



NEWSLETTER

Nr. 8 - 28 février 2006

Il est possible de [souscrire un abonnement](#) à la Newsletter du CEPD sur notre site Internet.

www.edps.europa.eu

Table des matières:

1. [L'affaire SWIFT](#)
2. Décision Europol - [l'avis du CEPD](#)
3. [Contrôles préalables](#) de traitements de données personnelles
4. [Plainte](#) à propos du droit d'accès
5. [Nouveau site internet](#) du CEPD
6. [Journée de la Protection des Données](#) : Le CEPD veut sensibiliser le personnel de l'UE
7. Séminaire sur la [protection des données dans les organisations internationales](#)
8. [Discours & articles](#)
9. Nouveaux [délégués à la protection des données](#)
10. [Colophon](#)

1. L'affaire SWIFT

Le 1er février, le Contrôleur européen de la protection des données (CEPD) a publié un avis sur le rôle de la Banque centrale européenne (BCE) dans l'affaire SWIFT (où des autorités américaines accèdent aux données

bancaires dans le cadre de la lutte contre le terrorisme). L'avis se concentre sur le rôle de la BCE en tant que "overseer", utilisateur et décideur.

- En tant que participante au groupe des banques centrales qui contrôlent les activités de SWIFT, la BCE peut exercer une pression morale. Bien que non contraignante, cette pression pourrait aussi être utilisée afin de prévenir toute violation de la protection des données qui pourrait entraver la stabilité financière et pour s'assurer que les autorités compétentes soient informées à temps.
- La BCE assume également des responsabilités vis à vis de ses propres clients dans la manière dont SWIFT traite les données de ceux-ci. Agir en tant que coresponsable de traitement signifie que la BCE doit garantir pour ses "clients" la totale conformité aux règles de protection des données. Le CEPD invite la BCE à préparer, avant la fin d'avril, un rapport sur les mesures prises pour se conformer à son avis.
- En tant que décideur de la mise au point de systèmes de paiement européens, la BCE doit s'assurer que l'architecture de ces systèmes ne permette pas que des informations sur tous les paiements européens soient transférées à des autorités dans des pays tiers en violation de la législation sur la protection des données.

Le 14 février, le Parlement européen a adopté une [résolution](#) conjointe sur "PNR" et SWIFT. En ce qui concerne SWIFT, le Parlement européen avalise l'avis du CEPD et appelle la BCE et d'autres institutions concernées à garantir que les systèmes de paiement européens soient totalement conformes à la législation européenne de la protection des données. Les autorités nationales de protection des données surveillent l'état d'avancement et coordonnent leurs actions dans cette affaire par l'intermédiaire du Groupe Article 29, qui a adopté un [avis](#) le 22 novembre 2006. Lors de la dernière [session plénière](#), le Groupe a décidé d'envoyer une lettre aux institutions européennes. Cette lettre rappelle que toute solution dans cette affaire - et en particulier tout accord international qui pourrait être négocié - devra se conformer aux principes européens de la protection des données.

Lire l'[avis](#) (en anglais), ou le [communiqué de presse](#).

2. Décision Europol - l'avis du CEPD

Le 16 février, le CEPD a publié un avis sur la proposition de décision du Conseil concernant Europol. Même si la proposition contient des dispositions très avancées en termes de protection des données, le CEPD recommande différentes améliorations indispensables afin de faire face à l'augmentation de l'utilisation des données personnelles par Europol. La garantie doit être donnée que les échanges avec les autres organes européens, tels OLAF, seront basés sur un niveau cohérent de protection des données et sur une coopération efficace dans le contrôle.

L'objectif de la proposition de décision du Conseil est de donner à Europol une nouvelle base légale plus flexible. Cependant, cela va entraîner des changements importants dans le mandat d'Europol, notamment en termes d'échanges de données. De plus, des efforts vont être entrepris pour assurer l'interopérabilité avec les bases de données nationales et européennes. Ceci appelle à une amélioration de la protection des données, et le CEPD recommande :

- d'assurer que les données recueillies provenant d'activités commerciales soient correctes;
- de mettre en œuvre des conditions strictes et des garanties lorsque des bases de données sont étroitement liées;
- d'harmoniser les règles et de limiter les exceptions relatives au droit d'accès de la personne concernée;
- d'incorporer des garanties pour assurer l'indépendance du délégué à la protection des données d'Europol (qui assure, de façon interne, le traitement légitime des données personnelles).

