Avis sur la notification d'un contrôle préalable reçue du délégué à la protection des données (DPD) de la Cour de justice des Communautés européennes à propos du dossier "horaire flexible"

Bruxelles, le 6 mai 2009 (Dossier 2007-437)

1. Procédure

Le Contrôleur européen de la protection des données (CEPD) a reçu, par courrier en date du 27 juin 2007, une notification dans le sens de l'article 27.3 du règlement (CE) n° 45/2001 envoyée par le Délégué à la protection des données (DPD) de la Cour de justice des Communautés européennes, concernant le dossier "horaire flexible" (2007-437). Le 13 juillet 2007, des questions sont transmises au DPD. Par e-mail en date du 7 octobre 2008, le DPD a informé le CEPD du fait que la première notification allait être retirée au profit d'une nouvelle notification incorporant entre autres des réponses aux questions posées par le CEPD et annulant la première notification. Cette seconde notification a été reçue le 26 novembre 2008.

Des questions se rapportant à cette dernière notification ont été transmises au DPD le 13 janvier 2009. Des réponses y ont été apportées le 9 février 2009. Le 11 février 2009, le CEPD a décidé de prolonger d'un mois le délai du contrôle préalable en raison de la complexité du statut du traitement de données. De nouvelles questions ont été adressées au responsable du traitement le 16 mars 2009. Le responsable du traitement y a répondu le 26 mars 2009.

2. Examen de l'affaire

2.1. Les faits

Dans le cadre de la gestion du temps de travail de son personnel, la Cour de justice envisage d'établir un régime d'horaire flexible.

Le régime d'horaire flexible est défini par la Cour dans une décision relative aux horaires de travail, adoptée le 25 janvier 2006. Après une courte étape d'expérimentation limitée à un cercle restreint de personnes à la fin 2007 (décision du 24 juillet 2007), la phase pilote, qui est en cours à ce jour, a été mise en place en 2008 (décision du 20 juin 2008, modifiant la précédente par l'ajout du Comité du personnel en tant que population test). L'application générale du système devrait intervenir plus tard qu'initialement prévu. Il est estimé que cette dernière aura probablement lieu au printemps 2009. Un manuel "utilisateurs" a été rédigé par la Cour.

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

La base juridique du traitement réside dans l'article 55 du statut des fonctionnaires des Communautés européennes (statut), dans l'article 16 du Régime applicable aux autres agents (RAA) - ainsi que dans la décision susmentionnée.

Dans le cadre de l'horaire flexible, la journée de travail est divisée en plages fixes et mobiles. Pendant les plages fixes, le personnel doit obligatoirement être présent. Pendant les plages mobiles, le personnel est libre de choisir ses heures d'arrivée et de départ. Ces plages sont définies par le projet de décision.

Les fonctionnaires, agents temporaires et contractuels ainsi que les experts nationaux détachés peuvent demander à leur supérieur d'exercer leurs fonctions selon l'horaire flexible. La demande, qui n'est accordée que si elle est compatible avec le bon fonctionnement du service, est ensuite transmise au service du personnel. Le refus d'autorisation ou le retrait d'autorisation de l'horaire flexible fait l'objet d'une décision écrite motivée, communiquée à l'intéressé. Les personnes qui ne veulent ou ne peuvent exercer leur fonction selon l'horaire flexible s'en tiennent à l'horaire fixe ou l'horaire mobile défini par la Cour (article 3 de la décision susmentionnée du 25 janvier 2006).

Chaque chef de service s'assure du respect des horaires par le personnel qui travaille sous sa responsabilité. Les intéressés reçoivent un badge électronique sur lequel figure un numéro d'identification unique. Les intéressés enregistrent leur entrée dans le bâtiment où ils se rendent, ainsi que leur sortie et leur pause pour le déjeuner. À cette fin, des lecteurs de badges sont implantés aux entrées principales des bâtiments de la Cour ainsi que dans les cantines, cafétérias et dans la salle de sport du bâtiment Erasmus.

