Avis sur une notification en vue d'un contrôle préalable adressée par le délégué à la protection des données de la Fondation européenne pour la formation concernant l'ETF - procédure Flexitime

Bruxelles, le 26 février 2009 (dossier 2008-697)

1. Procédure

Le 18 novembre 2008, le Contrôleur européen de la protection des données (CEPD) a reçu du délégué à la protection des données (DPD) de la Fondation européenne pour la formation (ETF) une notification en vue d'un contrôle préalable concernant le traitement des données à caractère personnel dans les opérations de traitement de Flexitime (enregistrement des congés et horaires flexibles [flexitime]) des membres du personnel.

Le projet de «Guide de l'horaire flexible» de l'ETF était joint à la notification.

Le dossier a été suspendu lorsqu'une demande d'informations complémentaires a été présentée le 5 décembre 2008; ces informations ont été fournies le 17 décembre 2008. Le dossier a été suspendu une nouvelle fois dans l'attente des observations sur les faits de l'affaire le 7 janvier 2009, et ces observations ont été transmises le 12 janvier 2009. Le dossier a été suspendu une troisième fois dans l'attente d'observations sur le projet d'avis du DPD le 3 février 2009, lesquelles ont été reçues le 11 février 2009.

2. Les faits

Selon la notification, **l'objectif** des traitements est d'assurer un traitement égal et équitable dans une approche du travail flexible afin d'aider les membres du personnel à mieux concilier travail et vie privée. L'ETF estime que Flexitime peut être un outil très efficace en vue de permettre aux collaborateurs d'équilibrer leurs engagements professionnels et privés. Ce qui intéresse l'ETF dans l'utilisation de Flexitime, c'est le renforcement de la motivation de ses collaborateurs découlant de leur responsabilité accrue dans l'organisation de leur temps de travail. En outre, le principal objectif du dispositif réside dans la flexibilité quotidienne, et non pas dans la récupération. Il y a lieu d'organiser le travail de telle sorte qu'il puisse être accompli sur une journée ouvrable normale de 7½ heures; le temps prévu au-delà ne doit être ouvré que lorsque la charge de travail le justifie ou comme convenu avec le supérieur. L'accumulation de crédit temps doit donc être en rapport direct avec le travail à accomplir; il convient d'éviter de prolonger le temps de travail quotidien dans le simple but d'accumuler du crédit temps. Comme l'explique le Guide de l'horaire flexible de l'ETF, la période durant laquelle les travailleurs flexibles sont libres de choisir leurs heures d'arrivée, de pause déjeuner et de départ va respectivement de 7 h 30 à 9 h 30, de 12 heures à 14 heures et de 16 heures à 20 h 30.

Les **personnes concernées** sont tous les membres du personnel de l'ETF visés par le Statut des fonctionnaires et le Régime applicable aux autres agents (agents contractuels, agents locaux,

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

agents temporaires), indépendamment du groupe de fonctions ou du grade, et les experts nationaux détachés. Les dispositions actuelles s'appliquent par analogie aux personnes autorisées à travailler à temps partiel. Dans ce cas, l'horaire de travail standard et les heures fixes, le temps compté pour les absences et le temps maximum crédité ou débité seront réduits en proportion du temps de travail réduit.

Les **données collectées** sont: le numéro de carte (dispositif RFID de type Mifare) lié à un identifiant (ce qui signifie lié au nom de la personne dans un second temps), les événements quotidiens tels que l'arrivée et le départ, la durée de la pause déjeuner, les congés, les vacances, les missions de tous les membres du personnel concernés. Sur la base de ces données, le système calcule pour chaque personne un solde (positif ou négatif) par rapport au nombre escompté d'heures mensuelles. Les données permettant la localisation des lecteurs Flexitime ne sont collectées qu'à des fins de résolution de problèmes et ne sont accessibles qu'à l'administrateur du système informatique disposant de droits spécifiques en matière de contrôle d'accès. Le système ne traite que les données relatives à la personne, à l'heure et à la direction (entrée ou sortie).

D'après la notification, outre les personnes concernées, les **destinataires** des données sont l'unité des Ressources humaines (directeur des RH, gestionnaire des congés) et les supérieurs hiérarchiques respectifs. Du fait des fonctions techniques du système liées à l'accès aux données à caractère personnel, l'unité Gestion des infrastructures et des technologies (ITM) (développeurs de logiciels) est également susceptible d'accéder aux données. Elle n'est pas considérée comme le destinataire des données, mais doit être informée et avisée des questions de protection des données (notamment la confidentialité et la sécurité). Aucun transfert de données à destination de pays tiers ou d'organisations internationales ne sera effectué. Flexitime est exclusivement destiné à l'usage interne au profit des membres du personnel, afin de les aider à mieux concilier leur vie professionnelle et leur vie privée.

Procédure d'utilisation de Flexitime:
Aux fins de l'introduction de Flexitime, l'unité des RH invitera tous les collaborateurs désireux de bénéficier d'un horaire de travail flexible à en discuter avec leur supérieur hiérarchique, qui validera la demande après s'être assuré que la continuité du service n'est pas compromise et informera l'unité des RH de sa décision. Le projet de «Guide de l'horaire flexible» envoyé au CEPD fait expressément référence au caractère volontaire de la participation à l'utilisation de Flexitime.

