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 oeuvre du Flexitime spécifique à la DG INFSO"

Bruxelles, le 19 octobre 2007 (Dossier 2007-218)

1. Procédure

Le 24 mars 2007, le Contrôleur européen de la protection des données (CEPD) a reçu, par courrier électronique du délégué à la protection des données (DPD) de la Commission, une notification concernant une consultation relative à la nécessité d'un contrôle préalable, au titre de l'article 27, paragraphe 3, du règlement (CE) n° 45/2001, du traitement des données à caractère personnel dans le cadre du "Flexitime spécifique à la DG INFSO - DPD-1611 Version 2". Le 29 mars 2007, le CEPD a admis que le système devait faire l'objet d'un contrôle préalable, conformément à l'article 27 du règlement (CE) n° 45/2001 (ci-après dénommé "le règlement"). Le délai de deux mois pendant lequel l'article 27, paragraphe 4, fait obligation au CEPD de rendre son avis a commencé à courir à partir de la date à laquelle le CEPD a accusé réception de la notification et de la nécessité d'un contrôle préalable, c'est-à-dire le 29 mars.

Les 4 et 16 avril 2007, le CEPD a transmis des demandes d'informations complémentaires, auxquelles le responsable du traitement des données a répondu le 7 mai 2007. Le CEPD a demandé et reçu certaines précisions supplémentaires par téléphone le 24 mai. Le même jour, le CEPD a également été informé que le système prévu allait être modifié afin d'être intégré dans le module TIM. Après de nouveaux contacts et éclaircissements, le CEPD a décidé de suspendre la procédure de contrôle préalable le 31 mai, dans l'attente que le responsable du traitement des données élabore les nouvelles spécifications techniques. Le 16 juillet, celui-ci a communiqué les nouvelles spécifications techniques du système Flexitime intégré dans le module TIM (le CEPD a reçu deux documents techniques intitulés: "Software Requirements Specifications" (Spécifications des exigences en matière de logiciel) et "Technology and Infrastructure" (Technologie et infrastructure), ainsi que les modifications afférentes de la notification en vue d'un contrôle préalable et un nouveau projet de déclaration spécifique de confidentialité). Compte tenu de la complexité du dossier, le CEPD a décidé, dans le respect de l'article 27, paragraphe 4, du règlement 45/2001, d'étendre d'un mois la date limite pour l'adoption de son avis. Le 10 septembre 2007, le CEPD a transmis son projet d'avis au DPD en lui demandant de communiquer ses observations. Celles-ci sont parvenues au CEPD le 21 septembre 2007.

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

2. Examen du dossier

Cadre et objectif de l'horaire flexible à la Commission

Le 19 décembre 2006, la Commission a adopté le nouveau système Flexitime[1] prévoyant l'introduction de l'horaire flexible au sein des services de la Commission pour le 1er avril 2007 au plus tard[2]. Le cadre général de la gestion du temps est réglementé par le "SYSPER 2 Time Management System" (système de gestion du temps de SYSPER 2). L'objectif est d'assurer le système général de gestion du temps mis en place par la Commission pour lui permettre de gérer les congés et les absences, et notamment de gérer les heures supplémentaires (Flexitime). Il a été jugé que ce système était soumis au contrôle préalable du CEPD sur la base de l'article 27, paragraphe 2, point a), (présence de données relatives à la santé) et de l'article 27, paragraphe 2, point b) (traitements destinés à évaluer des aspects de la personnalité des personnes concernées). Le CEPD a rendu un avis sur ce système le 29 mars 2007[3].

À la lumière du Guide de l'horaire flexible, la Commission, estimant que l'un des principaux aspects de sa réforme administrative consiste à adoucir ses méthodes de travail en vue de permettre à ses agents de mieux concilier les obligations de la vie privée avec celles de la vie professionnelle, a décidé d'appuyer la mise en œuvre de l'horaire flexible dans ses services en permettant à tout le personnel de la Commission de bénéficier de cette possibilité dans le cadre de la semaine de travail de 37 heures et demie, dans le plein respect des dispositions du statut des fonctionnaires et de l'intérêt du service. Ce faisant, la Commission entend accroître la motivation de son personnel en le rendant davantage responsable de l'organisation de son temps de travail.

Les DG ou services de la Commission qui choisissent de mettre en œuvre ou de mettre à l'essai l'horaire flexible peuvent, sur la base du "Guide de l'horaire flexible"[4], recourir à des systèmes d'enregistrement manuel, de fichiers électroniques, de cartes magnétiques ou autres. La DG INFSO a décidé de mettre en œuvre l'horaire flexible en faisant usage de cette dernière possibilité.

Le présent dossier, intitulé "Système de gestion du temps de SYSPER 2 - Flexitime spécifique à la DG INFSO - DPO-1611 Version 2" (ci après dénommé "Flexitime (à la) DG INFSO) est lié à la notification susmentionnée car il ajoute à la mise en œuvre du système Flexitime à la DG INFSO une composante supplémentaire et de poids sous la forme d'une puce RFID intégrée dans le badge personnel nécessaire au pointage. L'introduction d'une technologie de cette nature dans un système d'horaire flexible augmente dès lors les risques spécifiques déjà inhérents au système. Sur la base de ce nouvel élément déterminant, le CEPD a dès lors considéré que le dossier en soit doit faire l'objet d'un contrôle préalable.

Description générale du système et justification de sa mise en oeuvre

La décision de mettre en œuvre le système Flexitime au moyen de badges électroniques au sein de la DG INFSO était fondée sur les résultats positifs issus d'un projet pilote mené dans cette DG entre mai et octobre 2005. Le 28 septembre 2006, la DG INFSO a fait connaître son intention de faire usage de badges électroniques aux DG ADMIN et DIGIT, qui ont répondu de manière positive.

---

1 Information administrative SEC(2006) 1796 5IA 62-2006 du 21 décembre 2006 - Guide de l'horaire flexible.

2 Un système Flexitime a déjà été élaboré dans une autre institution, à savoir le Conseil, au sujet duquel le CEPD a adopté un avis de contrôle préalable (dossier 2004-258 du 19 janvier 2006).

3 Voir www.edps.europa.eu.

4 Information administrative n° 62-2006 en date du 21 décembre 2006. Voir aussi la communication de la Commission sur l'utilisation de l'horaire flexible dans les services de la Commission (SEC(2006) 956 du 19 juillet 2006).

La participation au système d'horaire flexible élaboré au sein de la DG INFSO est fondée sur la participation volontaire, l'existence de ce système ne contraignant dès lors pas le personnel à s'écarter de l'horaire de travail normal. Les agents de la DG INFSO qui optent pour l'horaire flexible peuvent choisir la manière de saisir les heures d'arrivée et de départ. Lorsque le système des badges sera disponible, ils auront la possibilité d'utiliser soit l'interface TIM, soit leur badge qu'ils présenteront aux lecteurs de badges réservés à cet effet.

Toutefois, un chef d'unité pourrait décider que son service recourra au seul système des badges pour la saisie des heures dans le cadre de l'horaire flexible.

Les services de la Commission responsables de l'application Flexitime collecteront des données à caractère personnel dans la mesure nécessaire pour permettre à tous les agents de travailler, d'une manière flexible, le même nombre d'heures qu'ils sont tenus de prester, afin de mieux concilier le travail et la vie privée. L'horaire flexible est fondé sur le principe de l'enregistrement des heures prestées par un système de vérification transparent, qui devrait être facile et rapide à utiliser.

Les opérations de traitement mises au point par la DG INFSO se subdivisent en trois parties.