Quand Europol fera partie de la structure européenne, le rôle opérationnel du CEPD sera de contrôler le traitement des données personnelles du personnel et les transferts de données des institutions et organes européens vers Europol.

Lire l'[avis](#) (en anglais), ou le [communiqué de presse](#).

3. 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 certaines personnes (les personnes concernées) fait l'objet d'un contrôle préalable de la part du CEPD. Cette procédure sert à 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.

Usage des téléphones de bureau - Banque centrale européenne

Cet avis est le premier dossier en matière de monitoring de l'utilisation des téléphones de bureau par le personnel. La banque centrale européenne a établi une procédure d'investigation sur l'utilisation des téléphones de bureau qui peut être mise en œuvre lorsqu'il y a un désaccord avec le contenu de la liste d'appels privés ou un désaccord dans le contenu des statistiques liées aux appels professionnels.

De façon générale, le CEPD a estimé que la procédure était en accord avec les principes contenus dans le règlement en matière de protection des données. Cependant, il a émis quelques recommandations notamment en matière de conservation des données et de l'information sur le traitement des données personnelles à inclure dans la circulaire administrative y afférente. Cette dernière est d'ores et déjà en cours de modification et reflètera les recommandations du CEPD.

Système d'alerte précoce - Commission européenne

Le Système d'alerte précoce (SAP) assure principalement la circulation d'information confidentielle relative à des parties-tiers (personne physique ou légale) parmi les différents départements de la Commission. Ces informations concernent les bénéficiaires de fonds communautaires qui ont commis des fraudes, des erreurs administratives ou des irrégularités, ainsi que les bénéficiaires représentant une menace pour les intérêts financiers de la Communauté européenne. Ces informations peuvent aussi concerner des personnes physiques ayant des pouvoirs de représentation, d'action ou de contrôle sur des personnes légales.

La Commission a suivi de façon substantielle le Règlement. Néanmoins le CEPD a émis quelques recommandations notamment sur :

- la possibilité de publier la décision SAP au Journal officiel pour des raisons de transparence,
- la qualité des données (par exemple, toute rectification de données incomplètes ou inexactes doit être reflétée dans le SAP),
- le droit ne peut être restreint qu'à titre d'exception et il doit être complété par un droit de rectification dans le cas d'erreurs ou de fausse évaluation,
- à titre de règle générale, la personne concernée doit être informée de l'existence d'une alerte à son encontre.

Les autres institutions n'ont pas établi leur propre base de données, mais utilisent celle de la Commission. Dans ce cadre, le CEPD a reçu une notification de la Cour de Justice sur son utilisation du SAP. Dans son avis, le CEPD a souligné l'importance des principes et droits énoncés ci-dessus.

En relation avec ces deux dossiers, le CEPD a émis un [avis](#) sur les propositions de modifications du règlement financier et de ses modalités d'exécution. Ces amendements :

1. introduisent une publication des listes des bénéficiaires de fonds communautaires,
2. adaptent le règlement à la pratique actuelle d'un unique SAP contrôlé par la Commission,
3. et étendent aux Etats membres et pays tiers la possibilité de recevoir et envoyer ces informations.

Le CEPD a souligné l'importance d'une approche proactive compte tenu du principe de transparence. Il a aussi également proposé la mise en œuvre de sécurités pour l'établissement d'une base de données centrale de candidats et soumissionnaires. Enfin, il a suggéré des modifications sur les durées de conservation et sur les contrôles budgétaires, afin d'être en accord avec le règlement 45/2001 au regard de la conservation des données de trafic.

Maintien des prestations en cas d'insuffisance professionnelle - Cour des Comptes

La Cour des Comptes a arrêté un projet de décision relative à la procédure pour identifier, gérer et remédier aux cas d'insuffisance professionnelle parmi le personnel de l'institution à la suite du rapport d'évaluation annuel. Parce qu'il s'agit d'évaluer des aspects de la personnalité des personnes concernées, notamment leur compétence, leur rendement ou leur comportement, ce traitement est soumis au contrôle préalable du CEPD. Les principales recommandations concernent l'information à fournir aux membres du personnel ainsi que les délais de conservation des données.