Un badge personnel est délivré à l'activation de Flexitime. Les membres du personnel qui n'auront pas d'emblée manifesté leur intérêt mais qui souhaiteraient à un moment donné bénéficier d'un horaire de travail flexible, feront part de leur décision à leur supérieur hiérarchique qui, comme indiqué ci-dessus, communiquera sa décision aux RH.

Un badge commun est utilisé à la fois pour entrer dans le bâtiment et pour Flexitime, mais les lecteurs Flexitime et les lecteurs de contrôle d'accès sont des machines distinctes. En outre, l'accès au bâtiment et les systèmes Flexitime ne sont pas liés entre eux et, par conséquent, les collaborateurs qui utilisent Flexitime doivent présenter leur badge aux deux machines: la première à l'entrée du bâtiment et la seconde pour Flexitime. Les membres du personnel qui n'utilisent pas Flexitime ne doivent présenter leur badge que pour entrer.

Les **informations** fournies aux personnes concernées sont décrites comme suit:
Des informations complètes sur la déclaration de confidentialité et le traitement des données seront intégrées à la politique concernée et placées sur l'intranet de l'ETF, accessible à tout moment à tout le personnel de l'ETF.

Les informations suivantes seront notamment transmises électroniquement à chaque "travailleur flexible":

- l'identité du responsable du traitement,
- l'objectif du traitement auquel les données sont destinées et la base juridique,

- les destinataires des données à caractère personnel,
- la provenance des données,
- le droit de la personne concernée à accéder aux données qui la concerne et à les rectifier,
- la période de rétention des données à l'ETF,
- le droit de former recours devant le CEPD à tout moment.

S'agissant des **droits des personnes concernées**, selon la notification, Flexitime est administré au moyen d'une base de données Lotus Notes et accessible sur l'intranet de l'ETF. Toute personne concernée peut accéder à cette base de données au moyen de son identifiant et de son mot de passe. C'est pourquoi les personnes concernées (les utilisateurs de l'application) peuvent vérifier et, si nécessaire, solliciter la correction/suppression des données par une demande électronique. Les demandes de correction introduites après plus de 5 jours de présence dans le bureau ne seront pas acceptées, sauf cas de force majeure. En outre, les personnes concernées peuvent exercer à tout moment leurs droits au titre du règlement (CE) n° 45/2001 sur demande adressée au responsable du traitement.

Traitement automatisé et manuel:
Les services de l'ETF chargés de l'application Flexitime ne collecteront de données à caractère personnel que dans la mesure nécessaire pour aider tous les membres du personnel à effectuer le même nombre d'heures dues de manière flexible afin de mieux concilier travail et vie privée. Flexitime est fondé sur le principe de l'enregistrement des heures ouvrées étayé par un système de vérification transparent, qui devrait être d'un emploi aisé et rapide.

Les opérations de traitement automatisé sont les suivantes:

- l'enregistrement (date et heure) des pointages pour chaque personne (identifiant unique et pointage);

- transfert des pointages vers le reste de l'application, où le lien est fait entre l'identifiant unique de la puce et une personne grâce au numéro personnel de la personne concernée. Les pointages d'une personne seront regroupés sur une journée et le lendemain matin, ils apparaîtront sur le Flexitime intranet personnel de chaque personne concernée. Si des données sont illisibles pour le système (lecture incorrecte du badge ou autre), une croix rouge apparaît pour le jour où un «problème» s'est produit et aucun temps de travail ne sera pris en compte. Cela permet l'envoi d'une notification rapide et claire à tout membre du personnel en vue de demander la correction;

- concernant le calcul du temps de travail et des crédits/débits temps correspondants, le système Flexitime est relié à d'autres applications telles que SIC Leave et SIC Mission[1]. Cette interconnexion permet au système de compter automatiquement le temps de travail et tout pointage en absence, au moyen de ces deux bases de données. Par conséquent, les données contenues dans le système Flexitime comprennent non seulement le nombre d'heures de travail effectuées par chaque collaborateur en un mois, mais aussi une référence aux jours de fermeture de l'ETF, aux week-ends et aux régimes de temps partiel. En fonction des informations complémentaires fournies, aucun traitement des données médicales n'est effectué lorsque des demandes validées sont envoyées de SIC

[1] Les demandes SIC Leave et SIC Mission validées sont transférées automatiquement dans le système *Flexitime*. Les opérations de traitement automatisé sont les suivantes:
- calcul du temps de travail sur la base des heures d'arrivée et de sortie enregistrées;
- calcul du temps de travail lorsque les collaborateurs ont une période d'absence validée par leur responsable via SIC (congé ou mission);
- nombre escompté d'heures devant être travaillées sur un mois compte tenu des jours de fermeture de l'ETF, des week-ends, etc.;
- crédits/débits temps.

Leave et SIC Mission vers Flexitime. En outre, le même symbole est utilisé dans la base de données Lotus pour indiquer les maladies, les congés spéciaux et les congés annuels;

- l'élaboration de rapports en fonction de l'intérêt du service et à des fins statistiques (et dès lors, des données agrégées anonymes sont utilisées);

- les demandes de correction du temps de travail doivent être transmises par voie électronique et validées par le supérieur hiérarchique respectif et, une fois validées, les données corrigées seront importées automatiquement dans le système Flexitime, où elles effaceront et remplaceront les données incorrectes.

