

Avis sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Cour des Comptes à propos du traitement des données "Système de gestion et de contrôle du Flexitime "

Bruxelles, le 5 décembre 2008 (Dossier 2008-173)

1. Procédure

Le 14 mars 2008, le Contrôleur européen de la protection des données (CEPD) a reçu la notification, de la part du délégué à la protection des données (DPD), pour contrôle préalable du traitement des données "Système de gestion et de contrôle du Flexitime". Des questions ont été posées au responsable du traitement le 19 mars 2008. Les réponses ont été fournies le 26 mars 2008. D'autres questions ont été posées le 16 avril et les réponses fournies le 9 octobre 2008.

Le projet d'avis a été envoyé au DPD pour commentaires le 6 novembre 2008. Ces derniers ont été reçus le 1er décembre 2008.

2. Les faits

L'horaire flexible est institué pour permettre un meilleur aménagement et une souplesse accrue en ce qui concerne l'organisation du travail des agents. Chaque fonctionnaire ou agent est tenu de prêter au cours de chaque mois un total d'heures correspondant à 37h30 par semaine.

Le service du personnel est chargé, sous le contrôle du chef de la division du personnel, de la gestion centralisée du système.

La finalité du traitement est la suivante :

- Traitements "FLEXITIME" = Suivre et contrôler le temps de présence des agents
- Enregistrement automatique des entrées et sortie du personnel de la cour ("badgeuses")
- Enregistrement automatique des "absences" autorisées : congés, absences, missions (interface "batch")
- Enregistrement des "absences" formation par le service formation
- Enregistrement des corrections et modifications manuelles par les gestionnaires du "Flexitime"
- Consultation des horaires prestés, transactions et corrections demandées par les agents
- Consultation des horaires des subordonnés par les supérieurs hiérarchiques
- Extraction mensuelles des heures supplémentaires susceptibles d'être payées pour validation et autorisation de payer par le supérieur hiérarchique
- Extraction de données statistiques globales pour le management et l'évaluation du système
- Extraction/impression de "Fiches de pointage" individuelles sur demande du Directeur des ressources humaines ou des directeurs des services concernés.

Modalités d'application du système

- **Entrée - sortie**

Toute entrée ou sortie du bâtiment doit faire l'objet d'un pointage, auprès d'un des lecteurs de badges installés dans le hall d'entrée de chaque bâtiment et parkings. Cela s'effectue sans contact (le badge doit être à quelques centimètres du lecteur pour pouvoir être lu) ce qui signifie que le badge comporte des technologies RFID (techniques d'identification par radio fréquence).

- **Informations disponibles**

Chaque agent peut obtenir, par simple introduction de son badge d'identification dans un lecteur, son solde en débit ou en crédit d'heures. Ce solde est calculé en permanence sur base d'un horaire moyen de 7h30 par jour. L'agent peut aussi accéder, via un PC, à ses données telles qu'enregistrées sur les deux derniers mois. En début de mois, un décompte détaillé de tous les enregistrements du mois précédent est transmis à chaque agent pour contrôle. Le chef de service doit certifier les enregistrements relatifs aux missions, ou au travail exceptionnel à domicile, ne nécessitant aucun ordre de mission.

- **Enregistrement des congés et missions**

Le service du personnel et le service de la formation professionnelle sont chargés d'introduire, chacun pour ce qui le concerne, toutes les informations relatives aux :

- congés annuels et spéciaux,
- absences maladies,
- missions,
- actions de formation,

après réception des formulaires adéquats (demandes de congés, ordres de mission, déclarations de frais de mission, déclarations d'absence de maladie, autorisations de formation). Aucune intervention du personnel n'est donc nécessaire sur les matières en question.

Seul le code "type" de la "non présence" pour la journée ou la demi-journée de l'agent est enregistré dans EFFICIENT (base de données gérant le flexitime) : Mission, Congé, maladie.

- **Demande de modification des enregistrements**

Une modification des données enregistrées peut être demandée à tout moment au service du personnel. Cette demande est à introduire au moyen d'un formulaire ad hoc ou au moyen de la boîte fonctionnelle indiquant obligatoirement :

- le numéro personnel ;
- les nom et prénom ;
- le numéro de téléphone ;
- les raisons de la demande de modification précisément détaillées (par exemple : perte de la carte/ badge) ;
- le jour concerné ;
- l'horaire modifié.