Les heures de présence sont comptabilisées à l'intérieur d'une plage d'acquisition allant de 7 heures à 22 heures, dans la limite d'un maximum de 10 heures par jour. Les heures effectuées en dehors de la plage d'acquisition ne sont pas comptabilisées, sauf si, pour des motifs exceptionnels, elles ont été prestées sur demande écrite préalable du chef de service de l'intéressé. Les heures prestées pendant les jours fériés et chômés, les jours de fermeture des bureaux ou le week-end, avec l'autorisation écrite préalable du chef de service, sont comptabilisées jusqu'à un maximum de 8 heures par jours ou de 16 heures par week-end.

Une pause déjeuner d'un minimum de 30 minutes est obligatoire pour toute personne qui effectue un horaire journalier d'une durée supérieure à 5 heures. Si le temps enregistré pour la pause déjeuner est inférieur à cette durée, un minimum de 30 minutes est décompté automatiquement du temps de travail.

Les missions sont comptabilisées en temps réel, à raison d'un maximum de 9 heures par jour, trajets inclus. Afin que ce temps soit crédité, les personnes concernées devront simultanément à l'envoi du décompte des frais de mission à leur supérieur hiérarchique, enregistrer une demande d'absence pour mission, via le système. Cette demande est soumise à validation par le supérieur hiérarchique.

Les trajets entre les bâtiments de la Cour sont comptabilisés comme temps de travail à raison d'un maximum de 20 minutes. Les trajets pour des raisons de service vers d'autres bâtiments que ceux de la Cour sont également comptabilisés comme temps de travail et doivent être déclarés par la personne concernée à son supérieur.

Les absences pour consultations médicales sont à justifier par la production d'un certificat médical (les absences ne pouvant pas dépasser sur une période trimestrielle, une moyenne de 4 heures par mois ou 12 heures par trimestre) et sont adressées directement au service médical.

Le nombre totale d'heures de travail à prester, qui constitue la référence pour le calcul du crédit ou du débit d'heures effectivement prestées, est de 38 heures 30 par semaine en temps normal et de 36 heures par semaine pendant les vacances judiciaires et les semaines blanches. La comptabilisation des heures effectivement prestées se fait à la fin de chaque mois. Le crédit d'heures maximal cumulé à la fin du mois est plafonné à 40 heures.

La récupération se fait par demi-journée, dans la limite de 2 jours par mois. Le chef de service est informé par écrit au préalable des demi-journées choisies pour la récupération. Si la récupération a lieu pendant une plage obligatoire fixe, elle est subordonnée à l'accord préalable du chef de service. L'accord ne peut être refusé que pour des raisons de service dûment justifiées. Pendant les vacances judiciaires, la récupération du crédit d'heures est possible en totalité, c'est-à-dire jusqu'à hauteur du plafond de 40 heures, sous réserve de l'accord préalable du chef de service. Les demandes de récupération sont introduites par la personne concernée via le système, par demi-journée. Les demandes sont validées par le supérieur hiérarchique.

Le cumul des heures en débit est plafonné à 16 heures. À la fin de chaque mois, tout dépassement constaté de ce plafond est immédiatement imputé sur le congé annuel. Tout débit d'heures restant à la fin de l'année civile est imputé sur le congé annuel.

Pour les fonctionnaires et agents travaillants à temps partiel, le nombre total d'heures à prester est déterminé en appliquant au nombre normal d'heures à prester le pourcentage de temps partiel pratiqué. Il en va de même pour le plafond du cumul des heures en crédit ou en débit.

Le traitement est partiellement manuel; les formulaires de demandes sont appelés à figurer sur support papier dans un fichier (un classeur) et partiellement automatisé; les décomptes horaires sont effectués par des moyens électroniques (le serveur central de la Cour de justice).

Les demandes d'absences (réunions, missions, etc) et de récupération au supérieur hiérarchique se font via la même base de données, "Efficient".