Les opérations de traitement manuel portent sur l'affectation aux travailleurs à temps partiel de leurs conditions à temps partiel respectives approuvées (50 %, 60 %, 70 %, 75 %, 80 %, 90 %). D'un point de vue technique, ce traitement implique que, pour chaque collaborateur à temps partiel, le pourcentage approuvé de leur régime de travail soit introduit manuellement afin d'obtenir le temps de travail escompté sur une période donnée et le solde proportionnel crédit/débit maximal qu'un travailleur à temps partiel peut générer. C'est pourquoi le traitement manuel partiel ne peut être appliqué que dans le cas spécifique des travailleurs à temps partiel.

En ce qui concerne **le verrouillage et l'effacement** des données, la notification prévoit une procédure de sortie avec possibilité d'effacer les données. En cas de demande de sortie de Flexitime, les membres du personnel sont invités à le faire à la fin d'un mois civil.

Le membre du personnel est donc invité à continuer d'enregistrer ses heures de travail quotidienne jusqu'à la fin d'un mois civil. Il n'est possible de quitter Flexitime que si le solde temps est au minimum nul, ou positif.

Bien que cette procédure de sortie ne soit pas comparable à une procédure de verrouillage ou d'effacement, lorsqu'une personne a quitté le système (solde à zéro), les données peuvent être intégralement effacées dans les deux semaines à compter de la demande. Seules les données anonymes seront conservées plus longuement à des fins statistiques.

Par conséquent, pour les données **statistiques** et **historiques**, seules les données anonymes seront conservées et, partant, aucun lien entre le nom et les données ne sera possible. Seules des données agrégées seront conservées.

S'agissant du **stockage**, les données sont conservées dans une base de données Lotus Notes. Elles sont transférées du dispositif RFID (où la personne est inconnue et seul un numéro de code est connu) vers Lotus Notes, où elles sont associées à chaque personne concernée.

Il y a 3 machines de pointage à l'entrée et à la sortie (aux 3 principales entrées du bâtiment de l'ETF). Il est impossible au badge d'être lu accidentellement, car les personnes doivent passer volontairement la carte sur les pointeuses.

La période de **rétention** est la suivante: les données Flexitime individuelles seront conservées pendant l'année civile en cours. Elles seront supprimées lorsque le transfert des jours de congé annuels inutilisés à l'année suivante est bouclé, et au maximum à la fin du mois de mars de l'année suivante. En outre, l'ETF prévoit que la période de rétention pour les deux types de données, administratives et techniques (historique) du système Flexitime sera identique (au maximum jusqu'à 15 mois). Dans les informations fournies, l'ETF s'assure que toutes les mesures techniques nécessaires sont mises en œuvre afin de garantir le respect de ce critère de sécurité.

Comme expliqué plus haut, les données agrégées rendues anonymes ne seront conservées plus longtemps qu'aux fins des statistiques sur les tendances passées.

Les **mesures de sécurité** du système
(...)

3. Analyse juridique

3.1. Contrôle préalable

Le règlement (CE) n° 45/2001 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (ci-après le «règlement (CE) n° 45/2001») s'applique au traitement des données à caractère personnel par les institutions et organes communautaires.

Les données à caractère personnel sont définies comme suit: toute information concernant une personne physique identifiée ou identifiable. Est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

L'application Flexitime de l'ETF traite des données à caractère personnel parce que lesdites données concernent des personnes physiques identifiables, par exemple grâce à des noms ou des numéros personnels. Même le numéro de série du badge, qui en soi n'est pas une donnée à caractère personnel, devient dans le système un numéro personnel dès lors qu'il est lié ou peut être lié aux données d'identification et qu'il est utilisé pour enregistrer le passage dans le lecteur d'un badge délivré à un membre du personnel donné. La personne physique peut être identifiée directement ou indirectement par référence à un numéro d'identification. Les données traitées en rapport aux congés et au Flexitime des collaborateurs de l'ETF constituent donc des données à caractère personnel au sens de l'article 2, point a), du règlement (CE) n° 45/2001.

Le traitement effectué par l'ETF est mis en œuvre pour l'exercice d'activités qui relèvent du champ d'application du droit communautaire (article 3, paragraphe 1, du règlement (CE) n° 45/2001).

L'article 27, paragraphe 1, du règlement (CE) n° 45/2001 soumet au contrôle préalable du CEPD tous «*[l]es 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*». Le système Flexitime de l'ETF utilise un système de badges fondé sur la technologie RFID. Le CEPD estime que l'utilisation de cette technologie (la puce RFID insérée dans le badge) dans le cadre d'un système Flexitime constitue une innovation importante dans un tel système et présente un risque spécifique.[2] C'est pourquoi le contrôle préalable actuel relève de l'article 27, paragraphe 1, du règlement.

Le système Flexitime de l'ETF comporte un traitement à la fois automatique et manuel. Il s'agit d'un traitement partiellement automatisé. C'est pourquoi l'article 3, paragraphe 2, du règlement s'applique.

Dès lors que le contrôle préalable vise à dépister les situations susceptibles de présenter certains risques, il y a lieu d'obtenir l'avis du CEPD avant le début du traitement. Le présent avis constitue un **véritable contrôle préalable**. Aussi le traitement ne devrait-il pas être entamé avant

[2] Voir Avis sur une notification en vue d'un contrôle préalable reçue du délégué à la protection des données de la Commission européenne à propos de la «mise en œuvre du Flexitime spécifique à la DG INFSO», délivré le 19 octobre 2007 (dossier 2007-218).

que les recommandations dudit avis soient prises en considération et que le CEPD soit informé des mesures de mise en œuvre.

