



## CONSULTATION

> Révision du mandat de l'Agence FRONTEX: le CEPD appelle à des règles claires sur la protection des données .....	2
> Avis du CEPD sur les abus sexuels concernant des enfants et la pédopornographie .....	3
> Avis du CEPD sur l'initiative citoyenne européenne .....	4
> Avis du CEPD sur les déchets d'équipements électriques et électroniques .....	5
> Avis du CEPD sur la vie privée à l'ère numérique .....	6
> Contribution du CEPD aux négociations sur l'accord avec les Etats-Unis dans le domaine policier et judiciaire .....	7
> Nouvel inventaire de consultations législatives du CEPD .....	7



## SUPERVISION

> Contrôles préalables de traitements de données personnelles .....	8
> Lignes directrices du CEPD .....	10
> Consultations sur les mesures administratives .....	12



## EVENEMENTS

>> Troisième atelier sur la protection des données dans les organisations internationales (Florence, 27-28 mai 2010) .....	14
>> Conférence bisannuelle sur la protection des données et l'application des lois (Trèves, 31 mai - 1er Juin 2010) .....	14
>> Transparence et protection des données personnelles: éléments complémentaires ou conflictuels de la bonne gouvernance? (Maastricht, 3-4 juin 2010) .....	14
>> Conférence de clôture du CSEE sur le cyber-harcèlement (Bratislava, 7-8 juin 2010) .....	15
>> Premier débat de la table ronde européenne de la sécurité sur le <i>cloud computing</i> (Bruxelles, 8 juin 2010) .....	15
>> La Conférence sur le Traité de Lisbonne - Evaluation de l'impact sur la législation et la politique du Royaume-Uni (Londres, 15 juin 2010) .....	16
>> Conférence européenne des commissaires à la protection des données (Prague, 29-30 avril 2010) .....	16
>> CEPD - Réunion des délégués à la protection des données (Bruxelles, 19 mars 2010) .....	17
>> Case Handling Workshop (Bruxelles, 18-19 mars 2010) .....	17



## DISCOURS ET PUBLICATIONS

### - Highlight -

## Réforme du cadre juridique européen de la protection des données: le CEPD demande à la Commission européenne d'être ambitieuse dans son approche

Dans un discours prononcé le 29 avril 2010 lors de la conférence des commissaires à la protection des données et de la vie privée d'Europe à Prague, le CEPD, Peter Hustinx, a insisté sur la nécessité d'être proactif dans le cadre des discussions en cours sur l'avenir du cadre juridique communautaire pour la protection des données. Le CEPD a demandé à la Commission européenne de rester ambitieuse dans la mise à jour du cadre existant afin d'éviter que la protection des données ne perde de sa pertinence et de son efficacité dans une société de plus en plus influencée par les changements technologiques et la mondialisation.

**“ L'enjeu n'est ni plus ni moins que celui de garantir la vie privée et la protection des données dans une société de l'information hautement développée en 2015, 2020 et au-delà. Une approche ambitieuse est la seule manière dont nous pouvons nous assurer que notre vie privée et nos données personnelles sont bien protégées, également dans l'avenir. Il est essentiel que la Commission fasse des propositions qui tiennent compte de ce qui est vraiment nécessaire et ne se contente pas de résultats moins ambitieux. ”**

**Peter Hustinx, CEPD**

Dans son discours, Peter Hustinx a insisté sur les conditions essentielles d'un cadre juridique efficace pour protéger les données personnelles dans l'UE. Cela inclut la nécessité d'un cadre juridique global visant à assurer une plus grande efficacité, ainsi que les éléments suivants:

- l'intégration des principes de "**privacy by design**" et "**privacy by default**" dans les technologies de l'information et de la communication;
- une **plus grande responsabilité pour les responsables du traitement**: les responsables du traitement doivent être rendus davantage responsables du respect des règles de protection des données dans la pratique. Cela apporterait une valeur ajoutée significative dans la mise en œuvre effective de la protection des données et aiderait considérablement les autorités de protection des données dans leurs tâches de supervision et d'exécution;
- des **pouvoirs d'exécution plus forts pour les autorités de protection des données**: il est essentiel que les autorités de protection des données disposent de ressources suffisantes pour exercer leurs tâches de surveillance et, si nécessaire, faire respecter les règles de protection des données.

