

## **Avis sur une notification en vue d'un contrôle préalable transmise par le délégué à la protection des données du Centre européen de prévention et de contrôle des maladies (ECDC) et relative à la "Gestion des présences et des absences"**

Bruxelles, le 22 juin 2009 (dossier 2009-0072)

### **1. Procédure**

Le 26 janvier 2009, le Contrôleur européen de la protection des données (ci-après dénommé "le CEPD") a reçu du délégué à la protection des données (ci-après dénommé "le DPD") du Centre européen de prévention et de contrôle des maladies (ci-après dénommé "l'ECDC") une notification en vue d'un contrôle préalable (ci-après dénommée "la notification") concernant le traitement de données relatif à la gestion des présences et des absences.

Le 9 février 2009, le CEPD a demandé un complément d'informations. Le 20 avril, l'ECDC lui a envoyé une deuxième notification destinée à remplacer la première et un complément d'informations.

Le 18 juin 2009, le CEPD a transmis au DPD le projet d'avis pour observations, lesquelles ont été reçues le 22 juin 2009.

### **2. Les faits**

Dans le cadre du statut des fonctionnaires des Communautés européennes (ci-après dénommé "le statut") et du régime applicable aux autres agents (ci-après dénommé "le régime"), ainsi que de la décision C(2004)1597 de la Commission introduisant des mesures d'exécution sur les absences et de la procédure interne de l'ECDC sur les heures de travail (ECDC/ADM/021) du 5 décembre 2007, la division des ressources humaines (RH) de l'ECDC (le "responsable du traitement") a instauré un traitement de données à la fois manuel et automatique afin de gérer les heures de présence et d'absence au travail du personnel de l'ECDC.

Depuis le 21 janvier 2008, le responsable du traitement a mis en œuvre un traitement automatique des données (SAP) afin de faciliter l'enregistrement et la gestion du temps du personnel travaillant à l'ECDC.

Le système SAP comprend deux applications principales: l'une est un portail "self-service" pour les employés, qui permet à ceux-ci d'alimenter la base de données avec leurs propres données; l'autre est un portail "self-service" pour les gestionnaires, accessible aux personnes autorisées qui, à l'ECDC, sont habilitées à gérer et approuver les présences et les absences du personnel.

La première application comporte les trois modules suivants:

- *recherche employé*: ce module permet au personnel de faire des recherches dans l'annuaire du personnel, qui donne des informations de base sur les agents et leur position dans l'ECDC;
- *informations personnelles*: le personnel y insère et modifie directement ses données à caractère personnel, comme les coordonnées et l'adresse en cas d'urgence;
- *horaires*: les agents enregistrent directement dans la base de données leurs horaires de travail et leurs absences (types d'absences prédéfinis), consultent l'état de leurs congés et introduisent des demandes concernant les absences et les horaires.

La deuxième application permet aux personnes autorisées (au sein des RH, des unités et de la hiérarchie) de consulter les horaires ainsi que les heures de présence ou d'absence du personnel, et d'approuver ou de refuser les demandes suivantes du personnel: congés annuels, congé temps flexible, congé spécial, réquisitions et compensations. En outre, la base de données du SAP permet aux personnes autorisées de produire des rapports réguliers, par personne et par unité, concernant: i) les congés pour maladie, ii) les heures de travail et les absences, iii) les droits aux congés et iv) les congés spéciaux, les congés de maternité, les congés pour convenance personnelle et toutes les autres formes d'absences prévues dans les règlements applicables. Ces informations sont également transférées sous forme électronique aux responsables des RH qui s'occupent de la boîte e-mail "présences".

Les rapports, produits sur une base individuelle, visent à s'assurer que l'employé ne dépasse pas le nombre de jours d'absence pour maladie sans fournir un certificat médical, à suivre les situations anormales et à contrôler les heures de travail des employés et des unités, le but étant d'éviter une surcharge de travail du personnel. L'ECDC a fait savoir au CEPD que les rapports ne servaient pas à évaluer la personne.

Le **traitement des données** effectué par les RH aux fins de la gestion des présences et des absences est en grande partie automatisé (utilisation du SAP), mais certaines de ses parties restent manuelles: en particulier, les documents justificatifs des absences et des congés sont généralement traités manuellement. De même, dans le cas de certains types particuliers de congés aussi, pour lesquels le personnel doit donner des informations supplémentaires, le traitement est manuel: horaire, mission, congé parental ou de maternité, congé pour raisons familiales, congé pour maladie et autres congés.