La notification a été reçue le 18 novembre 2008. Conformément à l'article 27, paragraphe 4, du règlement (CE) n° 45/2001, le délai de deux mois dont le CEPD dispose pour émettre son avis a été suspendu pendant un total de 17 jours afin d'obtenir des informations complémentaires. Il a également été suspendu pendant 7 jours pour permettre les commentaires sur le projet d'avis. Eu égard aux nouveaux éléments transmis par la DPD dans ses observations, le CEPD a décidé de prolonger de deux semaines le délai dont il dispose pour adopter son avis, lequel doit donc être délivré au pour tard le 27 février 2009.

3.2. Licéité du traitement

Les données à caractère personnel ne peuvent être traitées que si un motif légal peut être trouvé à l'article 5 du règlement (CE) n° 45/2001.

Parmi les différents motifs énumérés à l'article 5 du règlement (CE) n° 45/2001, le traitement notifié en vue d'un contrôle préalable relève de l'article 5, point a), selon lequel le traitement de données à caractère personnel peut être effectué s'il «*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 de déterminer si les traitements sont conformes à l'article 5, point a), du règlement (CE) n° 45/2001, selon l'article 5, point a) il convient tout d'abord de déterminer si le traitement a une base juridique spécifique: une disposition du Traité ou tout autre acte législatif adopté sur la base des traités. Il faut ensuite déterminer si le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public. Pour satisfaire à ce second point, il y a lieu en l'occurrence de tenir compte du considérant 27 du règlement, qui précise que «*[l]e 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*». Dans le présent dossier, la seconde question est donc de savoir si le traitement est nécessaire et proportionnel à la gestion et au fonctionnement de l'ETF.

Bases juridiques pertinentes dans le Traité ou autres instruments juridiques
La base juridique du traitement peut être trouvée dans:

- le Statut des fonctionnaires des Communautés européennes et le Régime applicable aux autres agents des Communautés européennes (notamment l'article 55);
- le Guide de l'horaire flexible de l'ETF qui sera adopté à la suite de l'avis du CEPD.

Nécessaire à l'exécution d'une tâche effectuée dans l'intérêt public
Dans l'examen consistant à déterminer si le traitement remplit la seconde condition visée à l'article 5, point a), la question n'est pas de savoir s'il existe un *besoin spécifique* de développer «un système de badges recourant à la RFID» pour mettre en œuvre un système Flexitime, mais si le traitement dans un tel système est nécessaire à l'exécution d'une tâche effectuée dans l'intérêt public.

En outre, ainsi qu'il a déjà été souligné lors de précédents contrôles préalables[3], le «besoin» requis ne signifie pas qu'il doive être *inévitable*, mais qu'il puisse être considéré comme raisonnablement nécessaire, dans le contexte spécifique, à la réalisation de l'objectif visé. Une certaine marge d'appréciation est donc laissée à la discrétion de l'administration en vue de décider s'il y a lieu de mettre en œuvre ce système fondé sur la technologie RFID.

Si les sauvegardes et la proportionnalité nécessaires sont présentes, on peut estimer qu'un tel système remplit les conditions de besoin.

Le CEPD observe que l'ETF met en œuvre les activités de traitement en vue d'une tâche effectuée dans l'intérêt public. En effet, les traitements s'inscrivent dans le cadre d'une mission effectuée dans l'intérêt public sur la base du Statut des fonctionnaires des Communautés européennes et du Régime applicable aux autres agents des Communautés européennes.

Enfin, comme décrit sous *Les faits*, la participation au système Flexitime lui-même se fait sur une base volontaire.

Le CEPD estime que le traitement en tant que tel répond aux conditions de licéité. Le présent avis se concentre en outre sur les sauvegardes afin de résoudre les risques spécifiques présentés par ce 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, paragraphe 1, point c), du règlement (CE) n° 45/2001).

Les données collectées sont les suivantes: un numéro de carte (numéro d'identification de série) et des événements quotidiens tels que l'arrivée et le départ. Il y a 3 pointeuses d'entrée et de sortie aux 3 principales entrées du bâtiment de l'ETF.

Les données précises collectées sont les suivantes: le numéro de carte lié à un identifiant, les événements quotidiens tels que l'arrivée et le départ, la durée de la pause déjeuner, les congés, les vacances, les missions de tous les membres du personnel concernés. Sur la base de ces données, le système calcule pour chaque personne un solde (positif ou négatif) par rapport au nombre escompté d'heures mensuelles. Il y a alors un transfert des pointages vers le reste de l'application, où le lien est fait entre l'identifiant unique de la puce RFID et une personne.

En outre, les données sont sauvegardées dans une base de données Lotus Notes. Le numéro de carte est transféré de la puce à Lotus Notes, où il est ensuite associé à chaque personne. En matière de qualité des données, le CEPD considère que les données à caractère personnel des membres du personnel de l'ETF qui ne souhaitent pas utiliser le Flexitime ne doivent pas être importées dans la base de données Lotus Notes.

À part cela, le CEPD estime que les données sont adéquates et pertinentes. Ces données ne sont pas considérées comme excessives.