Les données traitées sont d'une part celles liées aux heures de présence : groupe horaire, cycle horaire, date de début, heure, temps prestation, durée du déjeuner, celles liées aux absences y compris l'indication du motif de l'absence, notamment l'indication selon laquelle l'absence est couverte par un congé de maladie (données extraites de la base de données "sic congé") ou s'il s'agit d'un congé annuel spécial, ou s'il s'agit d'une mission, d'une formation etc., et d'autres part les données d'identification : nom, prénom, numéro de matricule, numéro de badge, service, adresse de courrier électronique, nom d'utilisateur web.

Les données sont conservées pendant une durée de deux ans à partir de leur enregistrement. Cette durée de conservation est également valable pour les données récoltées durant la phase de test.

Il s'agit d'un traitement partiellement automatisé car les formulaires de demandes se sont sur papier. Ils sont appelés à figurer dans un fichier (un classeur). Les décomptes horaires sont effectués par des moyens automatiques (un logiciel spécialisé sur le serveur central).

Les fonctionnaires responsables de la gestion de l'horaire flexible (le chef d'unité, un administrateur habilité et le gestionnaire de l'application) peuvent introduire des données, les rectifier et les modifier. Les deux chefs ou supérieurs hiérarchiques directs de la personne concernée peuvent visualiser ses comptes individuels d'heures pour vérifier sa disponibilité et apporter les modifications nécessaires sur la carte des badgeages. Un fonctionnaire de la

division de l'informatique et des nouvelles technologies peut avoir accès au système en cas de problème informatique. Dans des cas particuliers, les données peuvent être communiquées à d'autres destinataires comme la Cour de justice, le Tribunal de première instance et/ou le Tribunal de la fonction publique, la Cour des comptes, le Parlement européen, le Médiateur européen et le CEPD.

La personne concernée a la possibilité de consulter ses données via une application informatique. Le système informatique d'horaire flexible permet la rectification de données inexactes ou incomplètes via l'introduction d'une demande au gestionnaire du système. Les données peuvent être verrouillées ou effacées par l'administration endéans les 15 jours.

Durant la phase pilote, les personnes peuvent demander des rectifications dans la base Efficient sans limite de délai. Pour le futur, la réglementation précise ce point comme suit :

Toute omission ou erreur de badgeage doit être notifiée par courrier électronique au supérieur hiérarchique dès qu'elle est constatée, et au plus tard dans un délai d'une semaine. Il en est de même pour toute autre demande de rectification sur la carte de badgeages. Le supérieur hiérarchique apporte les modifications et annotations nécessaires dans les meilleurs délais. Il peut aussi donner son accord par mail au gestionnaire de l'application pour qu'il apporte les modifications et annotations nécessaires en son nom.

Les données figurant sur les cartes de badgeages d'un mois donné ne peuvent plus être modifiées à partir du 20 du mois suivant. Au-delà de cette date, seules les absences pour raisons de service pourront exceptionnellement donner lieu à rectification par le gestionnaire de l'application informatique, avec l'accord du supérieur hiérarchique."

La Cour de justice prévoit d'informer les personnes concernées via le formulaire de demande et à l'aide d'un document expliquant le système d'horaire flexible (Manuel utilisateurs) et via un document d'information spécifique au traitement et répondant aux articles 11 et 12 du règlement (CE) n°45/2001. Ces deux documents sont annexés à la notification.

Des mesures de sécurité ont été adoptées. Chaque fonctionnaire habilité a accès aux applications informatiques au moyen d'un identifiant et d'un mot de passe spécifiques au traitement. Il a été précisé par la Cour que l'intégrité des données était garantie par un dispositif de sauvegarde.

Les caractéristiques du badge sont les suivantes : il s'agit d'un badge RFID de 125 KHz dont le numéro est stocké dans une puce électronique coulée dans le badge. Le numéro est stocké sous forme hexadécimal simple. Il ne peut être lu à distance, mais doit être mis en contact avec le lecteur de badge par l'utilisateur. Chaque trame remontée vers l'application est composée :
- d'une identification du type de trame
- d'un numéro de lecteur (le numéro de lecteur est lié à une adresse IP unique pour chaque terminal)
- d'un numéro de badge
- de la date du mouvement
- de l'heure du mouvement
- d'un checksum de contrôle de cohérence de la trame.