Les **personnes concernées** par le traitement des données effectué dans la base de données du SAP sont les membres du personnel de l'ECDC, à savoir des agents temporaires, des agents contractuels et des experts nationaux détachés. En outre, les données des stagiaires relatives aux absences et aux congés sont traitées manuellement par la division des RH. Certaines données relatives aux membres des familles du personnel peuvent aussi être collectées et traitées.

Les opérations de traitement, tant automatiques que manuelles, poursuivent les **finalités** suivantes: i) permettre au personnel de gérer son horaire dans le cadre de la politique de l'horaire flexible, ii) permettre à la direction d'approuver les heures de travail, les congés et les absences et iii) veiller à ce que les documents justificatifs soient fournis.

Les **catégories de données** suivantes sont traitées:

- dans le SAP: i) données personnelles, telles que nom, prénom, date de naissance, sexe, nationalité, adresse électronique, adresse privée, adresse en cas d'urgence, pays, téléphone, télécopieur, numéro personnel (d'identification), données sur les proches,

données sur les personnes à charge; ii) données sur l'horaire, les droits aux congés légaux et à l'horaire flexible, les absences, les congés et les raisons du congé;

- dans le dossier "présences" (dossier papier): nom, prénom, date de naissance, sexe, nationalité, adresse électronique, adresse privée, adresse en cas d'urgence, pays, téléphone, télécopieur, numéro personnel (d'identification), données sur les proches, données sur les personnes à charge, justifications des absences (par exemple, certificats médicaux), dépenses et remboursements médicaux, justifications de congés spéciaux (par exemple, contrat de location ou d'achat d'un bien immobilier, certificats de décès de proches, certificats de naissance d'enfants, certificats de mariage), demandes de modification de congés légaux (pour des raisons privées ou religieuses), informations sur les astreintes (afin d'assurer une compensation financière). Occasionnellement, des données relatives à la vie privée de la personne concernée (par exemple, son orientation sexuelle), à la paie et aux allocations, à la famille de la personne concernée ou à des missions et déplacements peuvent apparaître dans les documents fournis pour justifier un congé ou une absence;
- dans le "dossier personnel" (électronique et papier): nom, prénom, date de naissance, sexe, nationalité, adresse électronique, adresse privée, adresse en cas d'urgence, pays, téléphone, télécopieur, numéro personnel (d'identification), données sur les proches, données sur les personnes à charge, contrats de location ou d'achat d'un bien immobilier, certificats de naissance des enfants, certificats de mariage (pour déterminer les droits et les allocations).

Les données sont accessibles aux **destinataires** suivants de l'ECCD:

- pour tous les traitements de données (SAP, dossier présence et dossier individuel): le directeur des RH, un assistant RH, un assistant de réserve et le secrétaire des RH ont accès à toutes les informations sur les présences et les absences de l'ensemble du personnel. Les justificatifs de congés et d'absences (comme les certificats médicaux, de naissance, de mariage et autres justificatifs) ne sont traités que par la division des RH et ne sont communiqués à personne d'autre qu'aux RH;
- en outre, pour les données traitées dans le SAP uniquement:
  - le chef d'unité et un(e) secrétaire par unité nommé(e) par les RH sur demande du supérieur hiérarchique ont accès aux données traitées dans le SAP relatives à l'ensemble du personnel de leur unité;
  - chaque supérieur hiérarchique dispose des données sur les présences et les absences traitées dans le SAP pour chacun des membres de son équipe;
  - en outre, les secrétaires disposant d'un accès spécial au système SAP peuvent:
    - accéder aux informations sur les présences ou absences des membres de leur unité
    - produire des rapports sur:
      - les missions, congés de maladie, congés spéciaux, etc., par personne et par unité
      - les horaires présentés par le personnel
    - en tant que premier point de contact, aider le personnel en cas de problèmes avec l'enregistrement des horaires
    - aider le chef d'unité et les supérieurs hiérarchiques au niveau de l'approbation des congés.

