CEPD NEWSLETTER

N° 12 - 20 Décembre 2007

Il est possible de souscrire un abonnement à la Newsletter du CEPD
sur notre site Internet:

www.edps.europa.eu

Sommaire:

1. Avis du CEPD sur le PNR européen

Le CEPD a adopté le 20 décembre 2007 un avis sur la proposition de Décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (*Passenger Name Record* - PNR) à des fins répressives. La proposition implique des obligations pour les transporteurs aériens de transmettre des données sur tous les passagers des vols à destination ou au départ d'un État membre de l'Union européenne.

L'avis se concentre sur l'impact déterminant de la proposition sur les questions relatives à la vie privée et à la protection des données des passagers aériens. Tout en reconnaissant que la lutte contre le terrorisme est un objectif légitime, le CEPD exprime de réelles préoccupations quant à la nécessité et la proportionnalité de la proposition qui, de son point de vue, ne sont pas suffisamment établies dans la proposition.
En outre, le CEPD adopte un regard critique sur le manque de clarté en ce qui concerne divers aspects de la proposition, en particulier le cadre juridique applicable, l'identité des destinataires des données à caractère personnel, et les conditions de transfert des données vers les pays tiers.

L'avis met l'accent sur quatre points clés et émet les conclusions suivantes:

- **légitimité du traitement**: la proposition ne fournit pas suffisamment d'éléments de justification pour appuyer et démontrer la légitimité du traitement des données;
- **cadre juridique applicable**: une absence significative de sécurité juridique est à relever quant au régime applicable aux différents acteurs impliqués dans le projet de décision;
- **identité des destinataires des données**: le projet de Décision ne prévoit aucune spécification concernant l'identité des destinataires des données à caractère personnel collectées par les compagnies aériennes;
- **transfert de données vers les pays tiers**: il est impératif que les conditions de transfert des données PNR vers des pays tiers soient cohérentes et soumises à un niveau de protection harmonisé.

Le CEPD recommande par ailleurs de ne pas adopter le projet de décision avant l'entrée en vigueur du nouveau Traité de Lisbonne, de sorte que la proposition puisse suivre la procédure de codécision prévue par le nouveau traité et que le Parlement européen soit pleinement impliqué dans le processus d'adoption.

☞ Avis du CEPD sur le PNR européen (pdf) (EN)

---

2. Avis du CEPD sur la RFID

Le Contrôleur européen de la protection des données (CEPD) a publié le 20 décembre 2007 son avis sur la communication de la Commission, adoptée en mars 2007, relative à l'identification par radiofréquence (RFID) en Europe.

L'avis porte sur l'utilisation croissante de puces RFID dans les produits de consommation et autres applications nouvelles qui affectent les individus.

Le CEPD accueille favorablement la communication de la Commission sur la RFID car elle aborde les principaux aspects découlant du déploiement de la technologie RFID, tout en tenant compte des questions relatives à la vie privée et la protection des données. Le CEPD partage l'avis de la Commission selon lequel il est approprié, dans un premier temps, de laisser la place aux instruments d'autorégulation. Toutefois, des mesures législatives supplémentaires peuvent être nécessaires afin de réglementer l'usage de la RFID en matière de respect de la vie privée et de protection des données.

Le CEPD exprime son soutien à l'application des principes d'"opt-in", de "privacy by design" (intégration des principes de protection des données dès la phase de conception des techniques) et à l'identification des "meilleures techniques disponibles". Il recommande également d'envisager l'adoption d'une législation communautaire permettant de réglementer les principales questions liées à l'utilisation de la RFID dans l'hypothèse d'une mise en œuvre défaillante du cadre juridique existant.

☞ Avis du CEPD sur le PNR européen (pdf) (EN)

---

3. Règles de mise en œuvre de l'Initiative Prüm - Avis du CEPD

Le 19 décembre, le CEPD a émis un avis sur l'initiative allemande visant à établir les règles de mise en œuvre nécessaires au fonctionnement de l'initiative Prüm du Conseil. Le CEPD avait déjà publié un avis (pdf) le 4 avril 2007 sur cette initiative relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière, en installant des mécanismes d'échange de données personnelles telles que les profils ADN et les empreintes digitales.