☞ Discours de Peter Hustinx (EN) ([pdf](#))



## CONSULTATION

### > Révision du mandat de l'Agence FRONTEX: le CEPD appelle à des règles claires sur la protection des données



L'avis du CEPD, adopté le 17 mai 2010, porte sur la proposition de la Commission européenne visant à renforcer les capacités opérationnelles de l'Agence européenne pour la coopération aux frontières extérieures de l'Union européenne, FRONTEX. L'avis met l'accent sur le développement des tâches de l'Agence, telles que prévues par la proposition, et leurs conséquences pour la protection des données personnelles.

Selon le CEPD, il est frappant que la proposition reste quasiment silencieuse sur le traitement des données personnelles par l'Agence FRONTEX, d'autant plus que le cadre juridique selon lequel l'Agence devra fonctionner est profondément remanié. Le CEPD exprime ses préoccupations sur le fait que la proposition ne précise pas dans quelle mesure FRONTEX serait

autorisée à traiter des données personnelles et, si tel était le cas, dans quelles circonstances et conditions et selon quelles restrictions.

**“ Il est essentiel de fixer des règles claires en matière de protection des données et apporter des éclaircissements sur les conditions et les circonstances dans lesquelles le traitement des données par l'agence FRONTEX pourrait avoir lieu. ”**  
**Peter Hustinx, CEPD**

Le CEPD estime que la proposition de règlement devrait aborder clairement la question du **champ d'activités** pouvant donner lieu à un traitement de données personnelles par FRONTEX.

Une **base juridique** spécifique, fondée sur des garanties solides en matière de protection des données et en conformité avec les principes de proportionnalité et de nécessité, est essentielle. Un traitement de données personnelles ne devrait être autorisé que si celui-ci est nécessaire pour des motifs légitimes et clairement identifiés.

La réticence de la Commission à préciser cette base juridique dans le règlement proposé, ou à indiquer clairement la date à laquelle elle entend le faire, suscite de sérieuses préoccupations. Selon le CEPD, une telle approche est susceptible de conduire à une **incertitude juridique** et entraîner un **risque important de non-respect** des règles et garanties de protection des données. Le Contrôleur insiste donc pour que le Conseil et le Parlement apportent davantage de clarté à cet égard.

➤ Avis du CEPD (EN) ([pdf](#))

## > Avis du CEPD sur les abus sexuels concernant des enfants et la pédopornographie



Le 10 mai 2010, le CEPD adopté un avis sur une proposition de directive de la Commission visant à lutter contre l'exploitation et les abus sexuels d'enfants et la pédopornographie.

L'objectif de la proposition est d'améliorer la lutte contre la violence envers les enfants selon différents aspects, notamment la criminalisation des formes graves de maltraitance d'enfants en ce qui concerne par exemple pour le tourisme sexuel impliquant des enfants, l'enquête pénale et la coordination des poursuites, les nouvelles infractions criminelles dans l'environnement

informatique, la protection des victimes et la prévention des infractions. En ce qui concerne l'objectif de prévenir les infractions, l'un des outils mis en place serait la restriction de l'accès à la pornographie infantile sur Internet.

Dans son avis, le CEPD ne remet pas en question la nécessité de mettre en place un meilleur cadre prévoyant des mesures adéquates pour protéger les enfants contre les abus. Il insiste néanmoins sur l'impact de certaines de ces mesures, notamment le blocage de sites web et la mise en place de permanences téléphoniques, sur les droits fondamentaux à la vie privée et à la protection des données des personnes concernées. La question n'est pas spécifique à la lutte contre la violence

faite aux enfants mais à toute initiative visant à la **collaboration du secteur privé à des fins de répression**.