Les personnes concernées peuvent contacter à tout moment le responsable du traitement, un assistant des RH, un assistant de réserve et un(e) secrétaire des RH pour exercer leurs **droits en termes d'accès, de rectification, de verrouillage, de suppression et d'opposition** sur des

informations de base sur leur identité. En outre, chaque membre du personnel a un accès personnel direct à ses propres données à caractère personnel stockées dans la base de données du SAP et peut corriger lui-même celles qui ont trait à ses coordonnées et la plupart de celles qui ont trait à ses heures de présence et d'absence. Les personnes concernées doivent néanmoins remplir une demande pour obtenir la correction des données suivantes: i) modification de congés légaux pour des raisons privées ou religieuses, ii) astreintes (les RH rassemblent les informations sur les heures d'astreintes et veillent à ce que les compensations financières dues soient payées).

En ce qui concerne les **informations sur le traitement des données**, l'ECDC a adopté une politique de protection des données à caractère personnel traitées dans le cadre de la gestion des présences et absences. En outre, une clause sur la protection des données a été insérée dans l'application "self-service" du SAP. Par ailleurs, au cours de la présentation faite aux nouveaux agents, ceux-ci sont informés de leurs droits et de la procédure à suivre pour accéder aux données les concernant et les rectifier.

En termes de **conservation des données**, il ressort de la notification que l'ECDC élabore actuellement un document sur la durée maximale de conservation des données, que le directeur du centre devrait adopter en 2009. Dans sa demande d'informations complémentaires, le CEPD a demandé qu'on lui en transmette le projet, mais cette demande est restée sans suite.

Pour ce qui est des **mesures de sécurité**, la notification précise que des copies sur support papier des documents et/ou des données sont transférées de la personne concernée aux RH dans une enveloppe fermée, par courriel ou déposées en mains propres aux RH, et qu'elles sont archivées dans une armoire protégée dans les locaux des RH. Toutes les données électroniques sont conservées dans le SAP. L'accès en est limité aux membres de l'équipe des RH chargés de la gestion des horaires, ainsi qu'au chef de la division administrative et au chef du service RH. Seuls les membres du personnel des RH peuvent avoir un accès physique et numérique aux dossiers individuels via des justificatifs du réseau de l'ECDC. Un code d'accès restreint aux systèmes informatiques est fourni. L'accès au SAP est adapté en fonction du profil de l'utilisateur.

### **3. Aspects juridiques**

#### **3.1 Contrôle préalable**

La gestion des présences et des absences par l'ECDC est un traitement qui rentre dans le champ d'application du règlement (CE) n° 45/2001 (ci-après dénommé "le règlement") parce qu'elle implique la collecte, l'enregistrement, la consultation et l'organisation de données à caractère personnel (article 2, point b) par un organe communautaire. Certaines parties du traitement sont automatisées (dans le SAP), d'autres étant manuelles; dans ce dernier cas, les données figurent dans un fichier (article 3, paragraphe 2). Le traitement porte notamment sur des données relatives à la santé, catégorie qualifiée de "particulière" et soumise à l'article 10 du règlement (voir le point 3.3 ci-dessous).

Selon l'article 27, paragraphe 1, du règlement, "*les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités sont soumis au contrôle préalable du CEPD*". Le paragraphe 2 énumère les traitements susceptibles de présenter de tels risques, et notamment celui de données relatives à la santé (point a) et celui de données destinées à évaluer des aspects de la personnalité des personnes concernées (point b).

Les traitements effectués dans le cadre de la gestion des absences et des présences présentent des risques particuliers en ce qu'ils impliquent de traiter des données révélant l'état de santé de la personne concernée (par exemple, les données sur le congé de maladie, les certificats médicaux).

Comme le traitement en cause implique le traitement régulier - et non occasionnel - de données relatives à la santé, il est nécessaire de procéder à un contrôle préalable au titre de l'article 27, paragraphe 2, point a), du règlement.

De plus, le traitement contribue largement à l'évaluation d'aspects de la personnalité des agents lorsqu'il faut décider s'il y a lieu d'accorder un congé ou un congé spécial. On peut de surcroît s'attendre à ce que les données recueillies dans le SAP soient utilisées aussi afin d'évaluer une personne soupçonnée de faute. Même si le traitement n'est pas destiné en lui-même à évaluer des aspects de la personnalité de la personne concernée tels que ses compétences, son rendement ou son comportement, il contribue largement à cette finalité, de sorte que l'article 27, paragraphe 2, point b), du règlement doit également être pris en compte comme fondement éventuel d'un contrôle préalable.