- **Débit d'heures**

En vertu des dispositions de l'article 60 du Statut, le débit en fin de mois, au-delà de 15 heures, est imputé sur les droits à congé annuel à raison d'une demi-journée par tranche de 3h45. Le solde de moins de 3h45 heures non prélevé d'office est conservé en mémoire.

- **Pause déjeuner**

Tout agent est tenu de pointer entre 12h00 et 14h30, faute de quoi les dispositions du point 2.4., dernier alinéa du règlement du système, seront mises en œuvre. Les agents travaillant dans

un bâtiment autre que le bâtiment principal du Kirchberg bénéficient d'un "délai de route" de 20 minutes.

- **Absences pour visites médicales**

Pour l'application du point 2.5. du règlement du système, le système octroie automatiquement 12 minutes forfaitaires par jour au titre des absences pour consultations médicales qui ne nécessitent pas un congé spécial.

- **Activités de service à l'intérieur du Grand-Duché du Luxembourg**

Les agents devant quitter le bâtiment pour une activité de service à Luxembourg (réunions, liaison entre les bâtiments de la Cour, etc.), enregistrent leur pointage sous la rubrique "Missions à Luxembourg" (touche F1 du lecteur). Un "délai de route" forfaitaire de 10 minutes est accordé aux agents qui suivent une formation autorisée en dehors du bâtiment d'affectation. Si l'agent part directement en mission de son domicile sans avoir pu pointer ou activer la touche F1, il informe le service du personnel de la durée de la "mission", pour enregistrement, au moyen d'un formulaire ad hoc.

- **Heures de travail à domicile**

Le travail à domicile (non permanent) peut être comptabilisé, à titre tout à fait exceptionnel, à condition qu'il ait été autorisé préalablement et certifié a posteriori par le supérieur hiérarchique. L'enregistrement est effectué par le service du personnel, au moyen d'un formulaire ad hoc.

- **Heures de travail prestées le week-end et les jours fériés**

Sans préjudice des dispositions propres aux missions évoquées aux points 2.7. et 2.8. du règlement du système, le travail presté le week-end et les jours fériés peut être comptabilisé, à titre tout à fait exceptionnel et à hauteur du plafond journalier stipulé au point 2.10. du règlement de base, à condition qu'il ait été autorisé préalablement et certifié a posteriori par le supérieur hiérarchique. L'enregistrement est effectué par le service du personnel au moyen d'un formulaire ad hoc.

Interconnexion entre les bases de données : le système flexitime est géré par la base de données EFFICIENT. Cette dernière importe des données concernant les personnes, les missions et les absences (congé légal, maladie, ...) donc des bases de données SIC CONGES mais également de l'application Mission développée par la Cour puisque qu'il y a enregistrement des "absences" formation par le service formation (mais pour ce dernier cas le traitement est manuel). Concernant l'import des données des agents, une donnée a été ajoutée par la suite : flag disant si la personne fait partie des Chauffeurs ou du Helpdesk. Par ailleurs, il est aussi prévu une exportation de données vers ART (logiciel de gestion pour les auditeurs) qui a pour objectif la réconciliation des données ART - EFFICIENT¹.

Les interfaces entre les bases de données n'utilisent que le numéro de matricule. Lors de la création de la personne dans le système, le numéro de matricule est associé au numéro de badge. Il n'y a pas de validation immédiate effectuée mais si un numéro de matricule est incorrect, l'interface le signalera dans la nuit qui suit et le matricule sera corrigé manuellement.

Les personnes concernées sont tous les agents ayant un lien statutaire ou un contrat de travail avec la Cour des Comptes ou une société qui travaille pour la Cour des comptes. Tout type de membre du personnel de la Cour des comptes qui est assujéti au contrôle des horaires de présence: statutaires, contractuels, prestataires de services et experts nationaux détachés.

¹ Dossier 2008-239 en cours pour contrôle préalable.