1. La collecte des pointages

La situation de l'horaire flexible à la DG INFSO peut se schématiser comme suit: une carte, deux lecteurs. Un lecteur est utilisé pour l'accès aux bâtiments et un autre est réservé à l'application Flexitime. La saisie des pointages pour l'horaire flexible s'effectuera via la présentation de la carte personnelle de l'agent. Ces cartes sont dotées de la technologie Mifare et comprennent un élément passif (le modèle employé est le classique Mifare 4 K, comme demandé par la Direction Sécurité). Flexitime utilisera des lecteurs spécifiques (c'est-à-dire distincts des lecteurs servant à la gestion du contrôle d'accès).

L'utilisateur doit présenter sa carte personnelle devant un des lecteurs installés dans le bâtiment. D'après la notification, cette technologie n'autorise qu'une distance d'au maximum 10 cm avec un lecteur extrêmement puissant, ce qui n'est pas le cas à la DG INFSO. Des essais ont montré que les lecteurs installés ne permettent qu'une distance maximale de 3 cm, ce qui évite toute activation involontaire. En outre, la distance de lecture maximale spécifiée dans le cahier des spécifications du fournisseur du lecteur de cartes est de 5 cm. Chaque puce Mifare se voit attribuer, au stade de la fabrication, un numéro de série unique, qui est la seule information transmise au lecteur.

2. Le transfert des pointages

Les données relatives aux pointages (l'identifiant unique et l'enregistrement de l'heure) sont ensuite transmises au reste de l'application, où le lien est établi entre l'identifiant unique de la puce Mifare et une personne donnée. Les pointages d'une personne sont recueillis tout au long de la journée et introduits le matin suivant dans le module TIM de SYSPER 2 via l'interface définie par la DG DIGIT.

Les données suivantes sont transférées: le numéro personnel, la date et les différents pointages que la personne a effectués au cours de la journée précédente. La personne recevra un courriel reprenant tous ses pointages pour éviter toute erreur dans la saisie des données dans le module TIM. Les erreurs doivent être rectifiées de manière interactive dans un délai de six jours à travers le module TIM de SYSPER 2.

Il est prévu de conserver une piste de vérification ("audit trail") de deux mois. Y figureront les pointages, le numéro personnel, l'état (erreur ou non) et la date de saisie. Un module sera prévu pour permettre au responsable du traitement des données de consulter cette piste de vérification (en cas de contentieux).
L'utilisateur peut vérifier chaque donnée à travers le module TIM de SYSPER 2.

3. Pointage au moyen de la carte personnelle

Un module d'application sera mis en place pour activer les cartes personnelles aux fins du pointage. Cette application enregistrera le lien entre le numéro personnel de l'utilisateur et l'identifiant unique de la puce Mifare intégrée dans la carte personnelle. Parallèlement, elle gérera également l'information indiquant si la personne a opté pour l'horaire flexible (son badge sera "activé" puisque seuls les agents optant pour l'horaire flexible sont appelés à utiliser les lecteurs destinés à cet effet). L'accès à cette application est protégé et n'est accordé qu'aux rôles d'"administrateur" et de "responsable du traitement des données". La DG INFSO recevra de la Direction Sécurité les données concernant le lien "numéro personnel-identifiant unique de la puce Mifare" et les données relatives au choix de l'horaire flexible seront disponibles sur SYSPER 2 (maître des données), la DG INFSO synchronisant ses données avec ces deux sources.

D'après la notification et les réponses complémentaires fournies au CEPD, la décision de la DG INFSO de mettre en oeuvre le système Flexitime par le biais de la technologie RFID s'appuie sur les motifs suivants:

Pour ce qui est de son caractère nécessaire, ce système de pointage électronique:
- représente un système dernier cri[5];
- garantit l'équité, la précision et la fiabilité des données;
- est une technologie familière à la DG INFSO, car celle-ci gère les projets de recherche européens en matière de technologies RFID;

En outre, pour ce qui est de son caractère proportionnel, ce système de pointage électronique:
- figure parmi les quelques possibilités autorisées par le point 5.1 du Guide de l'horaire flexible pour l'enregistrement des heures de travail dans le cadre de l'horaire flexible;
- est plus simple et entraîne une réduction considérable de la charge administrative pesant sur le personnel (voir les résultats positifs du projet pilote);
- est avant tout considéré comme ne portant pas atteinte à la vie privée, étant donné que:
  - la distance de lecture est limitée à quelques centimètres (le système est techniquement incapable de surveiller les déplacements dans un bâtiment ou entre plusieurs bâtiments);
  - chaque agent maîtrise l'utilisation de son badge et agit de manière volontaire (il présente son badge "flexitime" au lecteur chaque fois qu'il désire que celui-ci soit lu);
  - la carte ne contient qu'un numéro de série. D'après la notification et l'interprétation de la DG INFSO, ce dernier n'est pas une information personnelle. Voit l'analyse au point 3.

Enfin, du point de vue de la sécurité, la DG INFSO a fondé son choix technologique sur les recommandations émanant de la Direction Sécurité.

[5] Selon le responsable du traitement, la technologie de pointage actuelle (NEDAP) est actuellement en phase de retrait progressif et la norme qui sera utilisée à la DG INFSO (Mifare) représente 80 % de toutes les "cartes à puce sans contact" utilisées en ce moment.

La Direction Sécurité a adopté comme norme la technologie de la carte à puce sans contact pour les raisons suivantes:

- clés privées gérées par la Direction Sécurité elle-même (plutôt que par une société extérieure, comme c'est le cas actuellement);
- possibilité d'adopter un niveau élevé de cryptage (64 bits). Le CEPD prend acte du fait que le cryptage n'est pas appliqué dans le programme Flexitime actuel. Par conséquent, le numéro de carte ne fait l'objet d'aucun cryptage;
- niveau de sécurité élevé: cette technologie est utilisée dans bon nombre de secteurs sensibles tels que les cartes bancaires ou de crédit, les cartes d'identité, etc.

Caractéristiques du badge

Les agents de la DG INFSO ont reçu une nouvelle carte personnelle, distribuée par la Direction Sécurité, qui comprend la double technologie (comme déjà indiqué, celle destinée à l'utilisation du RFID pour l'horaire flexible est fondée sur la norme Mifare, tandis que l'autre, servant pour l'accès aux bâtiments, s'appuie sur la technologie actuellement utilisée et fournie par Nedap). La Direction Sécurité d'ADMIN a lié le numéro de la carte à la liste des personnes et a transmis toutes les cartes au responsable local de la sécurité de la DG INFSO.

Deux numéros sont dès lors associés à ces cartes: l'un est le "numéro Flexitime" et l'autre est le "numéro d'accès".
L'étiquette lisible sans fil, qu'on appelle "carte à puce sans contact", et qui est fondée sur la norme ISO 14443, est intégrée dans le badge personnel. Ces étiquettes appartiennent à un type particulier d'étiquettes RFID (à identification par radiofréquence), appelées étiquettes de proximité. Leur fréquence de service limite la distance de lecture à quelques centimètres (technologie de la carte à puce passive) D'après la notification, les lecteurs installés à la DG INFSO n'autorisent qu'une distance maximale de 3 cm. La seule information utilisée par la DG INFSO est l'identifiant unique de la puce RFID.

Pour le système Flexitime, la DG INFSO utilisera des lecteurs spécifiques (distincts et séparés de ceux servant à la gestion du contrôle d'accès aux bâtiments de la Commission et qui sont placés sous la responsabilité de la Direction Sécurité). Des lecteurs sont installés aux entrées empruntées par les agents pour accéder aux bâtiments. Dans les bâtiments BU 33 et BU 31, deux lecteurs seront placés dans le hall d'entrée et deux autres à chaque étage des parkings en sous-sol. Dans les bâtiments EUFO et BU 25, tous les lecteurs (quatre au total) ont été installés au rez-de-chaussée, puisque c'est le passage obligé pour tous les membres du personnel. Au total, vingt lecteurs sont en cours d'installation.