Le badge horaire flexible est séparé de la carte de service gérant les accès. De ce fait, il n'est pas pris en compte par les autres systèmes de la Cour, par exemple, les bornes et portes d'accès des garages etc. Efficient n'est pas lié aux autres systèmes de façon à garantir que les données concernant les personnes ne sont pas transmises.

Le logiciel (Efficient) dispose sur la version actuellement en production à la Cour, d'un rapport permettant de visualiser les lieux de pointages avec l'indication de la touche utilisée éventuelle (cas du trajet d'un bâtiment à l'autre). Seuls les responsables IT de la gestion de l'application de l'horaire flexible ont accès à ce rapport. Ils sont en mesure de produire ce rapport à la demande pour vérifier l'exactitude des données enregistrées. La durée de conservation est la même que pour les autres données de la base.

Dès que les informations sont transmises de la badgeuse à la base de données, elles sont automatiquement radiées de la mémoire de la badgeuse. Les données sont formatées quand elles arrivent dans Efficient et seul le logfile des transactions est conservé.

3. Les aspects légaux

3.1. Contrôle préalable

Le traitement des données concernant la gestion des horaires flexibles constitue un traitement de données à caractère personnel au sens des articles 2.a et 2.b du règlement (CE) n°45/2001. En effet, les données d'identification (nom, numéro personnel) des participants à l'horaire flexible sont collectées, enregistrées, conservées et consultées. Même le numéro de série devient un numéro personnel dès lors qu'il est relié ou qu'il peut être relié à des données relatives à l'identification et qu'il est utilisé pour enregistrer le fait qu'un badge délivré à un agent donné a été présenté au lecteur. La personne physique peut être identifiée, directement ou indirectement, par référence à un numéro d'identification.

Le traitement de données présenté est effectué par la Cour de justice et est mis en œuvre pour l'exercice d'activités relevant du champ d'application du droit communautaire. Les données sont traitées par la Cour 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) n°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.

L'article 27.2 contient une liste de traitements susceptibles de présenter semblables risques. L'article 27.2.a présente comme traitements susceptibles de présenter de tels risques "les traitements de données relatives à la santé ...", et l'article 27.2.b vise " traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur compétence, leur rendement ou leur comportement".

Le CEPD n'effectue pas de contrôle préalable parce que des données relatives à la santé peuvent occasionnellement apparaître, mais parce que dans le cas d'espèce, l'horaire flexible est destiné structurellement à collecter des données relatives à la santé. Dans le cas de la Cour en en effet, la solution choisie d'horaire flexible incorpore structurellement des données relatives à la santé (visite médicale pendant les heures de travail, congé de maladie). Ceci n'est pas fait de façon occasionnel, il en sera toujours ainsi.

Le CEPD a bien noté la remarque concernant l'application de l'article 27.2.b dans la notification. Le traitement n'a pas pour finalité d'évaluer le rendement ou le comportement du fonctionnaire ou agent. Les décisions adoptées par la Cour et l'information prévue pour la personne concernée sont clairs à cet égard; la finalité annoncée est **la gestion du temps de**

travail de manière à offrir au personnel une souplesse accrue dans l'organisation de son travail. Or l'article 27.2.b. est sans équivoque sur la notion de "finalité" puisque le traitement doit être "destiné" à évaluer. Le traitement ne présente donc pas de risques particuliers tels que ceux prévus à l'article 27.2.b. Le CEPD voudrait souligner que dans le cadre d'une évaluation par essence toujours subjective, un grand nombre de données vont être prises en compte, inconsciemment parfois, par l'évaluateur. C'est le cas de la donnée concernant une personne arrivant systématiquement en retard, que cela soit avec un système d'horaire flexible ou sans. Il est bien entendu que si à l'avenir, le système d'horaire flexible devait devenir un outil d'évaluation, il devrait respecter le contrôle préalable sur la procédure d'évaluation déjà effectué par le CEPD (2004-281).