Les règles de mise en œuvre et leurs annexes revêtent une importance significative dans la mesure où elles définissent les aspects déterminants et les outils pour les échanges de données qui sont essentiels pour fournir des garanties aux personnes concernées. En outre, ces règles doivent bénéficier d'une attention particulière vu le contexte actuel marqué par l'absence d'un cadre général au niveau de l'UE permettant de garantir une harmonisation de la protection des données dans le domaine policier et judiciaire.

L'avis du CEPD recommande en particulier que :

- la combinaison de dispositions générales et de règles spécifiques à la protection des données doit assurer non seulement les droits des citoyens mais aussi l'efficacité des autorités répressives lorsque la proposition sera mise en œuvre;
- l'exactitude dans les recherches et les comparaisons des profils ADN et des empreintes digitales devraient être dûment prise en compte et

contrôlée en permanence, et également en gardant à l'esprit qu'il s'agit d'échanges à grande échelle;
- les autorités de protection des données concernées devraient être en position de mener à bien leur rôle de supervision et de conseil à tous les stades de la mise en œuvre.

☞ Avis du CEPD sur les règles de mise en œuvre de l'initiative Prüm (pdf) (EN)

---

4. Arrêt du Tribunal de première instance dans l'affaire Bavarian Lager vs. Commission (T-194/04)

Le 8 novembre 2007, le Tribunal de première instance (TPI) a rendu un arrêt dans une affaire mettant en jeu deux droits fondamentaux: le droit d'accès aux documents de l'Union européenne et le droit à la protection des données. Cet arrêt marque une étape importante dans le débat sur l'équilibre entre ces droits.

Le TPI a annulé la décision de la Commission européenne de refuser l'accès au compte-rendu d'une réunion organisée par l'institution qui mentionnait le nom des participants. Le TPI a statué que la communication des noms des représentants d'un organe collectif ne mettait pas la protection de leur vie privée et de leur intégrité en danger.

Le CEPD est intervenu dans cette affaire en soutenant la demande d'accès du requérant et a défendu une position qui, en substance, a été confirmée par le TPI.

La Commission doit maintenant décider s'il y a lieu d'aller en appel auprès de la Cour de justice.

☞ Affaire T-194/04: Bavarian Lager v. Commission

---

5. Le CEPD souhaite intervenir dans le recours contre EPSO concernant l'accès aux documents relatifs aux concours (T-374/07)

Le CEPD a demandé à ce qu'il lui soit permis d'intervenir dans une affaire portée devant le Tribunal de première instance et concernant l'accès à des documents établis dans le cadre d'un concours EPSO (Office européen de sélection du personnel).

Le requérant dans cette affaire a participé à un concours visant à recruter des administrateurs juristes-linguistes de langue grecque. Le candidat avait demandé une copie des épreuves qu'il avait passées ainsi que des réponses correctes. Cette demande a cependant été refusée par EPSO.

La question de l'accès des candidats aux résultats de leurs épreuves et documents connexes dans le cadre d'un concours EPSO a déjà fait l'objet de plusieurs contrôles préalables menés par le CEPD.

☞ Affaire T-374/07: Pachitis vs. Commission des Communautés européennes et EPSO (pdf)

---

6. Publication de l'inventaire du CEPD pour 2008 (consultation législative)

Le second inventaire public du CEPD en tant qu'autorité consultative sur les propositions de législation sur les questions de protection des données et documents connexes a été publié sur le site Internet du CEPD.

Cet inventaire fait partie du cycle de travail annuel du Contrôleur. Une fois par an, le CEPD fait état, a posteriori, de ses activités dans un Rapport annuel. En outre, le CEPD publie un inventaire de son programme de travail pour l'année suivante dans le domaine de sa mission de consultation.

L'inventaire se base essentiellement sur le programme de travail de la Commission pour 2008 (pdf). Il se compose d'une partie introductive qui comprend les priorités pour le CEPD pour 2008, ainsi que d'une annexe des propositions de la Commission et autres documents nécessitant l'attention du contrôleur.