Comme le contrôle préalable est conçu pour s'appliquer à des situations susceptibles de présenter des risques particuliers, le CEPD devrait rendre son avis avant que le traitement ne commence. Dans le présent dossier, celui-ci a néanmoins déjà commencé. Mais cela ne pose pas vraiment de problème puisque les recommandations formulées par le CEPD peuvent encore être adoptées en conséquence.

La notification du DPD a été reçue le 26 janvier 2009. Une demande d'informations a suspendu le délai de deux mois dans lequel le CEPD doit rendre son avis. Une deuxième notification, remplaçant la première, a ensuite été envoyée au CEPD le 20 avril 2009, date à laquelle commence à courir le délai de deux mois, augmenté de trois jours de suspension pour la communication des observations. Le présent avis doit donc être rendu au plus tard le 24 juin 2009.

### **3.2 Licéité du traitement**

Des données à caractère personnel ne peuvent être traitées que si l'on trouve des fondements à cet effet dans l'article 5 du règlement, dont le point a) précise en particulier que "*le traitement (doit être) 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*".

Pour déterminer si les traitements sont visés par l'article 5, point a), il faut prendre en compte deux éléments: il s'agit de savoir premièrement si le traité ou un autre acte législatif prévoit une mission d'intérêt public, et deuxièmement si les traitements effectués par le responsable du traitement sont nécessaires à l'exécution de cette mission.

**Base juridique.** Le statut (et en particulier ses articles 55 à 61) et le régime (et en particulier ses articles 16, 17, 57 à 60 et 91) énoncent les règles concernant le temps de travail ainsi que les congés et les absences des fonctionnaires et autres agents. Dans le cadre de ces règles et de la décision C(2004)1597 de la Commission introduisant des règles d'exécution sur les congés, l'ECDC a adopté une procédure interne sur les heures de travail (ECDC/ADM/021), qui présente et définit les modalités du système d'horaire flexible et précise les règles relatives à l'horaire de travail ainsi qu'aux congés et absences applicables à l'ECDC. En outre, les règles sur les astreintes applicables à l'ECDC sont définies dans la décision n° 12/2007 du directeur de l'ECDC. Le statut, le régime, les règles d'exécution sur les congés et les décisions internes de l'ECDC offrent les bases juridiques justifiant le traitement des données du personnel travaillant à l'ECDC ayant pour finalité la gestion des présences et des absences.

Le CEPD insiste néanmoins sur le fait que, si le traitement est destiné à contrôler régulièrement le personnel pour évaluer certains aspects de la personnalité de la personne concernée comme ses compétences, son rendement ou son comportement, l'ECDC devrait adopter une base juridique particulière pour effectuer le traitement en vue de ces finalités. À cet égard, le CEPD fait observer que, si la base juridique autorise la production de rapports individuels dans le SAP à des fins de gestion des présences et absences, elle n'est pas suffisante pour autoriser l'utilisation de ces rapports individuels pour contrôler le personnel en vue d'évaluer ses compétences, son rendement ou son comportement.

**Critère de la nécessité.** Selon l'article 5, point a), du règlement, le traitement doit être "*nécessaire à l'exécution d'une mission*" telle que décrite plus haut. Le traitement de données mis en œuvre par l'ECDC est nécessaire pour veiller à ce que le Centre s'acquitte de ses obligations légales en tant qu'employeur et offre à son personnel tous les droits et avantages dans le domaine de l'emploi. Dès lors, le CEPD estime que le traitement de données satisfait au critère de la nécessité et peut être considéré comme licite au titre de l'article 5, point a), du règlement, à condition qu'il ne soit pas utilisé pour d'autres finalités que la gestion des présences et des absences.

### **3.3 Traitement portant sur des catégories particulières de données**

Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé ou à la vie sexuelle sont interdits, sauf dans les circonstances particulières définies à l'article 10, paragraphe 2 ou 3, du règlement.

Le traitement en cause peut porter sur des données médicales au sens strict ou sur des données relatives à la santé de la personne concernée en ce que les données révèlent des informations sur l'état de santé de la personne (absence pour raison de santé). En outre, les justificatifs d'un congé ou d'une absence peuvent aussi contenir des informations révélant les convictions religieuses ou la vie sexuelle de la personne. Il faut dès lors vérifier si l'article 10, paragraphe 2, contient des motifs justifiant le traitement des données.