Le traitement est actuellement en phase de test. Une expérience pilote est en cours au sein de la direction de la traduction de la Cour ainsi que dans certains services administratifs. Le CEPD souligne que la procédure à suivre en cas de projet pilote (ou de phase de pré-initialisation ou de pré-production) est de soumettre, en amont de la mise en place du projet pilote, une notification distincte concernant cette phase puisque il s'agit d'un traitement en soi qui doit être soumis pour contrôle préalable pour les mêmes raisons que le traitement définitif. Les données vont être différentes (population test ciblée par exemple) et les conditions techniques peuvent changer du test à la version finale suite aux conclusions tirées de la phase de test. De plus, mettre en place la protection des données "by design" c'est à dire dès la conception du projet, représente un double gain pour l'institution d'un point de vue pratique mais aussi financier. C'est particulièrement vrai pour les spécifications techniques du système. Pour ces raisons, le CEPD regrette que la protection des données ait été tenue à l'écart de la phase de conception du projet pilote et que le statut de ce dernier et de la phase finale soient restés confus.

Le cas sous analyse demeure un vrai contrôle préalable en ce sens que la mise en place finale de l'horaire flexible n'a pas encore eu lieu et qu'elle devra tenir compte des recommandations du CEPD.

La seconde notification du DPD a été reçue le 26 novembre 2008. Conformément à l'article 27.4, le présent avis doit être rendu dans les deux mois qui suivent. Le Contrôleur aurait dû donc rendre son avis le 27 janvier 2009. Une demande d'information complémentaire a suspendu pendant 27 jours le délai dans lequel le CEPD doit rendre son avis. L'avis doit donc être rendu au plus tard pour le xxx (27 janvier + 37 jours de suspension + un mois d'extension + commentaires).

3.2. Licéité du traitement

La licéité du traitement doit être examinée à la lumière de l'article 5.a du règlement (CE) n°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*".

Afin d'établir si le traitement est conforme à l'article 5.a. du règlement (CE) n° 45/2001, trois éléments doivent être pris en considération: premièrement, si le traité ou d'autres actes législatifs prévoient le type de traitement de données effectué; deuxièmement, si le traitement est mis en œuvre dans l'intérêt public et, troisièmement, si le traitement est nécessaire. Bien évidemment, ces trois exigences sont étroitement liées.

Bases juridiques pertinentes dans le traité ou dans d'autres actes législatifs

La base juridique pour le traitement est constituée par :

- le statut des fonctionnaires des Communautés européennes et le régime applicable aux autres agents (en particulier l'article 55 et l'article 16 du RAA),
- la décision relative aux horaires de travail, adoptée le 25 janvier 2006,
- la décision du greffier de la Cour de justice instituant une expérience pilote en matière de modalités d'application du régime flexible du 24 juillet 2007 ainsi que sa modification le 20 juin 2008,

Le traitement est effectué dans l'exercice légitime de l'autorité publique

Le CEPD note que la Cour met en œuvre le traitement dans l'exercice légitime de son autorité publique. En effet, le traitement s'inscrit dans le cadre d'une mission menée dans l'intérêt public sur la base du statut des fonctionnaires des Communautés européennes et du régime applicable aux autres agents des Communautés européennes. Le critère d'admissibilité du traitement est donc respecté.

Test de nécessité

Selon l'article 5.a. du règlement (CE) n° 45/2001, le traitement doit être "*nécessaire à l'exécution d'une mission*", comme indiqué ci-dessus. À cet égard, le considérant 27 précise que: "*le traitement de données à caractère personnel effectué pour l'exécution de missions d'intérêt public par les institutions et les organes communautaires comprend le traitement de données à caractère personnel nécessaires pour la gestion et le fonctionnement de ces institutions et organes*".