Parmi ses priorités pour 2008, le CEPD examinera notamment les conséquences de l'entrée en vigueur du Traité de Lisbonne dans le domaine de la protection des données.

☞ Inventaire 2008 du CEPD (EN)

---

7. Rapport du CEPD sur l'audit de sécurité du système EURODAC

En sa qualité d'autorité chargée d'assurer le contrôle de l'unité centrale d'EURODAC, le CEPD a lancé une inspection étendue du système EURODAC qui a été finalisée en mars 2006. Cet exercice a donné lieu à la décision d'entreprendre un audit de sécurité approfondi dont les résultats ont été présentés à la Commission européenne le 9 novembre 2007.

Les mesures de sécurité initialement mises en œuvre concernant le système EURODAC et la gestion de celles-ci ont fourni jusqu'à présent un niveau adéquat de protection. Cependant, certains éléments des systèmes et la sécurité des aspects organisationnels présentent des faiblesses qui devront être traitées afin qu'EURODAC puisse pleinement respecter les meilleures pratiques et l'application des meilleures techniques disponibles.

Le CEPD examinera la mise en œuvre appropriée des mesures de suivi qui seront adoptées sur la base du présent rapport.

Bien que le rapport soit classifié "Restreint UE", un bref résumé (pdf) (EN) est disponible sur le site du CEPD.

---

8. Le CEPD publie des observations sur le contrôle de l'utilisation d'Internet par les employés

En réponse à une consultation de la Cour des comptes européenne, le CEPD a rendu ses observations le 26 novembre 2007 à propos du projet de la Cour en ce qui concerne sa politique en matière de sécurité de l'Internet. Selon l'article 28(1) du Règlement (EC) 45/2001 (pdf) le CEPD doit en effet être informé des mesures administratives relatives au traitement de données à caractère personnel qu'il doit ensuite commenter.

Les observations du CEPD sont de plusieurs ordres. Il insiste d'abord sur l'importance de la transparence et souligne le devoir pour la Cour d'utiliser tous les moyens disponibles, en ligne ou non, pour communiquer et sensibiliser les employés à la politique en matière de sécurité de l'Internet. A propos du consentement des employés utilisé pour légitimer le contrôle de l'Internet, le CEPD exprime de sérieux doutes quant au choix - réel et librement consenti - dont ceux-ci ont pu disposer sur le fait d'accepter le contrôle de leur utilisation d'Internet.

En ce qui concerne l'utilisation d'Internet à des fins privées, le CEPD considère qu'une politique de tolérance zéro n'est ni praticable, ni réaliste. Le CEPD est favorable à l'établissement de limites claires, telles que l'allocation de plages horaires permettant d'utiliser Internet à des fins privées, par exemple entre midi et 14 heures, et avant 8 heures et après 18 heures.

De plus, le CEPD marque sa préférence pour l'utilisation de logiciels de filtrage qui impliquent une approche préventive sur l'utilisation abusive d'Internet, plutôt qu'une démarche basée sur la détection des abus.

En ce qui concerne les conditions de contrôle de l'utilisation d'Internet, le Contrôleur souscrit à l'établissement de limites claires qui garantissent que le contrôle est effectué seulement lorsqu'il est absolument nécessaire et mené à des fins précises. Le CEPD appuie des mesures telles que des contrôles sporadiques plutôt que des contrôles permanents, ainsi que le contrôle du volume du trafic par département plutôt que par individu. Il recommande également d'établir des limites de conservation des fichiers-journaux (pour un maximum de six mois).

☞ Observations du CEPD sur la politique en matière de sécurité de l'Internet à la Cour des comptes européennes (pdf) (EN)

---

9. Contrôles préalables de traitements de données personnelles

Le traitement des données à caractère personnel par l'administration de l'UE susceptible de présenter des risques particuliers pour les personnes concernées fait l'objet d'un contrôle préalable de la part du CEPD. Cette procédure permet de déterminer si le traitement est conforme ou non au règlement (CE) 45/2001 qui établit les obligations des institutions et organes européens en matière de protection des données.