Les données sont les suivantes :

* Personne:

- Numéro de matricule
- Nom
- Prénom
- Site (Bâtiment).
- Code du service d'affectation
- Grade
- Date début / fin du contrôle Efficient
- Type d'horaire de la personne
- N° du badge électronique de pointage
- login et mot de passe de l'interface de consultation

Au regard des données de localisation, la justification apportée par la Cour est que le règlement donne des compensations horaires différentes suivant le bâtiment dans lequel les personnes sont affectées (pour prendre en compte le temps de transport entre le siège central et les autres bâtiments). La localisation est un des paramètres du calcul de l'horaire journalier. L'information suivante est ajoutée : le lieu du pointage (identifiant de la badgeuse) n'est actuellement pas disponible via l'application (ni à l'utilisateur, ni au supérieur ou à l'administrateur, seul un technicien peut éventuellement retrouver l'information en accédant directement aux tables de la base de données). L'information est cependant présente dans la base de données mais n'est jamais visible ni utilisée.

* Supérieur hiérarchique (Directeurs, chefs de divisions/unité)

- Code(s) du(des) service(s) administré(s)
- login / password "Administrateur"

* Pointage

- N° du Badge + Date et heure du pointage

L'information des personnes concernées est effectuée via le règlement du système qui est disponible sur l'intranet de la Cour et dans l'application de consultation des horaires. Les personnes sont informées du règlement et du système lors de leur entrée en service, lors de la remise en main propre du "badge" électronique de pointage.

Concernant les droits d'accès et de rectification, l'application permet à chacun de consulter les enregistrements qui le concernent pour le mois courant et le mois précédent. Sur demande motivée de l'intéressé, une "fiche de pointage" historique (mois précédents) peut être envoyée à l'intéressé. Une correction ou modification des pointages pour le mois en cours et le mois précédent peut être demandée par l'agent aux gestionnaires via une boîte à lettre fonctionnelle. (En cas de circonstances exceptionnelles motivées, des modifications/corrections sont effectuées sur des données plus anciennes).

La procédure de traitement est automatisée et manuelle :

Traitement automatisé :

- Synchronisation journalière des données de bases des agents (Nom, matricule, code du service d'affectation, bâtiment, groupe de fonction, grade) à partir de la base de données du personnel
- Synchronisation journalières des absences "autorisées" à partir des systèmes SIC-Congés et Missions

Traitement manuel :

- Création des nouveaux agents (attribution du "Badge", login et password)
- Enregistrement des "formations" par le service formation
- Enregistrement des corrections et modifications envoyées par les agents (via boîte à lettre fonctionnelle)
- Extraction mensuelle du rapport "Heures supplémentaires" pour l'équipe en charge du paiement éventuel (sous réserve de validation / acceptation)
- Extraction/impression sur demande du Directeur des ressources humaines de "fiches de pointage" individuelles.

Quant au support de stockage, les données "Flexitime" sont gérées et stockées dans un système et une base de données indépendante dénommée "EFFICIENT". Cette base de données SQL Server est située sur un serveur dédié à l'application EFFICIENT.

Quelle que soit la technologie utilisée, il existe un numéro de carte. Ce numéro n'est pas utilisé pour d'autres finalités que celle du flexitime. Le numéro de badge ne sert que dans EFFICIENT. Un programme Windows tourne en permanence sur le serveur, assurant les transferts entre les badgeuses et la base de données. En cas de coupure de la connexion entre le serveur et une badgeuse, cette dernière conserve les données.

Les destinataires sont : la Division des Ressources humaines et tous les Directeurs, Chefs d'unités, pour le personnel affecté dans chaque entité, AIPN, le comptable pour paiement des heures supplémentaires, contrôleurs internes ou externes dans le cadre d'un audit, le cas échéant le service juridique. L'accès complet à la base de données est donné uniquement à l'Administrateur DB et à son backup. Tous les autres accès se font via l'interface web de l'application.

Il existe plusieurs populations d'utilisateurs : Administrateurs (consultation et modification des paramètres de l'application et des horaires des agents), Formation (consultation et ajout de formations), Responsable (consultation des données des personnes de son service), Utilisateur (consultation de ses propres données de pointage pour le mois en cours et le mois précédent).