Le point b) prévoit que des données sensibles peuvent être traitées si le traitement est nécessaire afin de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par les traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités. À cet égard, le CEPD insiste sur le fait que les données sensibles dont le traitement par l'ECDC rentre dans le champ dudit point b) ne peuvent être traitées qu'en vue des finalités légales pour lesquelles le traitement est effectué.

Le CEPD voudrait insister en outre sur la nécessité de fournir des garanties spécifiques: dans le cadre du traitement effectué par l'ECDC, le traitement de données relatives à la santé doit être strictement limité aux données indiquant l'état de maladie mais ne peut s'étendre à l'obtention d'informations confidentielles donnant un diagnostic médical sur la santé des personnes concernées. Il ajoute que, conformément à l'article 10, paragraphe 3, du règlement, le traitement des données médicales au sens strict doit être effectué uniquement par un praticien de la santé soumis au secret professionnel ou par une autre personne également soumise à une obligation de secret équivalente.

En ce qui concerne les autres données sensibles pouvant être collectées par l'ECDC, des garanties doivent être instaurées pour veiller à ce que ces informations ne soient pas utilisées à l'encontre de la personne concernée. Par exemple, les informations données à la personne concernée devraient clairement avertir cette dernière de la présence desdites données et de la finalité pour

laquelle elles seront utilisées. Il faut veiller à ce que les personnes ayant accès aux données ne les utilisent pour aucune autre finalité que celle à laquelle elles sont destinées.

### 3.4 Qualité des données

**Adéquation, pertinence et proportionnalité.** Selon l'article 4, paragraphe 1, point c), du règlement, 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*". Sur la base des informations dont il dispose, le CEPD estime que la collecte par la division RH des dépenses et remboursement médicaux dans le dossier "présences" n'est pas pertinente au regard de la finalité qu'est la gestion des présences et des absences.

**Loyauté et licéité.** Les données doivent également être "*traitées loyalement et licitement*" (article 4, paragraphe 1, point a), du règlement). La question de la licéité a déjà été analysée ci-dessus (point 3.2) et celle de la loyauté sera traitée dans le cadre du point 3.9, consacré aux informations à fournir aux personnes concernées.

**Exactitude.** Enfin, les données à caractère personnel doivent être "*exactes et, si nécessaire, mises à jour*" et "*toutes les mesures raisonnables sont prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées*" (article 4, paragraphe 1, point d), du règlement). Le fait que le personnel inscrive lui-même ses données dans SAP contribue à maintenir les données exactes et à jour. En outre, comme on le verra ci-dessous, au point 3.8, la personne concernée doit aussi avoir des droits d'accès et de rectification pour veiller à ce que les dossiers la concernant sont aussi complets que possible.

### 3.5 Conservation des données

Selon l'article 4, paragraphe 1, point e), du règlement, 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*". Les données peuvent être conservées au-delà de la période précitée à des fins historiques, statistiques ou scientifiques, mais soit sous une forme qui les rend anonymes, soit à condition que l'identité de la personne concernée soit cryptée.

L'ECDC n'a pas encore arrêté de durée maximale pour la conservation des données. Selon la notification transmise par le DPD, l'ECDC est en train d'élaborer une politique de limitation de la durée de conservation des données qui sera adoptée fin 2009.

Le CEPD souhaite insister sur la nécessité de fixer des périodes adéquates de conservation des données, dont la durée doit être évaluée sur la base des finalités pour lesquelles les données sont collectées et traitées. En l'espèce, il peut être nécessaire de définir différentes périodes de conservation en fonction du mode de traitement effectué, en se demandant combien de temps il serait nécessaire de conserver les données pour chacun de ces modes (sur SAP, sur d'autres fichiers électroniques, et sous format papier) afin de réaliser les finalités pour lesquelles elles ont été collectées. À cet égard, le CEPD souhaite être informé des périodes de conservation adoptées par l'ECDC.

### **3.6 Transfert des données**

Selon la notification, les données ne seront transférées qu'au sein de l'ECDC; il convient d'examiner ces transferts au regard de l'article 7 du règlement, qui 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*" (paragraphe 1) et que "*le destinataire traite les données à caractère personnel uniquement aux fins qui ont motivé leur transmission*" (paragraphe 3).