En outre, la notification affirme qu'aucune donnée relevant des catégories particulières de données visées à l'article 10, paragraphe 1 (catégories particulières de données) n'est traitée dans le cadre des traitements de données notifiés en vue d'un contrôle préalable. Eu égard à l'objectif

[3] Voir par exemple le document 2007-218 cité ci-dessus à la note 2.

global poursuivi par l'ETF lorsqu'il met en œuvre les traitements de données Flexitime, le CEPD estime que l'intention de l'ETF n'est pas de collecter des catégories particulières de données.

Les données doivent être traitées «*loyalement et licitement*» (article 4, paragraphe 1, point a), du règlement). Le caractère licite du traitement a déjà été examiné (voir point 3.2 ci-dessus). Quant au caractère loyal, il concerne les informations transmises aux personnes concernées (voir point 3.9 ci-dessous).

Les données doivent être «*exactes et, si nécessaire, mises à jour*» (article 4, paragraphe 1, point d). Le système en général doit garantir l'exactitude et la mise à jour des données. Dans le traitement analysé ici, chaque personne concernée peut accéder à la base de données Lotus grâce à son identifiant et son mot de passe. De la sorte, les personnes concernées (les utilisateurs de l'application) peuvent vérifier et, si nécessaire, solliciter la correction/suppression des données au moyen d'une demande électronique. Les demandes de correction introduites après plus de 5 jours de présence dans le bureau ne seront pas acceptées, sauf cas de force majeure. En outre, les personnes concernées peuvent exercer à tout moment leurs droits au titre du règlement (CE) n° 45/2001 sur demande adressée au responsable du traitement.

Comme expliqué dans *Les faits*, en cas de données illisibles pour le système (lecture incorrecte du badge ou autre), une croix rouge apparaît pour le jour où un «problème» s'est produit et aucun temps de travail ne sera pris en compte. Cela permet l'envoi d'une notification rapide et claire à tout membre du personnel en vue de demander la correction. Le CEPD considère cependant que cette pratique n'est pas suffisante pour garantir la qualité des données. Il propose donc que, lorsqu'une erreur survient dans l'enregistrement des heures ou dans le transfert des données vers la base de données Lotus, un courrier électronique soit envoyé à la personne concernée avec tous ses enregistrements d'heures afin de l'informer qu'une erreur s'est produite.

La personne concernée a le droit d'accéder à ses données et de les rectifier, afin que le fichier puisse être aussi complet que possible. En outre, sur le droit d'accès et de rectification, voir le point 3.8 ci-dessous.

3.4. Conservation / rétention des données

L'article 4, paragraphe 1, point e), du règlement (CE) n° 45/2001 énonce le principe selon lequel «*[l]es 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. L'institution ou l'organe communautaire prévoit, pour les données à caractère personnel qui doivent être conservées au-delà de la période précitée à des fins statistiques* […]*, soit qu'elles ne seront conservées que sous une forme qui les rend anonymes, soit, si cela est impossible, qu'elles ne seront stockées qu'à condition que l'identité de la personne concernée soit cryptée.*»

D'après les informations fournies par l'ETF, la période de rétention sera la même pour les deux types de données, administratives et techniques (historique), du système Flexitime: au maximum jusqu'à 15 mois. Le CEPD accepte la proposition selon laquelle les données administratives du Flexitime sont sauvegardées pendant l'année civile en cours et supprimées lorsque le transfert des jours de congé annuels inutilisés à l'année suivante est bouclé, et au maximum à la fin du mois de mars de l'année suivante.

Cependant, le CEPD ne peut accepter une période de rétention similaire pour les données techniques dans l'application de l'ETF (données relatives à l'historique). En effet, l'application Flexitime sert de mémoire tampon pour les enregistrements d'heures avant leur envoi vers la base de données Lotus Notes. Il n'est dès lors pas nécessaire de conserver ces données pendant une longue période de temps. Dans le cas de l'ETF et eu égard à la nécessité de conserver un historique de l'application Flexitime, le CEPD conseille de respecter une durée de conservation des données d'un mois au maximum.

Le projet de Guide de l'horaire flexible prévoit que les personnes concernées qui quittent le système Flexitime ont le droit (à condition que le solde de leurs crédits/débits temps soit de zéro) de solliciter la suppression de leurs données personnelles. Lorsque la personne a quitté le système (avec un solde à zéro), les données peuvent être entièrement effacées dans les 2 semaines à compter de la demande. Le CEPD souhaite que cette période de 2 semaines soit expressément ajoutée à la déclaration de confidentialité du Flexitime de l'ETF.

De la même façon, l'ETF devrait prévoir une procédure afin de supprimer les données Flexitime (données administratives et historiques) des personnes qui ont quitté l'agence. Dans ce genre de cas, le CEPD a déjà estimé qu'une période de 2 semaines était proportionnelle à l'objectif du traitement.

S'agissant des données statistiques, les données agrégées rendues anonymes ne seront conservées pendant une période plus longue qu'aux fins de statistiques sur les tendances passées. Le CEPD estime que cette rétention est proportionnelle et conforme à l'article 4, paragraphe 1, point e).

3.5. Utilisation compatible / changement de finalité

L'article 4, paragraphe 1, point b), du règlement, dispose que les données à caractère personnel doivent être «*collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités*». La finalité du traitement est d'assurer, sur la base du principe d'enregistrement des heures de travail effectuées, l'objectif principal du système, à savoir la flexibilité journalière, et non la récupération. En effet, la finalité de Flexitime est de permettre aux membres du personnel de décider quand ils souhaitent commencer à travailler, prendre leur déjeuner et rentrer chez eux dans le cadre général d'une semaine de 37½ heures[4] tout en assurant les heures fixes et l'intérêt du service.