Au regard de la conservation des données, elles peuvent être conservées jusqu'à l'extinction des droits et des possibilités de recours (5 ans). L'effacement des données lors de la cessation de fonction à l'issue de la détermination des droits financiers et sous réserve de recours est prévu dans les 18 mois après la cessation de fonction. Le logiciel EFFICIENT conserve toutes les données, y compris les entrées/sortie dans une base de données centralisée qui est construite de façon "incrémentale": les données d'aujourd'hui sont basées sur celles du mois précédent, qui sont basées sur le mois précédent et ainsi de suite. Dans ce logiciel, il n'est pas prévu de pouvoir effacer certaines données individuelles (par exemple, les pointages individuels): on ne peut effacer que l'ensemble des données couvrant une période du passé. (Si on efface les entrées/sortie d'une personne dans le passé, le système va considérer automatiquement que la personne n'a pas pointé à ces dates et recalculer toutes les données jusqu'à aujourd'hui). C'est pourquoi, il est prévu que, dès que l'AIPN constatera que l'ensemble des données d'une année n'est plus utile, mais en tout cas au maximum après 5 ans, l'ensemble des données de l'année dans la base de données sera effacé, ceci inclut les codes de "non-présence" des journées ou demi-journées et les pointages enregistrés de tous les agents. Les données de badgeuses ne sont conservées que temporairement jusqu'à ce qu'elles soient chargées dans la base de données. La gestion impose régulièrement de pouvoir retrouver le détail des pointages longtemps dans le passé: le cas le plus classique, étant une personne qui revient après un long congé ou une longue absence (les congés de convenance personnelle sont souvent de plusieurs années) et qui est soit réintégrée (il faut reprendre la situation telle qu'elle était à son départ) soit quitte

l'institution (il faut, dans certains cas, lui payer ou lui demander de rembourser les heures prestées avec les justificatifs appropriés et pouvoir répondre aux recours éventuels).

L'effacement des données personnelles est une procédure comprise entre 3 et 6 mois dès la départ ceci afin de permettre la liquidation des effets financiers. Dans certains cas exceptionnels, la procédure peut être plus longue. Sur demande et sous réserve de recours, la personne n'exerçant plus de fonction au sein de la Cour des comptes peut demander l'effacement des données qui la concerne. L'effacement se fait dans les 18 mois. Pour les agents qui travaillent encore et sur demande le **blocage** des données contestées par la personne concernée est faisable immédiatement.

Sur demande de l'AIPN, pour les besoins de suivi des évolutions des usages du "Flexitime" des rapports statistiques globaux peuvent être produits : ils ne contiennent pas de données individuelles. A ce stade et faute de moyens informatiques, il n'a pas été mis en place d'environnement de "reporting" pour EFFICIENT : l'analyse des besoins du management pour ces rapports statistiques devrait démarrer en 2009. Il ne s'agirait en tout cas que de rapports statistiques "anonymes" globaux statistiques (heure d'arrivée/départ moyenne, durée de la pause "standard", nombre d'heures par jours...) destinés à évaluer le système d'horaire variable dans son ensemble, par exemple, lors d'une révision de la réglementation. Cela avait été prévu lors du lancement d'EFFICIENT mais le besoin ne semble ni prioritaire, ni urgent mais l'AIPN désire se réserver la possibilité de la faire dans le futur si elle le trouve nécessaire.

Les mesures de sécurité sont garanties et traitées par le service informatique. La génération de l'exportation est effectuée via un script tournant directement sur le serveur EFFICIENT (accès limité à l'administrateur système et à son backup). L'accès à la base Oracle est également protégé par login/mot de passe (accès limité à l'administrateur ART et à son backup). L'administrateur et son back up qui gèrent la base de données EFFICIENT appartiennent à la Direction de l'Informatique et des Télécommunications, service "**Développement**".

- Les mesures de sécurité de l'ensemble du système sont [...].

3. Les aspects légaux

3.1. Contrôle préalable

La gestion des données concernant les dossiers relatifs aux absences, aux différents types de congés et aux horaires de présence constitue un traitement de données à caractère personnel ("toute information concernant une personne physique identifiée ou identifiable (...) " article 2.a du règlement (CE) 45/2001). Le traitement de données présenté est effectué par une Institution et est mis en œuvre pour l'exercice d'activités relevant du champ d'application du droit communautaire.