Ces recommandations seront mises en place par la publication de la décision avec ses annexes faisant référence aux dispositions du règlement et ce dernier sera respecté par l'insertion dans la décision proposée d'une période de conservation en conformité avec l'article 4.1.e du règlement.

Les avis publiés sont accessibles sur le [site internet](#) du CEPD.

4. Plainte à propos du droit d'accès

Le CEPD a traité plusieurs plaintes au sujet de la restriction du droit d'accès à des documents contenant les données personnelles d'une personne concernée (Article 20 du Règlement). Dans un cas récent à propos de harcèlement au travail, le plaignant voulait avoir un accès au rapport établi suite au présumé harcèlement et mauvais management. Au début, cette demande fut refusée avec la motivation qu'il n'était pas considéré comme 'personne concernée'. Un accès très limité au rapport lui fut ensuite accordé.

Après enquête, le CEPD a affirmé que toute restriction au droit d'accès d'une personne concernée à ses données personnelles devait être interprétée de manière stricte. Le CEPD a demandé que de plus grandes parties du rapport soient mises à la disposition du plaignant, notamment tous les résultats de l'enquête qui le concernent. De plus, le CEPD a admis que certaines limites soient nécessaires dans le but de protéger les droits d'autres personnes (p.ex. des témoins, la personne qui fait l'objet d'une enquête). Toutefois, le CEPD n'a approuvé aucune restriction basée sur la protection de l'enquêteur. Le fait de savoir au préalable qu'il est possible qu'un rapport soit divulgué est une garantie de rigueur et d'impartialité de la procédure, et n'est pas un obstacle à ce que l'enquêteur remplisse dûment son rôle.

5. Nouveau site internet du CEPD

A la fin du mois de janvier, le CEPD a lancé son site internet de deuxième génération. L'objectif est de mieux communiquer au sujet de la protection des données et des activités du CEPD et d'ainsi d'augmenter le nombre de visiteurs et d'améliorer leur navigation sur le site web.

La première version du site fut développée durant la phase initiale de mise en place du Secrétariat du CEPD, en été 2004. Après trois ans d'activités, il a paru nécessaire de construire une nouvelle structure de site internet permettant la publication de documents sur base des trois tâches principales du CEPD - la supervision, la consultation et la coopération. Un chapitre général intitulé "Le CEPD" a également été introduit. Par rapport à l'ancienne version, le nouveau site internet contient de nouveaux niveaux d'information, comme par exemple les résumés des avis, ou des introductions décrivant certaines tâches particulières du CEPD.

La version française du site est également disponible depuis peu. De nouveaux contenus seront ajoutés graduellement.

6. Journée de la protection des données: Le CEPD veut sensibiliser le personnel de l'UE

Les états membres du Conseil de l'Europe ont célébré pour la première fois le 28 janvier 2007 la journée de la protection des données. Cette date correspond à l'anniversaire de l'ouverture à la signature en 1981 du premier instrument international juridique contraignant dans le domaine de la protection des données - la Convention 108 du Conseil de l'Europe.

Le CEPD a soutenu cette initiative et a mis l'accent sur la sensibilisation du personnel de l'UE aux droits et obligations de la protection des données. Le CEPD a donc installé un stand d'information pendant un jour à l'intérieur du Parlement Européen puis à l'intérieur de la Commission européenne. Un [quiz](#) a été proposé au personnel des institutions.

7. Séminaire sur la protection des données dans les organisations internationales

En 2005, le CEPD était le principal organisateur d'un séminaire intitulé "la protection des données dans le cadre de la bonne gouvernance". Un séminaire de suivi aura lieu à Munich le 29 mars. Il abordera des thèmes spécifiques aux organisations internationales, qui ne sont généralement pas soumises aux législations nationales. Quelques places sont encore disponibles. Les personnes intéressées qui travaillent au sein d'une organisation internationale devraient dès lors contacter le CEPD dès que possible.

[Pour en savoir plus.](#)

8. Discours & articles

Protection des données - les normes actuelles de coopération policière sont-elles satisfaisantes ?