Le CEPD estime qu'il n'y a aucun changement de la finalité du traitement et qu'aucune finalité secondaire n'est visée. Aussi suggère-t-il d'ajouter au projet de Guide de l'horaire flexible de l'ETF que ce dernier n'utilise pas les données traitées dans le contexte analysé ici à d'autres fins que celles qu'il vise à remplir, et que le «numéro de carte» n'est pas utilisé à d'autres fins que dans le cadre de Flexitime et qu'il n'est sauvegardé dans l'application Flexitime de l'ETF qu'afin de faire le lien entre la carte et la personne concernée.

L'article 6, paragraphe 1, du règlement (CE) n° 45/2001 n'est pas applicable au cas d'espèce et l'article 4, paragraphe 1, point b), du règlement est respecté, à condition que les recommandations soient mises en œuvre.

3.6. Transfert de données

L'article 7 du règlement dispose que «*[l]es 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*».

La notification précise quelles catégories de personnes pourraient accéder aux données enregistrées par l'application d'enregistrement informatique de l'ETF. Ainsi qu'il a été expliqué dans *Les faits*, en raison des fonctions techniques du système liées à l'accès aux données à caractère personnel, l'unité Gestion des infrastructures et des technologies (ITM) (développeurs de logiciels) est également susceptible d'accéder aux données, même si elle n'est pas le destinataire escompté susceptible de traiter les données. Le CEPD ne la considère pas comme la destinataire des données. Toutefois, l'ETF doit veiller à ce qu'elle soit informée et avisée des questions de protection des données (notamment la confidentialité et la sécurité).

[4] Conformément à l'article 55 du Statut des fonctionnaires.

En outre, le CEPD ne considère pas les personnes concernées comme les destinataires des données. En effet, elles sont les personnes concernées par le traitement des données, mais non les destinataires desdites données.

Les catégories de destinataires sont donc le responsable du traitement des données (chef de l'unité des RH responsable de la gestion des congés/absences) et les supérieurs hiérarchiques respectifs. Les transferts à ces destinataires sont légitimes dès lors qu'ils sont nécessaires à l'exécution légitime des missions relevant de la compétence du destinataire.

Le CEPD comprend également qu'il n'y aura aucun transfert des données à l'extérieur de l'ETF. Les données collectées dans l'application Flexitime ne sont accessibles à personne en dehors de l'ETF.

Aucun transfert de données à destination de pays tiers ou d'organisations internationales ne sera effectué. Flexitime est exclusivement destiné à l'usage interne au profit des membres du personnel, afin de les aider à mieux concilier leur vie professionnelle et leur vie privée.

3.7. Traitement du numéro personnel ou de l'identifiant unique

L'article 10, paragraphe 6, du règlement prévoit que «*[l]e 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 vise pas à établir les conditions générales d'une telle utilisation d'un numéro personnel, mais à envisager les mesures spécifiques nécessaires dans le cadre de Flexitime.

Le numéro de badge et le numéro personnel coexistent dans le système Flexitime pour des raisons pratiques. Le numéro de badge est nécessaire parce que le badge personnel est utilisé pour enregistrer l'arrivée / le départ au moyen des lecteurs de badges. Dans le cas d'espèce, l'utilisation du numéro personnel des collaborateurs afin d'enregistrer des données dans le système est raisonnable étant donné que ce numéro est utilisé pour identifier la personne dans le système et contribue de la sorte à garantir l'exactitude des données. L'article 10, paragraphe 6 est donc respecté.

3.8. Droit d'accès et de rectification

L'article 13 du règlement (CE) n° 45/2001 instaure un droit d'accès – et en prévoit les modalités d'exercice –, à la demande des personnes concernées. L'article 14 prévoit un droit de rectification des données inexactes ou incomplètes.

La notification en vue d'un contrôle préalable et les informations complémentaires transmises par le responsable du traitement décrivent la possibilité offerte aux membres du personnel d'accéder à leurs données à caractère personnel et de les rectifier: dans le système Flexitime de l'ETF, une personne concernée a le *droit d'accéder* à ses données personnelles *et d'en solliciter la rectification* par une demande électronique.

D'après la notification, Flexitime est administré par une base de données Lotus Notes et accessible sur l'intranet de l'ETF. Toute personne concernée peut accéder à cette base de données au moyen de son identifiant et de son mot de passe. Les travailleurs flexibles peuvent consulter leur compte temps à tout moment. C'est pourquoi les personnes concernées (les utilisateurs de l'application) peuvent vérifier et, si nécessaire, solliciter la correction/suppression des données par une demande électronique. Les travailleurs flexibles sont tenus de vérifier les heures enregistrées par le système électronique en place et d'informer les RH des corrections à apporter en temps opportun à travers eRequest (Flexitime). Les demandes de correction introduites après plus de 5 jours de présence dans le bureau ne seront pas acceptées, sauf cas de

force majeure. En outre, les personnes concernées peuvent exercer à tout moment leurs droits au titre du règlement (CE) n° 45/2001 sur demande adressée au responsable du traitement.