Les données gérées par EFFICIENT, application de la Cour des Comptes, sont traitées de façon tant automatisée que manuelle. Elles sont donc constitutives d'un traitement partiellement automatisé (article 3.2 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 les traitements présentant des risques particuliers au regard des droits et libertés des personnes concernées. Le CEPD estime que l'insertion de technologies telles que les techniques d'identification par radio fréquence (RFID) représente un risque spécifique. C'est pourquoi les

dossiers gérés par l'interface EFFICIENT représentent un traitement de données personnelles entrant dans le cadre de l'article 27.1 du règlement.

En principe, le contrôle effectué par le CEPD est préalable à la mise en place du traitement. A défaut, 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 CEPD.

La notification officielle a été reçue par e-mail en date du 14 mars 2008. Un délai de 25 jours a été octroyé afin de permettre au DPD d'apporter ses commentaires sur le projet d'avis du CEPD. Conformément à l'article 27.4 du règlement, le CEPD rendra donc son avis au plus tard le 8 décembre 2008 (15 mai + 145 jours de suspension + mois d'août + 25 jours pour commentaires).

3.2. Licéité du traitement

La licéité du traitement doit être examinée à la lumière de l'article 5.a du règlement (CE) 45/2001 qui 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 investi l'institution ou l'organe communautaire ou le tiers auquel les données sont communiquées"*.

Dans le présent dossier, les personnes en charge de la gestion de la base de données EFFICIENT interviennent dans le cadre d'une mission effectuée dans l'intérêt public sur base du Statut des fonctionnaires des Communautés européennes et du régime applicable aux autres agents des Communautés européennes.

La base légale sur laquelle repose le traitement de données en question repose sur les articles:

Base légale pour le travail à temps partiel :

- Article 55 bis et l'Annexe IV bis dudit Statut, article 55 ter du Statut sur les activités à mi-temps,

Base légale pour l'horaire flexible:

- Article 55 du Statut.
- Règlement "Modification du règlement de base instituant un horaire de travail flexible" COM PER 34/2005 du 17 juin 2006.

Base légale pour les heures supplémentaires :

- Article 56 du Statut

L'ensemble de ces bases légales est donc conforme et vient à l'appui de la licéité du traitement.

3.3. Qualité des données

"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.c du règlement).

Les données traitées dans le cadre du présent dossier décrites ci-dessus semblent globalement pertinentes et adéquates. .

Les données de localisation méritent une analyse particulière. La justification avancée par la Cour réside dans le fait que le règlement donne des compensations horaires différentes suivant le bâtiment dans lequel les personnes sont affectées (pour prendre en compte le temps de

transport entre le siège central et les autres bâtiments). La localisation est un des paramètres du calcul de l'horaire journalier. La donnée est présente dans le système mais non accessible sauf par un technicien. La manière dont sont traitées ces données, c'est à dire avec l'impossibilité pour le supérieur hiérarchique d'y avoir accès, est satisfaisante au regard du principe de qualité des données du règlement 45/2001. Par ailleurs le maintien de ces données dans le système et qui évite le contrôle par le supérieur hiérarchique permet la possibilité de rectification en cas de problème ou contestation.

Au regard des rapports statistiques globaux qui peuvent être produits sur demande de l'AIPN, pour les besoins de suivi des évolutions des usages du "Flexitime", ces rapports ne contiennent pas de données individuelles. Pour mémoire, il n'existe pas encore de fonction reporting dans EFFICIENT : l'analyse des besoins du management pour ces rapports statistiques devrait démarrer en 2009. Il ne s'agirait en tout cas que de rapports statistiques "anonymes" globaux (heure d'arrivée/départ moyenne, durée de la pause "standard", nombre d'heures par jours...) destinés à évaluer le système d'horaire variable dans son ensemble, par exemple, lors d'une révision de la réglementation.

A cet égard le CEPD se réjouit que cette perspective soit envisagée dans un cadre d'anonymisation et considère l'article 4.1.e. respecté.

