rectification de son décompte d'heures soit directement par son accès via son PC individuel, soit en adressant un e-mail au gestionnaire du système, soit en envoyant un courrier interne au gestionnaire, soit en déléguant un accès à une autre personne de confiance. Cette possibilité d'accès permet donc à la personne concernée d'exercer son droit d'accès et de rectification.

2.2.9. Information des personnes concernées

Les articles 11 et 12 du règlement (CE) 45/2001 prévoient que la personne concernée doit être informée lorsqu'il y a traitement de ses données personnelles et énumère une série de mentions obligatoires dans cette information. Dans le cas présent, une partie des données est collectée directement auprès de la personne concernée, une partie est collectée auprès d'autres sources. Les deux articles sont dès lors d'application.

Comme mentionné dans les faits, lors de son entrée en fonction, tout agent de la BEI reçoit un document explicatif sur l'application GDT. Ce document explique le fonctionnement du système. Il mentionne entre autres, la finalité du système, les données reprises dans le système, les modes d'introduction de données par les agents ainsi que la possibilité de corriger les données inexactes et les possibilités d'accès pour d'autres personnes dans le système (destinataires des données). Au regard des dispositions du règlement le CEPD souhaiterai que les membres du personnel concernés par le système soient également informés de l'identité du responsable du traitement, de la base juridique du traitement, et du délai de conservation des données. Elles devraient également être informées de la possibilité de saisir le contrôleur européen de la protection des données.

2.2.10. Sécurité

Conformément aux articles 22 et 23 du règlement, le responsable du traitement et le sous-traitant sont tenus de mettre en œuvre 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. Ces mesures de sécurité doivent notamment empêcher toute diffusion ou tout accès non autorisés, toute destruction accidentelle ou illicite, toute perte accidentelle ou toute altération, ainsi que toute autre forme de traitement illicite.

L'accès aux applications informatiques est sécurisé via l'accès au PC individuel de chaque agent. Au regard du caractère relativement peu sensible des données en ce qui concerne chaque membre du personnel, le CEPD considère cela comme étant adéquat.

2.2.11. Traitement des données pour le compte du responsable du traitement

L'article 23 énonce les obligations à respecter lorsque le traitement est effectué pour le compte du responsable du traitement: le responsable du traitement doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation; la réalisation de traitements doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que le sous-traitant ne peut agir que s'il a reçu des instructions à cet effet du responsable du traitement; les obligations visées aux articles 21 et 22 incombent également au sous-traitant. Aux fins de la conservation des preuves, les éléments du contrat ou de l'acte juridique relatifs à la protection des données et les exigences portant sur les mesures visées à l'article 22 sont consignés par écrit ou sous une autre forme équivalente.

La maintenance de GDT est sous-traitée à une firme de consultants qui agit au sein même de la BEI. Cette maintenance porte uniquement sur les aspects techniques. La sous-traitance est régie par un contrat entre la BEI et la firme de consultants.

Dans le contrat qui lie le sous-traitant à la BEI, il conviendra de s'assurer que les obligations du sous-traitant en matière de sécurité (articles 21 et 22 du règlement) soient mentionnées et qu'il soit stipulé que la société de sous-traitance ne peut agir que sur instruction de la BEI. Le CEPD souhaite que cette vérification soit faite et recommande, le cas échéant, que ces précisions soient apportées dans le corps du contrat.

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 délai de conservation à long terme soit revu;

- si les données sont conservées à fins de statistiques relatives aux heures de travail, elles soient rendues anonymes;

- la délégation des directeurs de la possibilité du devoir d'autorisation/validation de demandes de congé, de visualisation de comptes individuels ou de calendriers soit assortie de garanties afin d'éviter notamment que les données fassent l'objet d'un traitement pour des finalités autres que la gestion des heures de récupération;

- Des garanties soient prévues pour que le gestionnaire du système qui a accès à l'ensemble des données, ne puisse les utiliser à des fins non compatibles avec les finalités de l'application GDT;

- les membres du personnel concernés par le système soient également informés de l'identité du responsable du traitement, de la base juridique du traitement, et du délai de conservation des données et de la possibilité de saisir le contrôleur européen de la protection des données;

- dans le contrat qui lie le sous-traitant à la BEI, soient mentionnées les obligations du sous-traitant en matière de sécurité et que la société de sous-traitance ne peut agir que sur instruction de la BEI.

Fait à Bruxelles, le 26 juin 2006.

Peter HUSTINX
Le Contrôleur européen de la protection des données

Note de suivi 6 novembre 2006

En date du 27 octobre 2006, la BEI a pris en compte l'ensemble des recommandations figurant dans cet avis.

Le Contrôleur européen de la protection des données