Compte tenu tant du droit de correction que de verrouillage, le CEPD considère que, dans certaines occasions, le droit de rectification des données (article 14) est exercé conjointement au droit de verrouillage desdites données (article 15), par exemple lorsque la personne concernée en conteste l'exactitude. L'article 14 du règlement dispose que «*[l]a personne concernée a le droit d'obtenir du responsable du traitement la rectification sans délai de données à caractère personnel inexactes ou incomplètes*». Au cours d'une période permettant au responsable du traitement de vérifier l'exactitude des données, celles-ci doivent être verrouillées (sur demande de la personne concernée).

Par conséquent, dans le cas, comme en l'espèce, d'une véritable analyse de contrôle préalable, le CEPD considère que l'ETF doit instaurer une procédure permettant aux personnes concernées de demander le verrouillage des données la concernant. Cette solution ne doit pas perturber le système.

Toutefois, si l'ETF considère qu'un tel système peut se révéler impossible à mettre en œuvre et qu'il peut transmettre des objections légitimes au CEPD, celui-ci peut proposer une alternative au verrouillage. Dans son avis du 29 mars 2007 dans le dossier relatif au module TIM intégré au système SYSPER 2 de la Commission européenne, le CEPD a accepté une solution qui pourrait également être applicable. À l'instar du module TIM intégré à SYSPER 2, le verrouillage des données dans le cadre de l'application Flexitime de l'ETF ne peut être appliqué que de façon sélective, car un verrouillage complet entraverait l'intégralité du traitement des données. La solution pourrait être, chaque fois qu'un verrouillage est sollicité pour prouver les faits, à prendre un «instantané» des données au moyen d'une impression, d'une copie de sauvegarde ou d'un CD-ROM comme sous SYSPER 2 - TIM. Grâce à cette solution, trois copies devraient être mises à disposition, une pour le demandeur (le plaignant), une pour le responsable du traitement des données et la dernière pour le DPD de l'ETF. En effet, en cas de plainte, cela facilitera l'intervention de ce dernier. Cette solution serait acceptable parce qu'elle sert une finalité probatoire (article 15, paragraphe 1, points b) et c) du règlement).

Le CEPD note que, selon la notification, l'article 20 du règlement (CE) n° 45/2001 ne doit pas être appliqué, en principe, dans le cadre du présent traitement de données.

En conclusion, le CEPD considère que les conditions des articles 13 et 14 du règlement sont remplies, compte dûment tenu de la modification de la période de rétention (voir point 3.4 Conservation des données).

3.9. Information de la personne concernée

Les articles 11 et 12 du règlement (CE) n° 45/2001 énumèrent les informations qui doivent être fournies aux personnes concernées. Ils énumèrent une série d'éléments obligatoires et une autre série d'informations. Ces dernières sont applicables pour autant que, compte tenu des circonstances particulières du traitement en cause, elles soient nécessaires pour assurer un traitement des données équitable eu égard à la personne concernée. En l'occurrence, les données sont en partie collectées directement auprès de la personne concernée et en partie à d'autres sources.

L'article 11 (*Informations à fournir lorsque les données sont collectées auprès de la personne concernée*) doit être respecté dans le cas d'espèce. Les membres du personnel entrent et sortent eux-mêmes du système, les personnes concernées elles-mêmes fournissent donc les données.

L'article 12 (*Informations à fournir lorsque les données n'ont pas été collectées auprès de la personne concernée*) doit également être respecté puisque la liste d'informations d'identification est obtenue auprès de l'unité des RH de l'ETF.

Comme décrit dans la notification, des informations complètes sur la déclaration de confidentialité et le traitement des données seront intégrées à la politique concernée et placées sur l'intranet de l'ETF, accessible à tout moment à tout le personnel de l'ETF. En outre, la déclaration de confidentialité sera remise à chaque travailleur flexible en même temps que son badge personnel.

Actuellement, la déclaration de confidentialité fait partie du Guide de l'horaire flexible de l'ETF (point 6 des questions de protection des données). Le CEPD suggère que l'ETF envisage de mieux mettre en valeur cette information dans le guide voire peut-être d'adopter une déclaration de confidentialité spécifique, qui serait matériellement distincte du guide mais remise en même temps que ce dernier. En tout état de cause, elle devrait être transmise aux membres du personnel avant qu'ils ne commencent à prendre part au système Flexitime. L'objectif est d'attirer clairement l'attention des personnes concernées sur leurs droits en les informant au moyen d'une déclaration de confidentialité spécifique.

Le projet de déclaration de confidentialité spécifique contient la plupart des éléments visés aux articles 11 et 12 du règlement n° 45/2001. Cependant, il y a lieu de le compléter de manière à ce qu'il soit entièrement conforme auxdits articles 11 et 12 du règlement n° 45/2001. Par exemple, la déclaration de confidentialité devrait également indiquer la finalité du traitement. Des précisions supplémentaires s'imposent également en matière de rétention des données (voir point 3.4 ci-dessus) et de verrouillage des données (voir point 3.8 ci-dessus).

3.10. Mesures de sécurité

Conformément à l'article 22, 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.

(...)

Le CEPD a déjà précisé, dans un précédent avis en vue d'un contrôle préalable[5], le statut d'un numéro de puce RFID inséré dans une carte. Le numéro d'identification associé à la puce RFID constitue la donnée à caractère personnel visée par le règlement (CE) n° 45/2001. En effet, lorsqu'il est utilisé pour enregistrer le comportement d'un collaborateur et est mis en liaison avec le numéro personnel (c'est-à-dire avec le nom d'une personne, comme dans le cas d'espèce), ce numéro d'identification fait de la démarche un traitement de données à caractère personnel, ce qui impose le respect des principes de la protection des données.