Les agents de la DG INFSO qui ne prennent pas part au système d'horaire flexible ne devront pas présenter leur badge et, par conséquent, ne feront pas usage de ces lecteurs. Puisque le module SYSPER II accepte ces saisies, le système local ne garde en mémoire les heures de début et de fin de journée que jusqu'à leur transfert au module SYSPER II.

Personnes concernées

D'après la notification, les personnes concernées visées par le système sont tous les agents des unités de la DG INFSO (fonctionnaires, agents temporaires, agents contractuels, personnel auxiliaire et experts nationaux détachés (END)). Le Guide de l'horaire flexible précise que celui-ci s'applique à tous les agents statutaires et aux personnes soumises au régime applicable aux autres agents, quel que soit leur groupe de fonction ou leur grade, ainsi qu'aux END. Toutefois, le point 1.4 de ce même Guide indique que certaines unités, parties d'unités ou catégories d'agents

peuvent être exclues de l'application de l'horaire flexible ou être soumises à un usage restreint de celui-ci en raison d'exigences de service particulières.

Les informaticiens ne sont pas soumis aux règles du statut du personnel et ne sont donc pas soumis à l'application Flexitime. Ils n'utiliseront dès lors pas les badges dotés d'une puce RFID à cet effet.

En outre, la DG INFSO suivra de près les instructions du Guide de l'horaire flexible. C'est ainsi qu'elle traitera les agents intérimaires et les stagiaires à l'instar des informaticiens et ne les autorisera pas à appliquer l'horaire flexible.

Les spécifications techniques complémentaires fournies au CEPD prévoient également que les membres du personnel qui ne figurent pas dans l'application mais qui travaillent à la DG INFSO d'après les informations disponibles dans le répertoire Ldap seront inclus dans l'application. Les données de ces agents qui seront importées sont les suivantes: adresse électronique, prénom, nom de famille, code d'accès et identifiant personnel. Il est également ajouté que les entrées des utilisateurs importés seront marquées "non enregistré" et "inactif".

Responsables du traitement et sous-traitants

Le responsable du traitement des données est le chef de l'unité INFSO R1 (propriétaire du système) et le sous-traitant est le chef de l'unité INFSO R4 (fournisseur du système).

Le responsable du traitement est le maître de l'application informatique. Il est le seul à pouvoir accéder à la piste de vérification de l'application (données temporelles et leur état de transmission au module TIM).

L'administrateur du système est désigné par le responsable du traitement. Il peut avoir accès aux liens entre identifiants uniques des badges et numéros personnels.

La possibilité de déléguer à un gestionnaire au sein de l'unité n'existe pas pour le logiciel développé à la DG INFSO. Les gestionnaires utilisent le module TIM de SYSPER 2.

Sur la base de la subdivision ci-dessus, la notification établit, pour le système, les deux catégories d'utilisateurs et les trois rôles ci-après:

Catégories d'utilisateurs:

- les utilisateurs types, c'est-à-dire tous les agents visés dans le Guide de l'horaire flexible (SEC(2006) 1796, §3;

- les utilisateurs avancés, soit toutes les personnes ayant accès à l'interface utilisateur graphique;

Rôles en matière d'accès:

- le rôle de responsable du traitement des données (catégorie d'utilisateurs avancés), qui aura accès à toutes les fonctionnalités; il est responsable de l'attribution des rôles d'administrateur;

- le rôle d'administrateur (catégorie d'utilisateurs avancés), qui aura accès à toutes les fonctionnalités, à l'exception des fonctions de vérification. Ce rôle est principalement défini à des fins de maintenance, puisque ces titulaires recevront des informations incohérentes ou

manquantes liées à des courriers électroniques. Ces personnes seront également chargées de la maintenance du lien agent/carte;

- le rôle standard (catégorie d'utilisateurs types), des utilisateurs qui n'auront pas accès à l'interface utilisateur graphique.

Une personne peut se voir attribuer plusieurs rôles à la fois. Il n'existe aucune hiérarchie dans les catégories d'utilisateurs. Par exemple, une personne peut être désignée comme responsable du traitement des données sans avoir de rôle standard. Cette exigence spécifique permet aux agents n'utilisant pas leur carte pour l'enregistrement des heures de travail de faire partie de la catégorie des utilisateurs avancés.

En ce qui concerne la gestion des rôles, l'application permet de désigner trois rôles de responsable du traitement des données et trois rôles d'administrateur.

Données requises pour le traitement

Les données recueillies lorsque la puce est présentée au lecteur sont le numéro de série de la carte et l'heure de présentation de celle-ci.

Le responsable du traitement décrit le système retenu par la DG INFSO comme une "mémoire tampon" entre les lecteurs de badges et le module TIM de SYSPER 2. C'est pourquoi aucun calcul de solde (entre les temps de travail officiel et réel) n'y est effectué. Ce calcul relève du traitement opéré par le module TIM de SYSPER 2. Cependant, d'autres traitements se produisent dans l'application Flexitime même (traitement du numéro personnel, du nom, etc.).

En fait, les données concernées vont au-delà de l'identifiant unique et de l'enregistrement des heures. Comme le montrait le projet de déclaration de confidentialité, les informations recueillies et ensuite traitées sur cette base sont, en fin de compte, les suivantes:
- l'identifiant unique du badge,
- les pointages et l'état de leur transfert vers le module TIM,
- le numéro personnel figurant dans SYSPER 2,
- l'indication que l'agent a choisi de participer à l'horaire flexible,
- le rôle de l'utilisateur au sein de l'application,
- l'adresse électronique,
- le prénom,
- le nom de famille,
- le code d'accès.

Information des personnes concernées

La notification prévoit la publication d'une déclaration spécifique de confidentialité pour l'horaire flexible, qui a été élaborée et sera disponible en ligne sur la page d'accueil de l'unité "Ressources humaines" (Responsable du traitement des données), à laquelle tous les agents de la DG INFSO peuvent avoir accès. Des projets de texte ont été soumis au CEPD pour examen.

Cette déclaration comprend une description générale du système, l'explication du transfert des pointages, ainsi que l'indication des personnes qui ont accès aux données et de celles à qui elles sont divulguées. Elle contient également des dispositions sur les modalités de protection et de sauvegarde des données, ainsi que sur les possibilités de vérification, de modification ou de suppression de celles-ci. On y trouve enfin des informations telles que la période de conservation des données, la base juridique et les coordonnées des personnes de contact.

Accès aux données à caractère personnel, rectification et effacement de celles-ci

Le projet de déclaration de confidentialité spécifiquement élaboré pour l'horaire flexible précise que, si les agents souhaitent vérifier, modifier ou supprimer une donnée les concernant, qui est enregistrée via l'application informatique d'enregistrement de l'horaire flexible de la DG INFSO, ils peuvent le faire à travers le module TIM de SYSPER 2, dans le respect des règles fixées par la DG ADMIN dans la notification de SYSPER 2 - TIM et ses annexes.

L'avis sur la notification en vue d'un contrôle préalable concernant SYSPER 2 indique, à propos de l'horaire flexible, que: "les droits d'accès, de rectification et d'opposition sont octroyés selon les moyens suivants: toutes les données personnelles (congés/ absences/ travail à temps partiel/ congés parental et familial, horaire flexible) sont accessibles par le titulaire (et partiellement fournies par lui), ce qui lui permet de les vérifier et au besoin de les corriger directement ou de demander la correction par un gestionnaire RRH (pour l'aspect des données relatives à l'identification) ou par son supérieur hiérarchique (pour l'aspect horaire flexible)".