9.1 "Data pool de l'information et du renseignement" de l'OLAF et bases de données de "renseignement"

Le “Data pool de l'information et du renseignement" représente toutes les données retenues au sein des attributions de l'Unité renseignement opérationnel (C4) de l'OLAF comprenant les bases de données de renseignement.

L'Information opérationnelle et l'utilisation du renseignement sont deux aspects essentiels du mandat de l'OLAF pour lutter contre la fraude, la corruption, n'importe quelle autre activité illégale portant atteinte aux intérêts financiers de la Communauté européenne ainsi que contre des problèmes sérieux liés à l'exécution des obligations professionnelles - ainsi qu'établi par l'article premier du règlement (CE) n° 1073/1999 (pdf) et l'article 2.5 de la décision de la Commission CE/1999/352 (pdf).

La finalité du traitement analysé est de favoriser l'exploitation du renseignement d'une part, et les activités opérationnelles de l'OLAF d'autre part. L'Unité C4 apporte aussi son appui dans le cadre d'affaires spécifiques, d'opérations et d'enquêtes, en vue d'assurer l'exactitude et la pertinence de l'information reçue, disséminée et traitée à des fins de renseignement mais aussi à des fins financières, administratives, disciplinaires et judiciaires. Ce soutien peut être fourni à différentes étapes des enquêtes de l'OLAF et des activités opérationnelles, et cela dans tous les secteurs. Si nécessaire, ces données sont enregistrées au sein du CMS (*Case Management System*).

Dans son avis du 21 novembre 2007 (pdf) (EN), le CEPD recommande notamment:

- d'indiquer dans le dossier "renseignement" lorsqu' une restriction fondée sur l'article 20 est appliquée;
- de respecter la confidentialité de l'identité du dénonciateur durant les activités de renseignement de l'OLAF, et ce jusqu'aux derniers stades si nécessaire;
- de fournir l'information (article 12 du règlement) aux personnes concernées dont les noms apparaissent dans la documentation sous analyse et qui ne sont ni les personnes incriminées, ni les témoins, ni les dénonciateurs et informateurs, à moins que cela soit impossible ou que cela implique des efforts disproportionnés. Dans ce cas seulement, l'obligation de fournir directement l'information peut être remplacée par

une disposition indirecte: une déclaration de confidentialité publiée sur le site internet de l'OLAF. Le même principe devrait être appliqué lorsque des activités de renseignement sont conduites indépendamment à une enquête.

- de publier sur le site internet de l'OLAF des avis d'information personnalisés aux individus (à moins que cela ne soit impossible ou ne requiert un effort disproportionné). Le CEPD appelle dès lors à l'OLAF à élaborer des pratiques basées sur l'octroi d'informations personnalisées aux individus concernés lorsque cela s'avère approprié dans le contexte des activités de renseignement. Le CEPD a demandé à l'OLAF de le tenir informé quant à ces mesures à prendre.

☞ Avis du CEPD (EN)

9.2 Flexitime - spécifique à la DG INFSO

Le 19 octobre 2007, le CEPD a adopté un avis sur "la mise en œuvre de l'horaire flexible spécifique à la DG INFSO".

Dans le cadre général de la gestion du temps de travail régi par le module Time management "SYSPER 2", la DG INFSO a ajouté à l'application de l'horaire flexible un élément supplémentaire important résidant dans l'ajout d'une puce RFID intégrée au badge du personnel en vue du pointage à l'entrée et à la sortie. L'inclusion d'une telle technologie dans un système d'horaires flexibles renforce les risques spécifiques déjà présents dans ce type de système. Par conséquent, le CEPD a considéré le dossier en tant que tel soumis à contrôle préalable.

Dans son analyse, le CEPD conclut que le système traite de données personnelles, car les données se rapportent à des personnes physiques qui sont identifiables, par exemple par l'utilisation de noms et de numéros d'identification. En outre, le CEPD a analysé de près l'application au système du test de nécessité. A ce sujet, il est d'avis que le développement d'un système de badges utilisant la technologie RFID pour mettre en œuvre un système d'horaires flexibles ne constitue pas un besoin spécifique, car le même objectif (gestion du temps de travail) peut être atteint par d'autres moyens moins intrusifs.