**Le CEPD a dans de précédents avis exprimé ses préoccupations concernant la surveillance des individus par le secteur privé (fournisseurs de services Internet (FSI) ou titulaires du droit d'auteur), dans des domaines qui relèvent en principe de la compétence des autorités policières et judiciaires.**

Dans son avis, le CEPD insiste en particulier sur la nécessité de garantir la sécurité juridique en ce qui concerne toutes les parties concernées, y compris les FSI, les victimes et les personnes utilisant le réseau. Bien que la proposition mentionne la nécessité de prendre en compte les droits fondamentaux des utilisateurs finaux, le CEPD estime que ceci devrait être complété par une obligation pour les États membres à veiller à la mise en place de procédures harmonisées, claires et détaillées dans le cadre de la lutte contre les contenus illicites, et ce sous la supervision d'autorités publiques indépendantes.

☞ Avis du CEPD (EN) ([pdf](#))

## > Avis du CEPD sur l'initiative citoyenne européenne



L'initiative citoyenne européenne est l'une des innovations introduites par le traité de Lisbonne. Elle permet à des citoyens, au nombre d'un million au moins, qui sont ressortissants d'un nombre significatif d'États membres, de présenter une proposition législative sur des questions présentant un intérêt pour eux. La collecte d'au moins un million de déclarations de soutien implique la collecte de données à caractère personnel. Dans son avis du 21 avril 2010, le CEPD a souligné que le plein respect des règles de protection des données contribuera grandement à la fiabilité, à la force et au succès de ce nouvel instrument.

Une proposition de règlement, adoptée le 31 mars 2010, détermine les modalités et conditions requises pour l'initiative citoyenne. De manière générale, le CEPD est **satisfait** de la façon dont les aspects de protection des données de l'initiative ont été abordés, mais il considère que des améliorations peuvent encore être apportées.

L'une des recommandations du CEPD concerne l'obligation pour l'organisateur d'une initiative ayant l'intention d'utiliser un système de collecte en ligne de demander une certification de sécurité de ce système à l'autorité compétente. Le CEPD suggère par ailleurs d'obliger l'organisateur de le faire *avant* qu'il ne commence la collecte des déclarations de soutien.



Une autre recommandation concerne le **principe de limitation des finalités**. Le CEPD suggère que le législateur s'assure que les données personnelles recueillies par l'organisateur ne soient pas utilisées à des fins autres que le soutien de l'initiative citoyenne en question et de s'assurer que les données reçues par l'autorité compétente sont uniquement utilisées dans le but de vérifier

l'authenticité des déclarations de soutien.

☞ Avis du CEPD (EN) ([pdf](#))

## > Avis du CEPD sur les déchets d'équipements électriques et électroniques

L'avis, publié le 15 avril 2010, Hier, porte sur la proposition de la Commission européenne visant à réviser la directive relative aux déchets d'équipements électriques et électroniques (DEEE ou "e-déchets"), une proposition faisant l'objet de discussions approfondies au sein du Parlement européen et du Conseil, mais sans prendre en compte les implications en matière de protection des données.

Tout en soutenant l'objectif de la proposition visant à améliorer les politiques respectueuses de l'environnement dans le domaine des e-déchets, le CEPD souligne que l'initiative ne porte que sur les risques environnementaux liés à l'élimination des DEEE et ne prend pas en compte les risques de protection des données qui peuvent survenir suite à une élimination, une réutilisation ou un recyclage inappropriés. Ces risques existent en particulier lorsque les données personnelles relatives aux utilisateurs des appareils et/ou appartenant à des tiers restent stockées dans des équipements informatiques et de télécommunications (ordinateurs personnels et ordinateurs portables, par exemple) au moment de leur destruction.

Compte tenu de ces risques, le CEPD souligne l'importance d'adopter des **mesures de sécurité** appropriées à chaque étape du traitement des données à caractère personnel, y compris pendant la phase de destruction des appareils contenant des données personnelles. Le principe du "**privacy by design**" ou, dans ce domaine précis, de "security by design", devrait également être inclus dans la proposition afin de s'assurer que des garanties en matière de vie privée et de sécurité soient intégrées par défaut dans la conception des équipements électriques et électroniques.