Par ailleurs, les données doivent être "traitées loyalement et licitement" (article 4.1.a du règlement). La licéité a déjà fait l'objet d'une analyse dans le point 3.2 de cette opinion. Quant à la loyauté, elle est liée aux informations qui doivent être transmises à la personne concernée (voir ci-dessous point 3.9).

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 effacés ou rectifiées" (article 4.1.d du règlement). Le programme Windows qui tourne en permanence sur le serveur, assurant les transferts entre les badgeuses et la base de données, permet de garantir la mise à jour des données. En cas de coupure de la connexion entre le serveur et une badgeuse, cette dernière conserve les données. Enfin dans le cadre de l'interconnexion des bases de données, l'utilisation du numéro personnel, qui facilitera l'interconnexion entre les différentes bases de données, a pour objectif de supprimer les inexactitudes qui pourraient apparaître dans le système central si les autres bases de données alimentant celui-ci ne sont pas synchronisées et que le système central n'est pas mis à jour. Les interconnexions entre les différents systèmes visent à améliorer la cohérence et l'exactitude des données. Le CEPD considère l'article 4.1.d respecté.

Les droits d'accès et de rectification de la personne concernée constituent également un moyen d'assurer l'exactitude et la mise à jour des données la concernant (voir également "droit d'accès et de rectification", point 3.8).

3.4. Conservation des données

Les données à caractère personnel 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. (...)*" (article 4.1.e du règlement). Conformément à l'article 4, paragraphe 1, lorsque des données à caractère personnel sont conservées au-delà de la période précitée à des fins historiques, statistiques ou scientifiques, il convient de les conserver sous une forme qui les rend anonymes ou de crypter l'identité de la personne concernée.

Les données peuvent être conservées jusqu'à l'extinction des droits et des possibilités de recours (5 ans). Le logiciel EFFICIENT conserve toutes les données, y compris les entrées/sortie dans une base de données centralisée.

La Cour justifie également la durée des 5 années par le fait que la gestion impose régulièrement de pouvoir retrouver le détail des pointages longtemps dans le passé: le cas le plus classique, étant une personne qui revient après un long congé ou une longue absence.

Le CEPD estime la durée de rétention des données excessive au regard de la finalité du traitement. Il tient à rappeler la règle applicable à la conservation des données qui a été présentée dans le cadre de différents dossiers relatifs au flexitime². En effet, pour ce qui est de l'aspect relatif à la conservation des données, il est souligné que les données concernant l'horaire flexible doivent être conservées pendant l'année calendrier en cours et être supprimées après clôture de la procédure de transfert à l'année suivante des jours de congé annuel non utilisés, et au plus tard à la fin du mois de mars de l'année suivante.

Le CEPD considère l'argument des 5 années en raison des recours non recevable. En effet, les recours seront formés dans l'année qui suit l'enregistrement des données, et dans ce cas effectivement les données, mais uniquement celles de la personne concernée, seront conservées (blocking), le temps que les procédures de recours soient terminées. Ceci ne justifie pas que l'ensemble des données de la base soit conservé pendant 5 ans. Par ailleurs l'argument relatif à la personne qui revient après un long congé ou absence n'est pas non plus fondé. Il appartient aux services Ressources Humaines d'établir un relevé des heures prestées avant le départ de la personne concernée.

Le CEPD recommande qu'une nouvelle durée fixe soit établie, de préférence 3 mois. La procédure des cas exceptionnels envisagés ne pourrait concerner que les hypothèses de contestation des données. Dans le cadre de cette dernière hypothèse, les données devront être marquées comme contestées.

Sur demande et sous réserve de recours, la personne n'exerçant plus de fonction au sein de la Cour des comptes peut demander l'effacement des données qui la concerne. L'effacement se fait dans les 18 mois. Pour les agents qui travaillent encore et sur demande le blocage des données de la personne concernée est faisable immédiatement. Le verrouillage des données est possible endéans 1 jour. L'effacement des données personnelles est une procédure comprise entre 3 et 6 mois dès la départ ceci afin de permettre la liquidation des effets financiers. Dans certains cas exceptionnels, la procédure peut être plus longue.