(...) le CEPD recommande à l'ETF de reconsidérer la décision prise en matière de choix technologiques à travers une nouvelle évaluation, y compris un calendrier réaliste afin de mettre en œuvre le changement de technologie, eu égard au choix des meilleures techniques disponibles[6]. Dans ce cas, l'ETF pourrait également s'inspirer de l'exemple d'autres institutions.

---

[5] Voir Avis sur une notification en vue d'un contrôle préalable reçue du délégué à la protection des données de la Commission européenne à propos de la «mise en œuvre du Flexitime spécifique à la DG INFSO», délivré le 19 octobre 2007 (dossier 2007-218).

[6] Cette notion des meilleures techniques disponibles a été mise en avant par le CEPD dans son rapport annuel 2006. En outre, le CEPD est disposé à porter assistance sur d'éventuels choix technologiques alternatifs à l'avenir.

Le CEPD recommande également que la confidentialité et la protection des données soient mieux protégées contre la reproduction du badge ou la localisation du titulaire de carte. Des technologies plus appropriées, telles que la carte à puce sans contact recourant à l'UID aléatoire, pourraient être sélectionnées et mises en œuvre[7]. Autre solution possible, l'ETF pourrait mettre en œuvre une protection renforcée de la carte qui n'est levée que lorsque la carte est utilisée. Ces mesures techniques devraient être complétées de procédures stratégiques telles que: (i) l'interdiction du partage ou du prêt des cartes d'accès, (ii) l'obligation de signaler aussitôt tout vol ou perte de carte et (iii) la recommandation que les collaborateurs cachent leur carte d'accès lorsqu'ils se trouvent en dehors de locaux de l'ETF.

(...) Du fait des fonctions techniques du système liées à l'accès aux données à caractère personnel, l'unité Gestion des infrastructures et des technologies (ITM) (développeurs de logiciels) est également susceptible d'accéder aux données. Elle doit être informée et avisée des questions de protection des données (notamment la confidentialité et la sécurité).

Après avoir examiné avec attention les mesures de sécurité adoptées, le CEPD estime qu'elles sont adéquates eu égard à l'article 22 du règlement (CE) n° 45/2001.

Conclusion:

Il n'y a pas lieu de conclure à une violation des dispositions du règlement (CE) n° 45/2001. De même, la Fondation européenne pour la formation a déjà mis en œuvre une partie des propositions de recommandations établies par le CEPD au cours du délai laissé à l'ETF pour transmettre ses observations sur le projet d'avis. Cependant, certaines de ces recommandations doivent encore être mises en œuvre. Ces recommandations invitent notamment l'ETF à:

- s'assurer que les données à caractère personnel de ceux de ses collaborateurs qui ne souhaitent pas utiliser Flexitime ne soient pas importées dans la base de données Lotus Notes;

- faire en sorte qu'en cas d'erreur lors de l'insertion de l'heure enregistrée ou du transfert des données vers la base de données Lotus, un moyen efficace d'informer la personne concernée soit mis en œuvre afin de garantir le principe de qualité des données;

- modifier la période de rétention qu'elle envisage en ce qui concerne la rétention de données historiques;

- prévoir une procédure de suppression des données Flexitime (administratives et historiques) des personnes qui ont quitté l'agence. Une période de 2 semaines est considérée comme proportionnelle à la finalité du traitement;

- instaurer une procédure permettant aux personnes concernées de solliciter le verrouillage de ses données personnelles en cas de différend;

- veiller à ce que la déclaration de confidentialité spécifique soit mieux mise en valeur, voire peut-être séparée du Guide de l'horaire flexible et remise aux travailleurs flexibles en même temps que leur badge;

[7] Cette question a été mise en lumière l'an dernier par l'Organisation de l'aviation civile internationale (OACI) – voir p. 22: http://www.mrtd.icao.int/component/option,com_remository/Itemid,256/func,startdown/id,26/

- compléter la déclaration de confidentialité en ajoutant:

    - un paragraphe précisant que, dans les 2 semaines à compter de l'approbation d'une demande de sortie du système, les données de la personne concernée seront supprimées de la base de données;
    - que les données traitées dans le contexte analysé ici ne sont pas utilisées à d'autres fins que la finalité visée et que le «numéro de carte» n'est pas utilisé à d'autres fins que dans le cadre de Flexitime et qu'il n'est sauvegardé dans l'application Flexitime de l'ETF qu'afin de faire le lien entre la carte et la personne concernée;
    - à côté de la mention de la rétention des données administratives, un paragraphe sur la rétention de données historiques conformément à la recommandation du CEPD;

- veiller à ce que les membres de l'unité Gestion des infrastructures et des technologies (ITM) soient informés des questions de protection des données liées au traitement;

- envisager d'instaurer une procédure permettant d'assurer le verrouillage des données. À cette fin, l'utilisation d'un «instantané» des données à travers une impression, une copie de sauvegarde ou un CD-ROM pourrait être envisagée;

- introduire des dispositifs de sécurité renforcés sur la carte et reconsidérer son choix technologique en matière de sécurité.

Fait à Bruxelles, le 26 février 2009

[Signé]

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données