**“ Il est important de prendre en compte les effets potentiellement dommageables de la destruction des DEEE sur la protection des données personnelles stockées dans les équipements utilisés. Le respect des mesures de sécurité et une approche basée sur le "privacy by design" devraient être considérés comme des conditions préalables primordiales afin de garantir de manière efficace le droit à la protection des données. ”** Peter Hustinx, CEPD

Rappelant que la phase de destruction de DEEE contenant des données personnelles entre dans le champ d'application de la directive 95/46/CE sur la protection des données, le CEPD recommande que le législateur:



- intègre "par défaut" la vie privée et la protection des données dans la conception des équipements électriques et électroniques afin de permettre aux utilisateurs de supprimer - de manière simple et gratuite - les données personnelles pouvant se trouver dans les appareils dans le cas où ceux-ci devraient être détruits;

- interdit la commercialisation d'appareils utilisés qui n'ont pas fait l'objet de mesures de sécurité appropriées, en conformité avec les normes techniques les plus avancées, afin d'effacer toutes les données personnelles qu'ils contiennent.

☞ Avis du CEPD (EN) ([pdf](#))

## > Avis du CEPD sur la vie privée à l'ère numérique

L'avis du CEPD intitulé "Promouvoir la confiance dans la société de l'information en encourageant la protection des données et la vie privée" a été adopté le 18 mars 2010 et tant que contribution au nouvel Agenda numérique européen. L'avis examine les mesures que l'Union européenne pourrait adopter ou promouvoir afin de garantir le droit à la vie privée et à la protection des données lors de l'utilisation des technologies de l'information et de la communication (TIC). L'identification par radiofréquence (RFID), les réseaux sociaux, la santé en ligne, et les systèmes de transport intelligents ne sont que quelques exemples.

L'avis souligne que **la confiance est une question essentielle** dans l'émergence et le succès du déploiement des TIC. Ces technologies offrent des opportunités et des avantages considérables, mais elles comportent aussi des **risques nouveaux**. Veiller à ce que l'utilisation des TIC ne compromette pas les droits fondamentaux à la vie privée et à la protection des données est un facteur clé pour garantir la confiance des utilisateurs dans la société de l'information.

Bien que l'UE dispose d'un cadre réglementaire solide dans le domaine de la protection des données, dans de nombreux cas les TIC suscitent de nouvelles inquiétudes qui ne sont pas prises en compte dans le cadre existant. **Il est donc nécessaire d'aller plus loin** afin de renforcer ce cadre. Selon le CEPD, cette action supplémentaire passe par la nécessité de garantir le **principe du "Privacy by design"** selon lequel les TIC sont conçues et développées en tenant compte de la vie privée et des exigences de protection des données depuis la création même de la technologie, et ce à tous les stades de son développement.



**“ Les avantages potentiels des TIC ne peuvent être appréciés dans la pratique que s'ils sont capables de susciter la confiance. Cette confiance ne sera obtenue que si les TIC sont fiables, sûrs, sous le contrôle des individus et si la protection de leurs données personnelles et la confidentialité est garantie. ”**

**Peter Hustinx, CEPD**

Afin de renforcer le cadre juridique européen de la protection des données européennes, le CEPD demande à la Commission européenne de suivre le plan d'action suivant:

- **approche générale basée sur le "privacy by design"**: la prise en compte du respect de la vie privée dès la conception doit être explicitement incluse en tant que principe général obligatoire dans le cadre juridique existant de la protection des données. Cela permettrait de rendre obligatoire sa mise en œuvre par les responsables du traitement des données, ainsi que par les concepteurs et fabricants de TIC, tout en offrant une plus grande légitimité aux autorités judiciaires et policières pour exiger son application effective. Le principe du "Privacy by design" doit également faire partie intégrante du prochain Agenda numérique européen et devenir contraignant dans les futures politiques de l'UE;