Le système Flexitime de la DG INFSO ne contient aucune interface graphique qui soit accessible aux personnes concernées recouvrant un "rôle standard" (catégorie d'utilisateurs types, par opposition à celle d'utilisateurs avancés, tels qu'un responsable du traitement des données ou un administrateur). Les personnes concernées utilisent le module TIM de SYSPER 2 (personnellement ou via le supérieur hiérarchique ou le gestionnaire) afin d'avoir accès à leurs données à caractère personnel, de les vérifier et, si nécessaire, de les corriger[6].

La DG INFSO introduit une distinction entre données relatives à l'identification et données spécifiquement liées à l'horaire flexible.

Dans le premier cas (identification), les données sont liées à SYSPER 2 et peuvent, si nécessaire, être modifiées en suivant la procédure décrite dans la notification relative à ce système; dans le deuxième cas (données liées à l'horaire flexible), les modifications sont apportées via le module TIM de SYSPER 2, dans le respect des règles définies par la DG ADMIN dans la notification de SYSPER 2 - TIM et ses annexes. En cas de contentieux, l'intéressé pourrait demander que les données soient conservées ou verrouillées par le responsable du traitement des données (en l'espèce, le chef de l'unité "Ressources humaines" de la DG INFSO).

Stockage des données

Les données sont stockées dans une base de données Oracle. Au cours des six premiers jours, aucun dossier papier spécifique n'est concerné. L'application transfère les pointages enregistrés au gestionnaire du module TIM conformément aux règles définies par la DG ADMIN dans la notification de SYSPER 2 - TIM et ses annexes. D'après les règles du module TIM de SYSPER 2, les corrections ou ajouts peuvent être effectués dans un délai de six jours par la personne concernée elle-même (pour autant que le supérieur hiérarchique n'ait pas décidé de centraliser l'encodage). Dans ce cas, l'incident n'est pas enregistré sur un formulaire papier standard.

Dès lors, un dossier papier enregistre les incidents de procédure afin de compléter ou corriger les données dans le module TIM de SYSPER 2 lorsque le délai de six jours s'est écoulé ou si le supérieur hiérarchique a opté pour l'accès centralisé au module TIM de SYSPER 2.

---

6 Voir à cet égard le contrôle préalable 2007-0063: "SYSPER 2: module Time Management".

L'application d'enregistrement électronique Flexitime de la DG INFSO agit comme une mémoire tampon pour les pointages devant être transférés vers le module TIM. Dans ces conditions et compte tenu de la nécessité de conserver une piste de vérification de l'enregistrement des données, la DG INFSO prévoit une piste de vérification avec une période de conservation de deux mois (voir description générale du système à la page trois ci-dessus).

Traitement automatisé

Les opérations de traitement automatisé sont les suivantes:
- l'enregistrement des pointages de chaque personne;
- le transfert des pointages vers le module TIM de SYSPER 2. En cas d'erreur, un courriel contenant les saisies de pointage est adressé à l'utilisateur;
- une fonction de gestion utilisateur/carte (synchronisation de l'utilisateur avec SYSPER 2, synchronisation de l'identifiant unique avec la base de données des cartes personnelles, création/modification, suppression d'utilisateur, création/modification/suppression de cartes);
- une fonction d'établissement de rapports (piste de vérification: liste des saisies de pointage avec l'état et la date pour chaque personne).

Traitement manuel

Conformément aux spécifications techniques, l'application de la DG INFSO ne prévoit aucun traitement manuel spécifique.

Les erreurs survenues lors de la saisie du pointage doivent être corrigées via le module TIM de SYSPER 2 dans le respect des règles définies par la DG ADMIN dans la notification du SYSPER 2 - TIM et ses annexes. Lorsque la modification peut être apportée par la personne concernée, celle-ci peut y procéder dans un délai de six jours. Passé ce délai, le supérieur hiérarchique ou le gestionnaire de l'unité peut corriger l'information. Si c'est l'approche centralisée qui a été choisie, toutes correction doit être demandée au gestionnaire de l'unité.

Selon la méthode choisie par le supérieur hiérarchique, cela peut se faire au moyen d'un formulaire papier normalisé. Les formulaires doivent être détruits une fois que le bilan mensuel des heures de travail a été validé.

Sécurité

Le Mifare utilisé est le standard 4 K, conformément aux prescriptions de la Direction Sécurité.

D'après les informations complémentaires fournies par la DG INFSO, l'analyse des différents scénarios a fait apparaître que les infimes risques potentiels ont été atténués par les mesures de sécurité adoptées, telles le choix de la technologie, le lieu sécurisé choisi pour l'installation du matériel, l'absence de données à caractère personnel sur les cartes, le rayon d'action extrêmement limité des lecteurs et le contrôle de l'accès à l'application.

Les données recueillies dans l'application Flexitime ne sont accessibles à personne en dehors de la Commission. En interne, l'accès aux données n'est octroyé qu'à la personne concernée ou aux fonctionnaires de la Commission désignés à cet effet, après introduction d'un code d'accès et d'un mot de passe.

Le système est hébergé sur des serveurs gérés par le personnel de la gestion des ressources informatiques de la DG INFSO (unité R 4) et situés physiquement dans des salles de serveurs sécurisées sous la contrôle de l'unité R 4.

Les contrôleurs sont situés dans la salle PABX (autocommutateur privé relié au réseau public) sécurisée. Pour accéder à cette salle, il faut soit appeler la DG DIGIT et motiver la nécessité d'ouvrir la salle, soit disposer d'une carte d'accès spécifique réservée uniquement aux personnes autorisées (maintenance). L'accès à la salle des ordinateurs requiert une carte d'accès spécifique avec un code PIN qui y est associé.

Les contrôleurs des lecteurs sont installés dans des salles PABX sécurisées placées sous le contrôle de la DG DIGIT.

En ce qui concerne l'accès logique au serveur, deux groupes de personnes sont identifiés: les administrateurs de bases de données (ABD) et les administrateurs de système locaux (ASL). Seules ces deux catégories de personnes possèdent un accès logique au serveur. Les ABD assurent des tâches de maintenance des bases de données (Oracle) telles que l'optimisation des prestations et des opérations de sauvegarde. Les ASL s'occupent de tâches de maintenance des ordinateurs serveurs telles que la mise à niveau et l'installation de patches de sécurité.

Les ABD et les ASL sont impérativement des personnes différentes, qui ne sont pas concernées par la portée fonctionnelle des applications dont elles s'occupent. La liste des ABD et des ASL sera communiquée au coordinateur de la protection des données (CPD).

3. Les aspects légaux

3.1 Contrôle préalable

Compte tenu de l'opération spécifique qui se déroule lors de ce traitement, le CEPD estime qu'il est important de se rapporter à la définition des termes "données à caractère personnel". Selon l'article 2, point a), du règlement, *"on entend par "données à caractère personnel": toute information concernant une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée"); 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*".

Il apparaît que le système examiné, à savoir l'application Flexitime spécifique à la DG INFSO, traite des données à caractère personnel puisque les données se rapportent à des personnes physiques pouvant être identifiées, par exemple, par le biais d'un nom ou d'un numéro personnel. Même le numéro de série, qui n'est pas en soi une donnée à caractère personnel, devient, au sein du système, un numéro personnel dès lors qu'il est relié ou reliable 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 effectué par la Commission est mis en oeuvre pour l'exercice d'activités qui relèvent du champ d'application du droit communautaire (article 3, paragraphe 1, du règlement (CE) n° 45/2001).

Le système Flexitime à la DG INFSO comporte un traitement tant automatique que manuel. Il s'agit donc d'un traitement en partie automatisé. Par conséquent, l'article 3, paragraphe 2, du règlement s'applique.