Le CEPD estime également la durée de 18 mois excessive pour l'effacement des données des personnes ayant quitté la Cour. Dans d'autres cas, le CEDP a estimé qu'une durée de 15 jours était proportionnelle à la finalité du traitement. Le CEPD recommande également la réévaluation de la durée nécessaire à l'effacement des données des personnes ayant quitté la Cour.

3.5. Changement de finalité / usage compatible

Des données sont extraites de ou introduites dans les bases de données du personnel. Le traitement des données a pour objet la gestion et le contrôle du flexitime (règles relatives à l'horaire flexible ainsi que la gestion des horaires de travail et des absences via un système automatisé). L'interconnexion entre les bases de données (EFFICIENT - SIC CONGES -

² Dossiers 2007-063 Sysper 2 : module Time Management de la Commission, 2007-218 Flexitime DG INFSO (site web du CEPD).

application Mission de la Cour) constitue un outil technique visant à faciliter le transfert de données à caractère personnel entre différents services (service Congés, ressources humaines, supérieur hiérarchique direct, responsable formation). Ce traitement est nécessaire à l'exécution légitime des missions liées au personnel et relevant de la compétence de ces services : heures supplémentaires, suivi des congés, planification des ressources humaines au sens étroit du terme et compensation des heures supplémentaires, formations et missions.

Le traitement analysé n'implique pas un changement général de la finalité prévue pour les bases de données relatives au personnel, la gestion des horaires et absences n'en étant qu'une partie. 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, étant donné que les finalités sont compatibles.

3.6. Transfert des données

Le traitement doit également être examiné à la lumière de l'article 7.1 du règlement. L'article 7 du règlement prévoit que *"les données à caractère personnel ne peuvent faire l'objet de transferts entre institutions ou organes communautaires ou en leur sein que si elles sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire."*

Les destinataires sont : la Division des Ressources humaines et tous les Directeurs, Chefs d'unités, pour le personnel affecté dans chaque entité, AIPN, le comptable pour paiement des heures supplémentaires, contrôleurs internes ou externes dans le cadre d'un audit, le cas échéant le service juridique. L'accès complet à la base de données est donné uniquement à l'Administrateur DB et à son backup. Tous les autres accès se font via l'interface web de l'application.

Le CEPD estime que ce partage d'informations est *nécessaire à l'exécution légitime de missions relevant de la compétence des destinataires*. En effet, ce traitement relève de la compétence des différents services de la Cour (Ressources Humaines, Informatique ...) et le transfert est licite dans la mesure où la finalité est couverte par les compétences des destinataires.

Néanmoins le responsable du traitement doit définir précisément les rôles et attributions de chaque utilisateur en fonction du critère de nécessité pour l'exercice de sa mission. Le CEPD recommande que les utilisateurs n'aient accès qu'aux données dont on peut raisonnablement penser qu'elles sont nécessaires à l'accomplissement de leur mission. Des garanties devraient être prévues pour que l'accès aux données à caractère personnel soit réservé aux seules personnes autorisées à en recevoir communication. De plus, les personnes ayant accès aux données enregistrées dans le système central doivent être informées qu'elles ne peuvent pas les utiliser à des fins non compatibles avec les finalités du système Flexitime.

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

L'article 10, paragraphe 6, du règlement prévoit que *"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."*

Le CEPD a déjà précisé le statut du numéro de la puce RFID³. Le numéro d'identification associé à la puce RFID est une des données à caractère personnel visées par le règlement 45/2001. En effet, lorsqu'il est utilisé pour enregistrer le comportement d'un agent et est relié au numéro personnel (c'est-à-dire lié au nom d'une personne, comme c'est le cas ici), ce numéro d'identification fait que le traitement relève de la catégorie des traitements de données à caractère personnel, ce qui impose le respect des principes s'appliquant à la protection des données.

L'utilisation du numéro personnel par la Cour ainsi que le numéro de badge coexistent dans le système Flexitime. Le numéro de badge est nécessaire puisqu'il sera utilisé pour pointer à l'entrée et à la sortie en utilisant les lecteurs de badges. En l'espèce, l'utilisation du numéro personnel d'un agent à des fins d'enregistrement des données dans le système est raisonnable puisque l'utilisation de ce numéro se fait à des fins d'identification de la personne dans le système et de suivi du dossier et ce afin de faciliter le travail du traitement et contribue dès lors à assurer l'exactitude des données. Dès lors l'article 10.6 est respecté.