Sur la base des informations dont il dispose, le CEPD fait observer que les transferts ressortissent en principe de l'exécution légitime des missions relevant de la compétence des divers destinataires. Il observe en particulier que les transferts vers les supérieurs hiérarchiques des personnes concernées, les secrétariats et le personnel de RH sont nécessaires à des fins administratives et pour la gestion des absences et des congés. Par conséquent, l'article 7, paragraphe 1, du règlement est respecté.

Il ressort de la notification que les certificats médicaux ne sont traités que par le personnel des RH et ne sont communiqués à aucun autre destinataire. Or, le CEPD souhaite faire observer que, par principe, tous les certificats contenant des données médicales qu'il faut produire dans le cadre de demandes de congés ou d'absences doivent être déposés directement auprès d'un service médical et non de l'administration. Certes, l'on peut envisager une exception à cette règle dans les petites agences ou organes qui ne disposent pas d'un service médical, mais le CEPD recommande vivement que les certificats contenant des données médicales soient directement transférés par les personnes concernées à un service médical externe - de préférence dans les institutions et organes communautaires -, ce transfert devant avoir lieu conformément à l'article 7 du règlement. La division des RH ne doit dès lors ni traiter ni conserver de données médicales dans quelque dossier de gestion des présences et absences que ce soit. Il faut avertir clairement les personnes concernées qu'elles doivent envoyer leurs certificats médicaux au service médical externe désigné.

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

La base de données du SAP et les formulaires papier impliquent le traitement du numéro d'identification personnel. En soi, l'utilisation d'un identifiant est simplement un moyen - et, en l'espèce, un moyen légitime - facilitant le travail du responsable du traitement, même si elle peut entraîner des conséquences importantes. Selon l'article 10, paragraphe 6, du règlement, c'est le CEPD qui doit déterminer 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.

Comme le numéro unique d'identification n'est utilisé que pour des raisons administratives, le CEPD estime que son utilisation ne pose aucun risque justifiant l'adoption de garanties particulières en l'espèce.

### **3.8 Droits d'accès et de rectification**

L'article 13 du règlement établit un droit d'accès aux données sur demande de la personne concernée. L'article 14 confère à la personne concernée un droit de rectification.

Le personnel statutaire de l'ECDC, qui est tenu d'utiliser le SAP, a un accès direct à la plupart de ses données à caractère personnel figurant dans la base de données du SAP et peut les corriger directement (dans les trois mois), ce qui lui permet d'exercer effectivement ses droits.

En général, le personnel travaillant à l'ECDC peut exercer à tout moment son droit d'accès et de rectification en contactant par écrit le responsable du traitement. Le CEPD constate toutefois que la déclaration de confidentialité fournie par l'ECDC concernant la gestion des présences et des absences limite l'exercice du droit d'accès et de rectification, sur demande faite au responsable du traitement, aux "informations de base sur l'identité". Il insiste sur le fait que le droit d'accès et de rectification s'applique à toute donnée à caractère personnel traitée relative à la personne concernée, que le traitement ait lieu dans SAP ou dans tout autre dossier électronique ou papier.

Par ailleurs, les stagiaires devraient également jouir du droit d'accès et de rectification à propos de leurs données, traitées dans des dossiers papier.

Le CEPD constate en outre que les membres des familles dont les données sont transmises par un membre du personnel devraient aussi se voir octroyer le droit d'accéder à leurs données et de les rectifier, ce qui pourrait être fait en insérant dans la déclaration de confidentialité une note demandant au membre du personnel qui fournit, dans le cadre de la gestion des présences et des absences, les informations sur un tiers (membre de la famille ou autre) d'avertir ce dernier de ses droits d'accéder aux données le concernant et de les rectifier.

Le CEPD recommande dès lors de modifier la déclaration de confidentialité de manière à tenir compte de la recommandation qui précède.

### **3.9 Information de la personne concernée**

Afin de garantir la transparence du traitement des données à caractère personnel, les articles 11 et 12 du règlement énumèrent les informations qu'il y a lieu de fournir aux personnes concernées. L'article 11 prévoit que ces informations doivent être données au moment de la collecte des données lorsque celles-ci sont collectées auprès de la personne concernée; si elles l'ont été auprès d'une autre source, les informations doivent être données dès l'enregistrement des données ou lors de leur communication, sauf si la personne en est déjà informée (article 12).