D'après le point 5.1 du Guide de l'horaire flexible[7], le pointage des heures peut se faire via des systèmes d'enregistrement manuels, des fichiers électroniques, des cartes magnétiques ou des systèmes similaires. L'article 27, paragraphe 1, du règlement (CE) n° 45/2001 soumet au contrôle préalable du CEPD tous les "*traitements susceptibles de présenter des risques spécifiques au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités*". Le système de gestion TIM, dont l'application Flexitime fait partie, a fait l'objet d'un contrôle préalable de la part du CEPD sur la base de l'article 27, paragraphe 2, points a) et b). Par ailleurs, le CEPD estime que l'introduction d'une technologie de cette nature (la puce RFID intégrée dans le badge) dans un système d'horaire flexible représente une innovation notable dans le système ayant déjà fait l'objet d'un contrôle préalable et qu'elle accroît les risques spécifiques déjà inhérents au système. Dès lors, le présent contrôle préalable relève de l'article 27, paragraphe 1, du règlement.

Le contrôle préalable visant à étudier les situations susceptibles de présenter certains risques, le CEPD devrait rendre son avis avant que le traitement ne commence. Le présent avis constitue un véritable contrôle préalable. A cet égard, le CEPD salue la note interne de la DG INFSO (courriel adressé au personnel de la DG INFSO le 30 mars 2007) par laquelle celle-ci déclarait qu'elle n'allait pas mettre en œuvre le système de pointage par badge avant d'avoir obtenu le feu vert du CEPD.

Toutefois, il est important de souligner que le CEPD est favorable (dans ses avis ainsi que dans ses rapports annuels) à l'idée que la mise au point de technologies "privacy by design" (prise en compte du respect de la vie privée dès la conception) pourrait promouvoir une meilleure protection des données. C'est la raison pour laquelle le CEPD aurait apprécié que lui-même ou le DPD aient été associés à un stade précoce au processus prévu à la DG INFSO, par exemple lorsque le projet pilote était en cours d'élaboration[8].

Dans le dossier de contrôle préalable susmentionné du 29 mars 2007, le CEPD a souligné qu'il n'y a aucun motif de croire à une violation des dispositions du règlement 45/2001, pour autant que les observations qu'il formule soient pleinement prises en compte. Par conséquent, les recommandations tant générales que spécifiques concernant le Flexitime figurant dans ledit avis relatif à un contrôle préalable demeurent valables pour l'examen du présent contrôle préalable.

Le CEPD a reçu la notification du DPD le 29 mars 2007. Une demande d'informations a été transmise le 4 avril 2007 et une nouvelle demande d'informations portant sur des aspects liés à la sécurité a été adressée le 16 avril 2007. Le délai de deux mois pendant lequel le CEPD doit rendre son avis pour un contrôle préalable a été suspendu. La Commission a transmis une réponse aux deux demandes le 7 mai 2007. Le 24 mai, le CEPD a demandé et reçu certaines informations supplémentaires par téléphone. Le responsable du traitement a également annoncé que les aspects techniques du système seraient modifiés. En raison des modifications qui allaient être apportées à la notification, le CEPD a suspendu la procédure le 31 mai, pour permettre au responsable du traitement d'élaborer les spécifications techniques. Les documents sont parvenus le 16 juillet. Compte tenu de la complexité du dossier, le CEPD a décidé, dans le respect de l'article 27, paragraphe 4, du règlement 45/2001, de retarder d'un mois la date limite pour l'adoption de son avis. Le 10 septembre 2007, le CEPD a transmis le projet d'avis au DPD en lui demandant de communiquer ses observations. Les observations de la Commission sont parvenues au CEPD le 21 septembre 2007 et une réunion entre les collaborateurs du CEPD, le responsable du traitement des données du système Flexitime et le DPD de la Commission a eu lieu

7 Information administrative n° 62-2006 en date du 21 décembre 2006.

8 A titre d'exemple, c'est la procédure qui a été suivie par le Conseil lors de la mise au point de son système Flexitime, à laquelle le CEPD est associé depuis le stade du projet pilote.

le 12 octobre 2007, la procédure étant suspendue jusqu'à la tenue de cette réunion. La procédure de contrôle préalable a été suspendue pour une durée de 100 jours + 11 jours (pour les observations) + 1 mois de prolongation (article 27, paragraphe 4). Le CEPD rendra son avis le 19 octobre 2007.

3.2 Licéité du traitement

Le traitement des données à caractère personnel ne peut s'effectuer qu'à condition de pouvoir le fonder sur l'article 5 du règlement n° 45/2001.

Parmi les différents motifs énumérés à l'article 5 du règlement (CE) n° 45/2001, le traitement notifié pour contrôle préalable relève du point a), qui prévoit que le traitement de données 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 d'établir si le traitement est conforme à l'article 5, point 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),
- la communication de la Commission sur l'utilisation de l'horaire flexible dans les services de la Commission (SEC(2006) 956 du 19 juillet 2006),
- l'information administrative n° 62-2006 en date du 21 décembre 2006: Guide de l'horaire flexible.

Le CEPD souligne que le Guide de l'horaire flexible prévoit à son point 5.1 concernant l'enregistrement des heures de travail, que: "*Le chef d'unité doit veiller à ce que les heures de travail de ses collaborateurs soient enregistrées conformément à la procédure visée au point 3.1. À cet effet, les DG et les services peuvent utiliser des systèmes d'enregistrement manuels, des fichiers électroniques, des cartes magnétiques ou des systèmes similaires. Tout système d'enregistrement doit être proportionné et conforme au règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires*".

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

Le CEPD note que la Commission 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, point 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*".

Tel que ce système de pointage électronique est présenté par la DG INFSO, du point de vue de la nécessité:

- il représente un système dernier cri;
- il garantit l'équité, la précision et la fiabilité des données;
- c'est une technologie familière à la DG INFSO, car celle-ci gère les projets de recherche européens en matière de technologies RFID.

Le CEPD estime qu'il n'y a pas de nécessité spécifique de mettre au point un système de pointage utilisant le 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 "nécessité" ne signifie pas que le procédé est 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 sauvegardes et la proportionnalité sont avérées, on peut conclure que ce système remplit les conditions de "nécessité".

Enfin, la participation au système Flexitime en soi est fondée sur une participation volontaire.

Pour ce qui est du système spécifique de saisie des heures d'arrivée et de départ, c'est-à-dire par l'utilisation de l'interface TIM ou de badges à présenter aux lecteurs de badges disposés à cet effet, le choix revient en principe à chaque participant, le chef d'unité pouvant toutefois décider l'adoption d'un système homogène dans son service.

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 recueillies sont un numéro de carte magnétique (numéro de série) et les événements quotidiens (arrivée et départ). En outre, le numéro d'identification du lecteur n'est jamais recueilli ou traité avec les événements quotidiens. Le CEPD juge cela adéquat et pertinent. Ces données ne sont pas considérées comme excessives.

Les spécifications techniques complémentaires fournies au CEPD prévoient également que les membres du personnel qui ne figurent pas dans l'application mais qui travaillent à la DG INFSO d'après les informations disponibles dans le répertoire Ldap, seront importés dans l'application. Les données de ces agents qui seront importées sont les suivantes: adresse électronique, prénom, nom de famille, code d'accès et identifiant personnel. Il est également ajouté que les entrées des utilisateurs importés seront marquées "non enregistré" et "inactif".