En décembre 2006, Peter Hustinx (CEPD) a participé à un séminaire public sur la coopération policière européenne au Parlement Européen. Mr Hustinx a souligné les points essentiels de ses deux avis sur la proposition de décision-cadre pour la protection des données dans le troisième pilier.

Premièrement, le CEPD a montré que les normes actuelles étaient inadéquates, puisque qu'il n'y a pas de cadre légal commun pour l'échange d'informations entre états membres. Deuxièmement, il affirme que les normes communes figurant dans la proposition de décision nécessitent une large portée. Elles doivent être applicables à tout traitement et ne pas limiter la protection aux seules données échangées entre les états membres, en excluant toutefois les traitements purement "domestiques". Troisièmement, Mr Hustinx a souligné le besoin de cohérence avec la directive 95/46 et a expliqué pourquoi cela serait approprié pour le travail de la police, bien que cette directive soit un instrument du premier pilier. Enfin, il a insisté sur le fait que le développement de normes adéquates dans la protection des données devrait être considéré comme une condition préalable pour une meilleure coopération et non une source de problèmes.

Le CEPD: Les Institutions des CE contrôlées par une autorité indépendante

Cet article, publié dans la "Common Market Law Review" et écrite par un membre du personnel du CEPD décrit le CEPD comme un nouveau phénomène dans le cadre institutionnel des Communautés.

Après quelques remarques introductives sur l'article 286 du traité des CE, la mission générale du CEPD et ses 3 principales activités sont précisées. L'article continue par une analyse détaillée du rôle du CEPD par la définition de ce que le CEPD n'est pas (différence avec les autres institutions et agences), par la présentation des raisons principales de sa création et les conditions d'exercice de ses fonctions, etc. De plus, il est expliqué sous quelles circonstances exceptionnelles le CEPD peut être sujet à un contrôle politique et judiciaire.

Dans ses dernières observations, l'article résume les caractéristiques essentielles du CEPD, à savoir donner un visage à la protection des données et assumer une indépendance, une expertise et un pouvoir approprié. En conclusion, il est souligné que ces caractéristiques offrent, sous différentes perspectives, plusieurs avantages au système de l'Union Européenne.

Le troisième pilier en pratique: composer avec les faiblesses - l'échange d'informations entre les Etats membres

En novembre 2006, un membre du personnel du CEPD a présenté ce document de réflexion à une réunion de l'Association Néerlandaise de Droit Européen.

En vue du Programme de La Haye (renforcer la liberté, la sécurité et la justice dans l'Union Européenne) et en dépit de l'absence d'un traité constitutionnel, un espace européen de justice criminelle doit être établi. Le document tente de donner une direction sur la façon dont l'UE peut faire renaître les aspirations énoncées dans le programme de La Haye, notamment en matière de coopération policière et judiciaire dans les affaires criminelles.

Quelques uns des aspects traités dans le document sont les suivants : le partage d'information présuppose une confiance mutuelle entre les Etats Membres. Les articles 29 à 32 du Traité de l'UE confèrent des pouvoirs généraux pour légiférer dans le but d'améliorer une telle confiance. En faisant cela, la plus grande attention doit être portée aux faiblesses du troisième pilier, comme le manque d'examen approfondi (démocratique) et de protection légale. De plus, suite au [jugement PNR](#), il reste une zone d'ombre entre le premier et le troisième pilier dans laquelle l'Union européenne n'a pas de pouvoir d'agir. Ces aspects et d'autres sont abordés dans ce document.

Voyez la section [Discours & articles](#) du site internet.

9. 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 :

- Hubert MONET, Agence exécutive "Education, audiovisuel et culture" (EACEA)
- Giuseppina LAURITANO, Contrôleur européen de la protection des données
- Martin BENISCH (succédant à M. Sommerfeld), Banque centrale européenne
- Andreas MITRAKAS, Agence européenne chargée de la sécurité des réseaux et de l'information - ENISA
- Jean-Marie ADJAH, Observatoire européen des phénomènes racistes et xénophobes
- Maria ARSENE (remplace temporairement Mme Candelier), Comité des Régions

La liste complète des DPDs est disponible [ici](#).

10. Colophon

Cette Newsletter 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 de la 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