Le CEPD estime qu'il n'y a pas de nécessité spécifique de mettre au point un système de pointage utilisant un badge muni d'un RFID pour mettre en œuvre un système d'horaire flexible, puisque le même but (la gestion de l'horaire de travail) pourrait être atteint par des moyens différents et moins intrusifs.

Toutefois, le CEPD admet également que la "nécessité" ne signifie pas que le procédé soit inévitable, mais qu'il peut être considéré comme raisonnablement nécessaire dans le cadre spécifique de la réalisation de l'objectif visé. Dès lors, une certaine marge d'appréciation est laissée à la discrétion de l'administration pour décider de la mise en œuvre de ce système au moyen de la technologie RFID. Si les garanties recommandées et la proportionnalité sont avérées, on peut conclure que ce système remplit les conditions de "nécessité". Enfin, la participation au système d'horaire flexible en soi est fondée sur une participation volontaire.

Par ailleurs, les données relatives à la santé sont qualifiées dans l'article 10 du règlement de "catégories particulières de données" et nécessite une protection particulière, comme analysée ci-dessous.

3.3. Traitement portant sur des catégories particulières de données

La base de données peut inclure, entre autres, des données relatives à la santé du fonctionnaire ou de l'agent.

L'article 10.1 indique que "*le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou*

philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé ou à la vie sexuelle sont interdits".

L'article 10.2.b s'applique en l'espèce : " *le paragraphe 1* (interdiction du traitement des données relatives à la santé ...) *ne s'applique pas lorsque le traitement est nécessaire afin de respecter les obligations et les droits spécifiques du responsable du traitement en matière du 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* ...". Il s'agit effectivement de la Cour en tant qu'employeur, qui respecte l'article 10.2.b en effectuant le traitement des données soumis.

Le personnel des différents services ayant accès aux données relatives la santé (congés de maladie, absence pour rendez-vous médical), doit être informé qu'il est soumis au respect de l'obligation de secret professionnel, afin de garantir le traitement des catégories particulières de données. Le CEPD souhaite qu'il soit rappelé à toutes les personnes pouvant avoir connaissance et/ou être en charge des dossiers entrant dans le cadre de l'horaire flexible de l'importance de l'obligation de secret professionnel et de la nécessité de s'y conformer.

3.4. 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). Pour rappel, les données traitées sont d'une part les données d'identification de la personne concernée et d'autre part les données liées aux heures de présence. L'article 4.1.c semble donc en partie respecté.

Toutefois, les données de localisation méritent une analyse particulière. La localisation est un des paramètres du calcul de l'horaire journalier. La donnée est reprise dans un rapport permettant de visualiser les lieux de pointages avec l'indication de la touche utilisée éventuelle (cas du trajet d'un bâtiment à l'autre). La manière dont sont traitées ces données, c'est à dire qu'elles sont inclues dans un rapport uniquement accessible au gestionnaire IT du système, est satisfaisante au regard du principe de qualité des données du règlement. Le maintien de ces données dans le rapport permet la possibilité de rectification en cas de problème ou contestation.

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 au point 3.2. de cet avis. Quant à la loyauté, elle est, en particulier, liée aux informations qui doivent être transmises à la personne concernée (voir ci-dessous point 3.9).

Les données à caractère personnel doivent également être "*exactes et, si nécessaire, mises à jour*". Le règlement prévoit également que "*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). Le système décrit contribue à assurer l'exactitude et la mise à jour des données, étant donné la possibilité, pour la personne concernée, de consulter ses données via une application informatique. Le système informatique horaire flexible offre également la possibilité d'introduire une demande de rectification auprès du gestionnaire du système afin qu'il rectifie les données si ces dernières sont inexactes ou incomplètes. Concernant ces deux droits voir le point 3.8 *infra*.

3.5. Conservation des données

L'article 4.1.e du règlement (CE) n°45/2001 pose le principe que 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*".