En principe, le CEPD jugerait l'inclusion des "utilisateurs inactifs" excessive aux fins du traitement, puisque cela concerne des personnes ne relevant pas du système Flexitime. Aucune motivation raisonnable n'ayant été apportée au CEPD pour justifier le maintien de cette catégorie d'agents dans la base de données (Oracle), le CEPD ne voit aucune raison d'inclure dans l'application des agents qui n'y font l'objet d'aucun traitement, tout en travaillant à la DG INFSO. Cela ne concerne pas uniquement les informaticiens, les agents intérimaires et les stagiaires, mais aussi, dans le respect du principe de minimisation des données traitées, les agents de la DG INFSO qui décident de ne pas adopter le système d'horaire flexible. Le CEPD recommande que la DG INFSO analyse les modalités et la fréquence des mises à jour de la base de données en vue de mettre en œuvre cette recommandation concernant les catégories de personnes qui ne doivent pas être incluses dans la base de données de l'horaire flexible et qu'elle l'informe des résultats obtenus.

En outre, la notification précise qu'aucune donnée relevant des catégories de données visées à l'article 10, paragraphe 1 (catégories particulières de données), n'est traitée dans le cadre du traitement notifié pour contrôle préalable. Compte tenu de l'objectif général visé par la DG INFSO lorsqu'elle met en œuvre un traitement de données relatives à l'horaire flexible, le CEPD estime que la collecte de catégories particulières de données ne figure pas dans les intentions de la DG INFSO.

Les données doivent être "*traitées loyalement et licitement*" (article 4, paragraphe 1, point a), du règlement). La licéité du traitement a déjà fait l'objet d'une analyse (voir point 3.2 ci-dessus). Quant à la loyauté, elle a trait aux informations qui doivent être communiquées à la personne concernée (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 dans son ensemble doit assurer l'exactitude et la mise à jour des données. Il en est ainsi dans ce cas.

Les erreurs survenues lors de la saisie du pointage doivent être corrigées via le module TIM de SYSPER 2 dans le respect des règles définies par la DG ADMIN dans la notification de SYSPER 2 - TIM et ses annexes. Lorsque la modification peut être apportée par la personne concernée, celle-ci peut y procéder dans un délai de six jours. Passé ce délai, le supérieur hiérarchique ou le gestionnaire de l'unité peut corriger l'information. Si c'est l'approche centralisée qui a été choisie, toutes les corrections doivent être demandées au gestionnaire de l'unité.

Par ailleurs, en ce qui concerne le droit d'accès et de rectification, voir point 3.8 ci-dessous.

3.4 Conservation des données

L'article 4, paragraphe 1, point 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*". *"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."*

Le CEPD tient à confirmer la règle applicable à la conservation des données, qui a été présentée dans le dossier de contrôle préalable concernant le module "Time Management" de SYSPER 2. En effet, pour ce qui est de l'aspect de SYSPER 2 relatif à la conservation des données, il est souligné que les données concernant l'horaire flexible sont conservées pendant l'année calendrier en cours. Ces données seront supprimées après la clôture de la procédure de transfert des jours de

congé annuel non pris à l'année suivante, et au plus tard à la fin de mars. Dans le cas où le calcul de l'horaire de travail quotidien se fait au niveau du chef d'unité ou de secteur et est basé sur des relevés intermédiaires, ces derniers seront détruits après la validation du bilan mensuel par le chef d'unité ou de secteur, et le 15 du mois suivant au plus tard.

Pour ce qui est de la conservation spécifique des données dans l'application de la DG INFSO, le projet de déclaration spécifique de confidentialité établit que l'application pourrait se décrire comme une simple mémoire tampon des données de pointage devant être transférées vers le module TIM et que, vu la nécessité de conserver une piste de vérification des données d'enregistrement, toutes les données reçues sont stockées pendant une durée maximale de deux mois.

Le même délai s'applique pour le verrouillage et l'effacement des données en cas de demande légitime motivée émanant des personnes concernées.

Le CEPD estime que ces périodes de conservation sont conformes aux exigences fixées à l'article 4, paragraphe 1, point e), du règlement.

À la lecture de la notification, le CEPD conclut que l'établissement de statistiques relatives aux données à caractère personnel n'est pas autorisé au-delà de la période de conservation d'un an, ce qui est conforme aux dispositions de l'article 4, paragraphe 1, point e). Néanmoins, le CEPD tient à souligner qu'en cas d'utilisation de ces données au-delà de la période de conservation des données, il est nécessaire que ces données soient anonymisées (article 4, paragraphe 1, point e), du règlement).

3.5 Usage 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*". Le traitement vise à ce que, sur la base du principe de la saisie des heures de travail, l'horaire flexible permette à tous les agents de travailler, d'une manière souple, le même nombre d'heures qu'ils sont tenus de prester, afin de mieux concilier le travail et la vie privée. La Commission n'utilise pas les données traitées dans le cadre examiné pour d'autres finalités que celle qu'elle s'est fixée. En outre, elle souligne avec énergie que le "numéro de carte magnétique" n'est pas utilisé à d'autres fins que dans le cadre de l'horaire flexible et qu'il n'est stocké dans l'application Flexitime de la DG INFSO que pour établir le lien entre la carte et la personne concernée. Le CEPD en conclut que les finalités du traitement restent inchangées. Par conséquent, l'article 6, paragraphe 1, du règlement ne s'applique pas à ce dossier et l'article 4, paragraphe 1, point b), est respecté.

3.6 Transfert des données

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*."

La déclaration spécifique de confidentialité explicite les catégories de personnes susceptibles d'avoir accès aux données enregistrées via l'application informatique d'enregistrement de la DG INFSO. Les deux catégories mentionnées sont les suivantes: le responsable du traitement et l'administrateur du système.

Ces transferts sont légitimes puisqu'ils sont nécessaires à l'exécution légitime des missions relevant de la compétence du destinataire.

En ce qui concerne la délivrance des cartes, elle donne lieu à un autre transfert de données. La DG INFSO a procédé au remplacement des cartes en une seule opération globale par l'envoi d'une liste des personnes dont la carte devait être remplacée et la réception des cartes correspondantes. Le CEPD note que les cartes établies par la Direction Sécurité ont été transmises, pour des raisons de sécurité, au responsable local de la sécurité de la DG INFSO. Le CEPD recommande que celui-ci ne conserve pas la(les) liste(s) comportant le lien entre les personnes et le numéro "Flexitime" de la carte. En effet, la situation régnant dans l'application Flexitime diffère de l'objectif de sécurité associé à l'autre numéro de la carte, qui doit servir au contrôle de l'accès au bâtiment. Dans le cas de l'horaire flexible, l'accès au numéro "Flexitime" de la carte doit être limité aux personnes compétentes de la DG INFSO, dont le responsable local de la sécurité ne fait pas partie. La DG INFSO devrait dès lors s'assurer que ce dernier n'entre pas en possession de cette liste. Cette recommandation s'applique également au cas des listes de nouveaux utilisateurs.

Le CEPD interprète également qu'il ne sera procédé à aucun transfert de données à l'extérieur de la Commission. Les données recueillies dans l'application Flexitime ne sont normalement accessibles à personne en dehors de la Commission.

3.7 Traitement d'un numéro personnel ou d'un identifiant unique

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 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 Flexitime.

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 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 a déjà été examinée dans le contrôle préalable de la gestion du TIM de SYSPER 2. 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 Flexitime. 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.

3.8 Droit d'accès et de rectification

L'article 13 du règlement (CE) n° 45/2001 établit un droit d'accès - et les modalités de son exercice - à la demande de la personne concernée par le traitement. L'article 14 prévoit le droit de rectifier des données à caractère personnel inexactes ou incomplètes.

La notification en vue d'un contrôle préalable et les informations complémentaires fournies par le responsable du traitement décrivent la possibilité d'accès aux données à caractère personnel les concernant et mentionnent la possibilité donnée aux agents de les rectifier.