3.8. Droit d'accès et de rectification

L'article 13 du Règlement dispose du droit d'accès - et de ses modalités - à la demande de la personne concernée par le traitement. L'article 14 du Règlement dispose du droit de rectification pour la personne concernée.

L'application permet à chacun de consulter les enregistrements qui le concernent pour le mois courant et le mois précédent. Sur demande motivée de l'intéressé, une "fiche de pointage" historique (mois précédents) peut être envoyée à l'intéressé. Une correction ou modification des pointages pour le mois en cours et le mois précédent peut être demandée par l'agent aux gestionnaires via une boîte à lettre fonctionnelle. (En cas de circonstances exceptionnelles motivées, des modifications/corrections sont effectuées sur des données plus anciennes).

Le CEPD estime que les conditions des articles 13 et 14 du règlement sont remplies sous réserve de la correction nécessaire à apporter à la durée (voir point 3.4 rétention des données). Quant aux droits d'accès accordés aux personnes autre que la personne concernée, voir infra mesures de sécurité (point 3.11).

3.9. Information des personnes concernées

Le règlement (CE) 45/2001 prévoit 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 et d'autres données auprès d'autres personnes.

Les dispositions de l'article 11 (*Informations à fournir lorsque les données sont collectées auprès de la personne concernée*) sur l'information de la personne concernée sont applicables en l'espèce puisque la personne concernée encode elle-même ses données.

Les dispositions de l'article 12 (*Informations à fournir lorsque les données n'ont pas été collectées auprès de la personne concernée*) sur l'information de la personne concernée sont aussi applicables en l'espèce, puisque des informations peuvent être encodées par le chef d'unité ou son secrétariat titulaire d'une délégation ad hoc.

³ Voir Dossier Flexitime DG INFSO 2007-218.

L'information des personnes concernées dans le cadre d'EFFICIENT est effectuée via le règlement du système qui est disponible sur l'intranet de la Cour et dans l'application de consultation des horaires. Les personnes sont informées du règlement et du système lors de l'entrée en service, lors de la remise en main propre du "badge" électronique de pointage. Néanmoins ce règlement du système ne fournit aucune autre des mentions reprises aux articles 11 et 12 du règlement 45/2001 que le droit d'accès et de rectification. Le CEPD recommande que soit ajouté à ce règlement l'ensemble des dispositions des articles 11 et 12 du règlement 45/2001, afin que l'information des personnes concernées soit complète et exhaustive.

3.10. Sécurité

Conformément à l'article 22 du règlement (CE) 45/2001 relatif à la sécurité des traitements, *"le responsable du traitement met 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"*.

Les mesures de sécurité sont [...].

[...] Le CEPD recommande par contre que la protection des données soit garantie le mieux possible contre la duplication du badge et la possibilité de tracer les déplacements du détenteur du badge. [...]

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 Cour réévalue la durée nécessaire à l'effacement des données des personnes ayant quitté l'Institution, fixe une durée déterminée pour l'effacement des données des agents travaillant à la Cour et prévoit le marquage des données en cas de contestation
- les utilisateurs n'aient accès qu'aux données dont on peut raisonnablement penser qu'elles sont nécessaires à l'accomplissement de leur mission.
- soient prévues des garanties pour que l'accès aux données à caractère personnel soit réservé aux seules personnes autorisées à en recevoir communication, et que les personnes ayant accès aux données enregistrées dans le système central soient informées qu'elles ne peuvent les utiliser à des fins non compatibles avec les finalités du système Flexitime,
- soit ajouté au règlement sur le système EFFICIENT l'ensemble des mentions reprises aux articles 11 et 12 du règlement 45/2001 afin que l'information des personnes concernées soit complète et exhaustive,
- la Cour établisse des mesures de sécurité [...]

Fait à Bruxelles, le 5 décembre 2008

(signé)

Joaquín BAYO DELGADO
Contrôleur européen adjoint à la protection des données