Pour mémoire, les données sont conservées 2 ans à partir de leur enregistrement. C'est à dire que les données de l'année en cours sont conservées les deux années entières suivantes. Le CEPD désire rappeler sa position concernant la durée de conservation des données administratives de l'horaire flexible. Celles-ci peuvent être conservées pour l'année en cours et doivent être supprimées après la clôture de la procédure de transfert des jours de congé annuel non pris à l'année suivante. Cette opération s'effectue généralement au plus tard à la fin du mois de mars de l'année suivante. Au vue de la finalité du traitement - la gestion du temps de travail - le CEPD estime que le délai de conservation plus long prévu par la Cour doit être justifié à la lumière de l'avis du CEPD. Cette durée de conservation des données est également valable pour les données collectées lors de la phase de test.

Les données de localisation et les logsfiles des transactions (entre les badgeuses et Efficient) ne doivent être conservées que le temps de contestation possible et de modification effective des données, c'est à dire au plus tard le 20 du mois qui suit le mois duquel les données sont contestées. Le CEPD recommande à la Cour de revoir la durée de conservation de ces données à la lumière de cette remarque.

3.6. Changement de finalité / Usage compatible

Des données sont extraites de ou introduites dans les bases de données du personnel (Centurio, "sic congé"). Le traitement des données a pour objet la gestion des règles relatives à l'horaire flexible via un système automatisé. Le traitement analysé n'implique pas un changement général de la finalité prévue pour les bases de données relatives au personnel. Ceci implique que l'article 6.1 du règlement (CE) n°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.

3.7. Transfert des données

Le traitement doit également être examiné à la lumière de l'article 7.1 du règlement. Le traitement au regard de l'article 7.1 concerne les transferts de données à caractère personnel entre institutions ou organes communautaires ou en leur sein "*si nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire*".

L'article 7.1 du règlement est respecté, car les communications de données, effectuées vers d'autres services de l'institution (responsable de la gestion de l'horaire flexible, fonctionnaire de la division de l'informatique et des nouvelles technologies) sont légitimes puisqu'ils sont nécessaires à l'exécution légitime des missions relevant de la compétence des destinataires. De même, les transferts effectués entre organes ou institutions communautaires le sont dans le cadre strict des compétences des destinataires. Les données traitées dans le cadre de l'horaire flexible sont strictement internes à la Cour et ne seront transférées que dans les circonstances précises prévues pour chaque destinataire (par exemple, en cas de plainte au Médiateur européen).

Lorsque les données sont transférées à la suite d'une demande du destinataire, tant le responsable du traitement que le destinataire assument la responsabilité de la légitimité du transfert (article 7.2).

Le CEPD rappelle que, tant les autres services de l'institution qu'entre institutions et organes, les destinataires ne doivent traiter les données qu'aux fins qui ont motivé leur transmission (article 7.3).

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

L'article 10.6 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 présent avis ne fixera pas les conditions générales de cette utilisation d'un numéro personnel, mais examinera les mesures particulières nécessaires à cet égard dans le cadre du système d'horaire flexible.

Le CEPD a déjà précisé le statut du numéro de la puce RFID dans le traitement actuel. Le numéro d'identification associé à la puce RFID est une des données à caractère personnel visées par le règlement (CE) n° 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.

Le numéro de badge sera nécessaire puisque le badge personnel sera utilisé pour pointer à l'entrée et à la sortie en utilisant les lecteurs de badges. Pour des raisons pratiques, le numéro de badge et le numéro personnel devraient coexister dans le système d'horaire flexible. 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 contribue dès lors à assurer l'exactitude des données.

3.9. Droit d'accès et de rectification, verrouillage et effacement

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. Ces deux droits sont garantis dans le traitement sous analyse. Les personnes peuvent demander des rectifications dans la base Efficient sans limite de délai pendant la phase de projet pilote et lors du projet final les personnes doivent notifier toute omission ou erreur de badgeage par courrier électronique au supérieur hiérarchique dès qu'elle est constatée, et au plus tard dans un délai d'une semaine. Il en est de même pour toute autre demande de rectification.