En ce qui concerne l'accès, le CEPD salue la distinction opérée par la DG INFSO entre deux catégories de données: les données relatives à l'identification et celles qui sont spécifiquement liées à l'horaire flexible. Les données relatives à l'identification sont liées à SYSPER 2 et peuvent, si nécessaire, être modifiées selon la procédure prévue pour ce système (voir avis relatif au contrôle préalable concernant SYSPER 2 - module TIM mentionné ci-dessus). Cet accès n'est accordé aux personnes concernées que moyennant la saisie d'un code d'accès et d'un mot de passe. Ces codes d'accès et mot de passe sont fondés sur le Service d'Authentification de la Commission Européenne (ECAS), qui permet également d'avoir accès à d'autres applications informatiques de la Commission. Les personnes concernées (les utilisateurs de l'application) pourraient avoir accès aux données les concernant afin de les vérifier et, si nécessaire, de les corriger.

Pour ce qui est des données liées à l'application Flexitime, les personnes concernées utilisent le module TIM de SYSPER 2 (personnellement ou via le supérieur hiérarchique ou le gestionnaire) afin d'avoir accès à leurs données personnelles, de les vérifier et, si nécessaire, de les corriger. Par conséquent, si le supérieur hiérarchique marque son accord pour que les agents accèdent personnellement à leurs données, ces derniers peuvent modifier ou compléter eux-mêmes les pointages enregistrés dans un délai de six jours via le module TIM de SYSPER 2. Passé ce délai, ou si le supérieur hiérarchique a opté pour une approche centralisée, il est nécessaire de passer par ce dernier ou par un gestionnaire désigné par lui pour obtenir la correction ou l'ajout de données.

Compte tenu tant du droit de rectification que du droit de verrouillage, le CEPD estime que, dans certains cas, le droit de rectification des données (article 14) est exercé simultanément avec le droit de verrouillage de celles-ci (article 15), notamment lorsque la personne concernée conteste leur exactitude. L'article 14 du règlement stipule que "*la personne concernée a le droit d'obtenir du responsable du traitement la rectification sans délai de données inexactes ou incomplètes"*. Lors de la période permettant au responsable du traitement de vérifier l'exactitude des données, ces dernières doivent être verrouillées (à la demande de la personne concernée).

Dans son avis du 29 mars 2007 relatif au module TIM incorporé dans SYSPER 2, le CEPD a marqué son accord sur une solution qui peut s'appliquer dans le présent dossier.
À l'instar du module TIM incorporé dans SYSPER 2, le verrouillage de données prévu dans l'application Flexitime de la DG INFSO ne pourrait s'appliquer que d'une manière sélective, étant donné qu'un verrouillage total entraverait l'ensemble du traitement des données. La DG INFSO explique que, à chaque demande de verrouillage en vue d'établir les faits, la DG INFSO sera en mesure de prendre une "photographie" des données au moyen d'une impression, d'une copie de sauvegarde ou d'un CD Rom, de la même manière que dans le module TIM de SYSPER 2. Deux copies sont mises à disposition, une pour le demandeur (plaignant) et une pour le responsable du traitement des données.

Comme il l'a expliqué dans le dossier de contrôle préalable concernant SYSPER 2, le CEPD peut accepter cette solution uniquement dans la mesure où la finalité est probatoire (article 15, paragraphe 1, points b) et c), du règlement) et où les implications informatiques pour modifier SYSPER 2 afin qu'il opère un verrouillage sélectif ne sont pas possibles à mettre en œuvre pour l'instant. Le verrouillage aurait en effet pour conséquence, dans ce cas, de pénaliser encore davantage la personne concernée.

En cas de mise en œuvre de la procédure de verrouillage, le CEPD souhaiterait qu'un troisième exemplaire de l'impression, de la copie de sauvegarde ou du CD Rom soit mis à la disposition du

coordinateur de la protection des données de la DG INFSO. Cela permettrait, en effet, de rendre son intervention plus aisée en cas de plainte.

Le CEPD note que, d'après la notification, l'article 20 du règlement 45/2001 ne doit pas s'appliquer, en principe, dans le cadre de ce traitement de données.

En conclusion, le CEPD estime que les conditions des articles 13 et 14 du règlement sont remplies.

3.9 Information de la personne concernée

Les articles 11 et 12 du règlement (CE) n° 45/2001 énumèrent les informations à fournir à la personne concernée. Dans ces articles figurent une liste de points obligatoires et une série d'autres informations. Ces dernières s'imposent dans la mesure où, en fonction des conditions particulières du traitement en question, elles sont nécessaires pour garantir un traitement équitable des données à l'égard de la personne concernée. En pareil cas, une partie des données sont collectées directement auprès de la personne concernée et une autre partie le sont auprès de tiers.

Dans le présent dossier, il y a lieu d'observer les dispositions de l'article 11 (*Informations à fournir lorsque les données sont collectées auprès de la personne concernée*). Les agents pointant personnellement dans le système, ce sont les personnes concernées qui fournissent elles-mêmes les données.

L'article 12 (*Informations à fournir lorsque les données n'ont pas été collectées auprès de la personne concernée*) devrait également s'appliquer, étant donné que la liste de données relatives à l'identification est extraite de SYSPER 2 à propos des agents de la DG INFSO.

Les personnes concernées sont informées de l'existence des actes suivants:
- le Guide de l'horaire flexible (information administrative n° 62 du 21 décembre 2006 - SEC(2006) 1796);
- la communication de la Commission sur l'utilisation de l'horaire flexible dans les services de la Commission (SEC(2006) 956 du 19 juillet 2006).
- une déclaration spécifique de confidentialité de la DG INFSO, que tout un chacun pourrait consulter en ligne sur la page d'accueil de l'application.

Le projet de déclaration spécifique de confidentialité, qui était annexé à la notification initiale, a été remplacé par une autre version pendant l'examen de la procédure de traitement; il contient la plupart des dispositions des articles 11 et 12 du règlement (CE) n° 45/2001.

Cette déclaration de confidentialité est intitulée: "*Specific privacy statement for IT flexitime registering application in DG INFSO*" (NDT: ce texte n'existant pour l'instant qu'en anglais, le titre et les citations qui suivent font l'objet d'une traduction non officielle en français) (Déclaration spécifique de confidentialité pour l'application d'enregistrement électronique de l'horaire flexible à la DG INFSO). Le CEPD est convaincu que l'emploi du terme anglais "registering" (enregistrement) n'est pas exact car l'application Flexitime est un système à part entière et pas uniquement une fonction d'enregistrement. Il s'ensuit que la déclaration de confidentialité ne vise pas seulement l'enregistrement, mais aussi l'application qui traite et agit en tant que mémoire tampon pour le module de gestion TIM. Cette déclaration spécifique de confidentialité vient s'ajouter à la déclaration générale de confidentialité concernant l'horaire flexible (émanant de la DG ADMIN), qui couvre également le personnel de la DG INFSO.