Cependant, le CEPD a également accepté qu'une marge d'appréciation soit laissée à la discrétion de l'administration dans sa décision de mettre en œuvre ce système en utilisant la technologie RFID. Si les mesures de protection et de proportionnalité sont respectées, on peut dès lors considérer qu'un tel système remplit les conditions de nécessité.

Dans ses conclusions, le CEPD demande d'apporter des modifications au système envisagé en ce qui concerne les aspects liés à la sécurité et, dans l'attente de ces mesures, autorise une solution provisoire. Les autres recommandations ont trait à l'élaboration d'une déclaration de confidentialité,

à des mesures organisationnelles et aux catégories de personnes concernées.

☞ Avis du CEPD sur la mise en œuvre du flexitime - spécifique à la DG INFSO (pdf) (EN)

---

10. Journée de la protection des données: 28 janvier 2008

Les Etats membres du Conseil de l'Europe et les institutions européennes célèbreront le 28 janvier 2008 la seconde édition de la Journée européenne de la protection des données. L'événement commémore l'adoption de la Convention 108 du Conseil de l'Europe qui constitue le premier instrument légalement contraignant au niveau international dans le domaine de la protection des données.

Le site Internet du Conseil de l'Europe propose une page spécifique dédiée à cet événement à partir de laquelle vous pouvez accéder – via la liste des drapeaux nationaux – aux différentes initiatives qui ont été ou seront menées à travers les pays européens pour célébrer la Journée de la protection des données.

Cette journée sera l'occasion pour le CEPD d'attirer l'attention des députés européens et du personnel des institutions européennes sur leurs droits et leurs obligations en matière de protection des données. A cette fin, un stand d'information sera mis en place dans les bâtiments du Parlement européen, de la Commission et du Conseil.

Le CEPD y présentera ses attributions liées à ses missions de supervision, de consultation et de coordination, ainsi que ses activités et travaux en cours. Différents outils de communication et de matériaux multimédia seront utilisés comme support d'information. Un quiz portant sur la thématique de la protection des données dans les institutions et organes européens sera proposé sur place aux visiteurs. Celui-ci pourra également être téléchargé à partir du site Internet du CEPD.

☞ **Informations pratiques:**

- Parlement européen: 28 janvier 2008 ; 11.00 - 15.00
  Bâtiment ASP, rez-de-chaussée, "main street"
- Conseil: 29 janvier ; 11.00 - 15.00
  Bâtiment Justus Lipsius
- Commission européenne: 30 janvier ; 11.00 - 15.00
  Bâtiment Berlaymont, hall d'entrée principal

---

11. Nouveaux délégués à la protection des données

Chaque institution ou organe européen doit nommer au moins une personne en tant que Délégué à la protection des données (DPD). La tâche de ces délégués est d'assurer de manière indépendante la mise en œuvre en interne du règlement 45/2001.

Nominations récentes

- Terry TAYLOR, Agence européenne pour la sécurité et la santé au travail (EU-OSHA);
- Jobst NEUSS, Fonds européen d'investissement (FEI);
- Arthur BECKAND, Agence européenne pour la sécurité aérienne (EASA);
- Martin DISCHENDORFER, Agence européenne pour la reconstruction (EAR).

☞ Liste complète des DPDs.

---

12. Colophon

Cette lettre d'information est publiée par le Contrôleur européen de la protection des données, une autorité européenne indépendante, créée en 2004 pour:

- contrôler le traitement des données personnelles dans les administrations de l'UE;
- conseiller sur la législation en matière de protection des données;
- coopérer avec les autorités similaires afin de garantir la cohérence en matière de protection des données.

Adresse postale:
EDPS - CEPD
Rue Wiertz 60 - MO 63
B-1047 Bruxelles
Belgique

Bureaux:
Rue Montoyer 63
Bruxelles
BELGIQUE

Coordonnées:
Tél: +32 (0)2 283 19 00
Fax: +32 (0)2 283 19 50

Courriel: edps@edps.europa.eu

CEPD - Le gardien européen de la protection des données personnelles
www.edps.europa.eu