L'article 16 du règlement prévoit que la personne concernée a le droit d'obtenir du responsable du traitement l'effacement de données si leur traitement est illicite. L'article 15 prévoit la possibilité de verrouiller les données lorsque leur exactitude est contestée par la personne concernée. La Cour a prévu un délai de 15 jours après requête légitime de la personne concernée, pour exercer ces deux droits.

3.10. Information des personnes concernées

Le règlement (CE) n° 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. 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 dans la mesure où le candidat à l'horaire flexible fournit lui-même une partie des données collectées via sa demande. 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 sont importées des bases de données "Centurio" et "sic congé".

Pour mémoire, la Cour projette d'informer les personnes concernées via le formulaire de demande et à l'aide d'un document expliquant le système d'horaire flexible. Le CEPD a vérifié leur conformité avec les articles 11 et 12 du règlement et a conclu que toutes les informations dictées par les articles 11 et 12 du règlement étaient reprises dans la notice d'information prévue.

3.11. Sécurité

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

En l'espèce, La Cour utilise pour la gestion de son contrôle d'accès, un badge[1] muni d'un identifiant par radiofréquence (RFID 125Khz). Le CEPD se félicite du fait que la distance de lecture soit inférieure à 10 centimètres[2], le badge doit être mis en contact avec le lecteur. 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. Des technologies plus appropriées, comme l'utilisation de "contactless smartcard" ayant la possibilité de générer un identifiant aléatoire permettant l'établissement de la communication entre le badge et le lecteur avant que le numéro du badge ne soit livré à la badgeuse, pourraient être sélectionnées et utilisées à l'avenir[3]. De manière alternative, la Cour pourrait mettre en place un bouclier de protection (une cage de Faraday[4]) du badge qui serait ouvert uniquement lorsque le badge est utilisé. Lors d'une future mise à jour du système, il serait nécessaire d'envisager de telles mesures contre la contrefaçon des badges.

En ce qui concerne les mesures organisationnelles, des indications claires feront partie de la formation des utilisateurs et seront intégrées dans le manuel d'utilisation sur papier et en ligne pour la mise en place du projet final. Le CEPD regrette que ces mesures n'aient pas été mises en place au moment de l'introduction du projet pilote.

---

[1] Les badges contiennent des informations personnelles dans la mesure où l'identifiant est unique et rattaché à une personne.

[2] Voir Dossier Flexitime DG INFSO 2007-218.

[3] Ce point a été souligné l'année dernière par l'organisation internationale de l'aviation civile (ICAO) voir page 22:http://www2.icao.int/en/MRTD/Downloads/Supplements%20to%20Doc%209303/Supplement%20to%20ICAO%20Doc%209303%20-%20Release%207.pdf

[4] La *cage de Faraday* (c'est-à-dire une enceinte conductrice qui n'est pas reliée à la terre de façon à maintenir son potentiel fixe) est étanche aux champs électriques (créés par la simple présence d'une différence de potentiel, sans qu'un courant ne soit nécessaire) et ce, que la source perturbatrice soit à l'intérieur ou à l'extérieur de l'enceinte. La puce ne pourra pas être activée par le lecteur tant que la protection sera maintenue.

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 informe le CEPD de toutes conclusions tirées de la phase de test, ainsi que de toutes modifications prévues pour le régime d'horaire flexible définitif;
- Qu'il soit rappelé à toutes les personnes pouvant avoir connaissance et/ou être en charge des dossiers entrant dans le cadre de l'horaire flexible de l'importance de l'obligation de confidentialité et de la nécessité de s'y conformer;
- Que la Cour revoie sa politique de conservation des données personnelles tant au regard des commentaires relatifs aux données administratives qu'à ceux relatifs aux données techniques;
- Que la Cour prenne les mesures organisationnelles prévues.

Fait à Bruxelles, le 6 mai 2009

(Signé)

Giovanni BUTTARELLI
Le Contrôleur européen adjoint de la protection des données