Toutefois, dans ce dossier particulier, dans la mesure où ces informations sont nécessaires afin de garantir un traitement équitable et compte tenu des spécificités de cette technologie et des inquiétudes qu'elle peut susciter, le CEPD conseille d'apporter les aménagements ci-après:

- il y a lieu de modifier la référence à l'avis du CEPD en remplaçant les termes "who delivered a favourable opinion" (qui a rendu un avis favorable) par "who delivered an opinion" (qui a rendu un avis). Le CEPD souhaiterait également que, pour des motifs de transparence, la déclaration de confidentialité contienne un lien vers le présent avis;
- pour être exhaustif et compte tenu de la faculté laissée aux chefs d'unité de déléguer leurs droits à un "gestionnaire" au sein de leur service, le CEPD souhaiterait que cette catégorie de personnes, susceptibles d'être destinataires des données, soit également citée dans la déclaration de confidentialité, au même titre que le responsable du traitement des données et l'administrateur du système;
- comme expliqué au point 3.1 ci-dessus, il convient de supprimer la phrase: "*This is not related to any personal data*";
- il faudrait ajouter un alinéa précisant clairement les personnes ou catégories de personnes de la DG INFSO qui sont autorisées à utiliser l'application Flexitime (c'est-à-dire les agents concernés);
- le projet de déclaration spécifique de confidentialité n'indique pas clairement les informations qui peuvent être directement modifiées par la personne concernée et celles pour lesquelles elle doit s'adresser à l'administrateur du système pour obtenir le changement. Il y a lieu, en effet, de reformuler le passage suivant: "*data subjects who wish to verify, modify or delete <u>any</u> of their data registered via the DG INFSO IT flexitime registering application can do it via their access to the SYSPER 2 - TIM module" (les personnes concernées souhaitant vérifier, modifier ou supprimer <u>toute</u> donnée à leur sujet enregistrée via l'application d'enregistrement électronique Flexitime de la DG INFSO peuvent le faire via leur accès au module TIM de SYSPER 2);*
- suite à la recommandation du CEPD concernant l'exécution d'une troisième copie, il convient que le coordinateur de la protection des données de la DG INFSO figure lui aussi dans la déclaration de confidentialité du système;
- il faudrait mentionner le caractère obligatoire ou facultatif de la réponse aux questions, ainsi que les conséquences éventuelles d'un défaut de réponse, par exemple, les conséquences résultant de l'absence de pointage. Par analogie avec un questionnaire, le personnel devrait être informé des implications pratiques du pointage ou de l'absence de pointage (c'est-à-dire l'inscription sur un fichier papier);
- il convient de mentionner la base juridique en plus du Guide de l'horaire flexible;
- il y a lieu d'indiquer la période de conservation de deux mois en ce qui concerne l'audit de vérification;
- il faudrait ajouter un alinéa spécifique sur le verrouillage des données en vertu de l'article 15 du règlement 45/2001, conformément au point 3.8 du présent avis;
- il convient d'ajouter un alinéa sur le droit de saisir à tout moment le Contrôleur européen de la protection des données.

3.10 Mesures de sécurité

L'article 22 prévoit que le responsable du traitement met en oeuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à caractère personnel à protéger.

Compte tenu des risques potentiels engendrés par l'utilisation de badges contenant une puce RFID intégrée, le CEPD a procédé à un examen attentif des mesures de sécurité mises en oeuvre.
[...]

Au terme de cet examen, et tenant compte de la mise en oeuvre future des recommandations formulées ci-dessus, le CEPD juge ces mesures suffisantes par rapport aux dispositions de l'article 22 du règlement (CE) n° 45/2001.

Conclusion:

Il n'y a aucune raison de conclure à une violation des dispositions du règlement n° 45/2001, pour autant que les éléments figurant ci-après soient pris en compte dans leur intégralité:

- le CEPD juge excessive l'inclusion dans l'application Flexitime de membres du personnel qui ne l'utilisent pas, bien que travaillant à la DG INFSO; il recommande que cette dernière étudie les modalités et la fréquence des mises à jour de la base de données et informe le CEPD des résultats de cet examen;

- le CEPD demande que le responsable local de la sécurité de la DG INFSO ne conserve pas le(s) listage(s) dans le(s)quel(s) le nom des agents est associé au numéro "Flexitime" de la carte;

- en ce qui concerne la procédure de verrouillage prévue par la DG INFSO (par le biais d'une "photographie" des données via une impression, une copie de sauvegarde ou un CD Rom), le CEPD souhaiterait également qu'un troisième exemplaire soit mis à la disposition du contrôleur de la protection des données de la DG INFSO;

- le CEPD estime que la DG INFSO devrait mettre en œuvre les modifications ci-après au projet de déclaration de confidentialité:

    - supprimer le terme "registering" (enregistrement) dans le titre de la déclaration de confidentialité;
    - modifier la référence à l'avis du CEPD en remplaçant les termes "who delivered a favourable opinion" (qui a rendu un avis favorable) par "who delivered an opinion" (qui a rendu un avis); le CEPD souhaiterait également que la déclaration de confidentialité contienne un lien vers l'avis;
    - supprimer la phrase suivante: "*This is not related to any personal data*";
    - le CEPD souhaiterait que la catégorie de personnes susceptibles d'être destinataires des données (à savoir le délégué du responsable du traitement) soit également citée dans la déclaration de confidentialité, au même titre que le responsable du traitement des données et l'administrateur du système;

    - ajouter un alinéa précisant clairement les personnes ou catégories de personnes de la DG INFSO qui sont autorisées à utiliser l'application Flexitime (c'est-à-dire les membres du personnel concernés);
    - reformuler la déclaration spécifique de confidentialité à propos des informations qui peuvent être directement modifiées par la personne concernée et celles pour lesquelles elle doit s'adresser à l'administrateur du système pour en obtenir le changement;
    - suite à la recommandation du CEPD concernant l'exécution d'une troisième copie, il convient que le coordinateur de la protection des données de la DG INFSO figure lui aussi dans la déclaration de confidentialité du système;
    - mentionner le caractère obligatoire ou facultatif de la réponse aux questions ainsi que les conséquences pratiques d'un défaut de réponse, par exemple, les conséquences résultant de l'absence de pointage;
    - mentionner la base juridique en plus du Guide de l'horaire flexible;
    - indiquer la date limite (période de conservation) de deux mois en ce qui concerne l'audit de vérification;
    - ajouter un alinéa spécifique sur le verrouillage des données en vertu de l'article 15 du règlement 45/2001, conformément au point 3.8 de l'avis.

- ajouter un alinéa sur le droit de saisir à tout moment le Contrôleur européen de la protection des données.

En ce qui concerne les mesures de sécurité:

- le CEPD recommande que la DG INFSO établisse des règles spécifiques afin de préciser les personnes ayant un accès logique aux serveurs;

- le CEPD suggère que soient apportées des précisions sur les personnes auxquelles seront confiés les rôles de responsable du traitement des données, d'administrateur du système ou de délégué du responsable du traitement à travers l'adoption d'une liste des noms d'agents et que cette liste soit mise à disposition dans le bureau du contrôleur de la protection des données. Cette liste devrait, au minimum, définir les qualités de la personne responsable. En outre, le CEPD souhaite proposer que ces personnes soient au courant des questions ayant trait à la protection des données;

- le CEPD recommande que la DG INFSO réexamine sa décision au sujet des choix technologiques qu'elle a opérés, en procédant à une nouvelle évaluation comprenant un calendrier réaliste de mise en œuvre des changements de technologie, en prenant en considération le choix des meilleures techniques disponibles. Au cours de la période transitoire, les possibilités offertes par le choix de technologie actuel doivent être pleinement mises en œuvre, comme exposé au point 3.10 ci-dessus;

- le CEPD conseille, à tout le moins, de veiller à ce que le système utilise la distance de lecture minimale spécifiée par le fournisseur entre le lecteur et la puce et que celle-ci ne puisse pas être modifiée;

- le CEPD juge qu'il est important d'opérer, dans l'ECAS, une distinction entre les fonctions de l'application liées à l'agent lui-même et les fonctions de l'application liées à l'horaire flexible d'autres personnes subordonnées à l'agent qui possède des droits avancés. C'est pourquoi le CEPD serait partisan d'une solution imposant la mise en œuvre d'un système de double identification lors de l'accès à l'application.

Fait à Bruxelles, le 19 octobre 2007

(signé)

Joaquín BAYO DELGADO
Contrôleur européen adjoint de la protection des données

Suivi du 6 novembre 2007:

Le contrôleur européen de la protection des données se félicite de ce que l'Institution (DG INFSO) ait mis en œuvre, à propos des mesures de sécurité, une solution provisoire conforme aux termes de sa recommandation.