En l'espèce, une déclaration de confidentialité est remise aux personnes travaillant à l'ECDC. Le CEPD suggère d'y apporter les modifications suivantes pour assurer le plein respect des articles 11 et 12 du règlement:

- les stagiaires et les membres des familles devraient être avertis du traitement de données les concernant. En ce qui concerne les membres des familles, ceci peut être fait en demandant aux membres du personnel d'informer les personnes dont ils communiquent des données du contenu de la déclaration de confidentialité;
- la déclaration doit indiquer clairement les périodes de conservation applicables;
- dans la partie intitulée "licéité du traitement et base juridique", on ne voit pas clairement la pertinence de la mention des "procédures de sélection sont nécessaires pour la gestion et le fonctionnement du centre" dans le cadre de la gestion des présences et des absences.

### 3.10 Mesures de sécurité

Selon l'article 22 du règlement, consacré à la sécurité du traitement, "*le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à caractère personnel à protéger*".

Se fondant sur les informations disponibles, le CEPD ne voit aucun élément lui laissant penser que l'ECDC n'aurait pas appliqué les mesures de sécurité requises à l'article 22 du règlement.

## 4. Conclusion

Rien ne permet de conclure à un manquement aux dispositions du règlement, sous réserve que les considérations figurant dans le présent avis soient pleinement prises en compte.

- Le traitement est licite pour autant qu'il soit limité à la finalité qu'est la gestion des présences et des absences; s'il est destiné à contrôler régulièrement le personnel et à évaluer des aspects de la personnalité de la personne concernée, tels que ses compétences, sa rentabilité ou son comportement, l'ECDC doit adopter une base juridique spécifique afin d'effectuer le traitement en vue de ces finalités. Il n'existe actuellement aucune base juridique justifiant la production de rapports individuels afin de contrôler le personnel en vue de l'évaluer.
- Des données sensibles dont le traitement par l'ECDC rentre dans le champ de l'article 10, paragraphe 2, point b), du règlement ne peuvent être traitées qu'en vue des finalités légales pour lesquelles le traitement est effectué. Le traitement de données relatives à la santé doit être strictement limité aux données indiquant le statut de malade mais ne peut s'étendre à l'obtention de données confidentielles apportant un diagnostic médical sur la santé des personnes concernées. En ce qui concerne le traitement d'autres données sensibles, des garanties doivent être instaurées pour veiller à ce que ces informations ne soient pas utilisées à l'encontre de la personne concernée (voir le point 3.3);
- La collecte par la division des RH des dépenses et remboursement médicaux dans le dossier "présences" n'est pas pertinente, au sens de l'article 4, paragraphe 1, point c), du règlement), au regard de la finalité qu'est la gestion des présences et absences.
- Le CEPD souhaite insister sur la nécessité de fixer des périodes adéquates de conservation des données, dont la durée doit être évaluée sur la base des finalités pour lesquelles les données sont collectées et traitées, en tenant dûment compte de tous les modes de traitement et de conservation utilisés.
- Les certificats contenant des données médicales doivent être directement transférés par les personnes concernées à un service médical externe - de préférence dans les institutions et organes communautaires -, ce transfert devant avoir lieu conformément à l'article 7 du règlement. La division des RH ne doit dès lors ni traiter ni conserver de données médicales dans quelque dossier de gestion des présences et absences que ce soit. Il faut avertir clairement les personnes concernées qu'elles doivent envoyer leurs certificats médicaux au service médical externe désigné.
- En ce qui concerne la qualité des données, il faut prendre toutes les mesures raisonnables permettant d'assurer que les données inexacts ou incomplètes soient supprimées ou corrigées. Le droit d'accès et de rectification doit être garanti à toute personne concernée,

y compris les stagiaires et les membres de la famille des agents dont les données sont communiquées, et ce pour toute donnée à caractère personnel traitée, quel que soit la forme dudit traitement.

- La déclaration de confidentialité doit être modifiée conformément aux recommandations figurant aux points 3.8 et 3.9 ci-dessus.

Fait à Bruxelles, le 22 juin 2009.

(signé)

Giovanni BUTTARELLI  
Contrôleur adjoint de la protection des données