- **"privacy by design" dans des secteurs spécifiques:** dans trois domaines présentant des risques spécifiques pour la vie privée et la protection des données, le CEPD recommande la prise en compte du respect de la vie privée dès la conception selon l'approche suivante: a) **RFID:** proposer des mesures législatives réglementant les principaux enjeux de l'usage de la RFID dans l'hypothèse où l'autorégulation ne fournit pas les résultats escomptés (p.ex. prévoir le principe du consentement préalable - "opt-in" - au point de vente); b) **Réseaux sociaux:** envisager une législation qui requiert des paramètres de protection de la vie privée par défaut ; c) **Paramètres du navigateur et publicité ciblée:** envisager une législation qui obligerait de fournir aux navigateurs des paramètres de confidentialité par défaut afin de faciliter l'obtention du consentement des utilisateurs pour recevoir de la publicité;
- mettre en œuvre le **principe de responsabilité** dans la directive européenne sur la protection des données et commencer le travail en vue de l'adoption des **mesures d'application des dispositions relatives aux failles de sécurité** dans la directive "vie privée et communications électroniques", et les appliquer de manière générale à tous les responsables de traitement de données.

☞ Avis du CEPD (EN) ([pdf](#))

## > Contribution du CEPD aux négociations sur l'accord avec les Etats-Unis dans le domaine policier et judiciaire



Le CEPD contribue actuellement aux discussions concernant l'élaboration d'un accord sur la protection des données entre l'Europe et les Etats-Unis. Cet accord fournirait des garanties élevées pour les échanges de données à caractère personnel dans le domaine de la coopération policière et judiciaire en matière pénale. Depuis 2007, le CEPD a suivi de près les travaux du "Groupe de Contact de Haut Niveau" (High Level Contact Group) incluant des représentants européens et américains, et il a activement contribué aux différentes phases du travail préparatoire.

Il a adopté un avis sur le sujet déjà en novembre 2008 ([pdf](#)), et il a pris part à la réunion et à la consultation publique organisées par la Commission. Alors qu'un mandat de négociation est aujourd'hui en cours de préparation, le CEPD soutient l'inclusion dans ce projet d'exigences essentielles en matière de protection des données, telles qu'une finalité et un champ d'application clairs, des dispositions concernant la mise en œuvre des droits des personnes concernées et une supervision indépendante.

## > Nouvel inventaire de consultations législatives du CEPD

Dans quelques jours, le quatrième inventaire public du CEPD en tant que conseiller sur les propositions de législation de l'UE et les documents connexes sera publié sur son site Internet. En raison de la publication du programme de travail 2010 de la Commission et du plan d'action de Stockholm - respectivement en mars et avril 2010, l'inventaire du CEPD est publié plus tard que d'habitude, à savoir en mai au lieu de décembre.

L'inventaire fait partie du cycle de travail annuel du CEPD. Une fois par an, le CEPD rend compte *a posteriori* de ses activités dans le rapport annuel. En outre, le CEPD publie un inventaire de ses intentions dans le domaine de la consultation pour l'année suivante. L'inventaire est accompagné d'un document qui liste les développements que le CEPD entend suivre en priorité. Pour 2010, ces développements couvrent le nouveau cadre juridique pour la protection des données, des propositions relatives au traitement des données et à l'échange dans le domaine de la coopération policière et judiciaire, y compris les accords avec les pays tiers sur les transferts de données, et les initiatives prises dans le cadre de l'Agenda numérique européen.

☞ [Inventaire du CEPD](#)



## SUPERVISION

### > Contrôles préalables de traitements de données personnelles

Une opération de traitement de données personnelles par l'administration européenne qui est susceptible de présenter des risques particuliers pour les personnes concernées doit faire l'objet d'un contrôle préalable par le CEPD. Cette procédure permet de déterminer si le traitement est conforme au règlement (CE) No 45/2001 qui établit les obligations des institutions et organes communautaires en matière de protection des données.

### >> Collecte de noms et de certaines données pertinentes des rapatriés pour des opérations de retour conjointes - FRONTEX

Le 26 avril 2010, le CEPD a adopté un avis sur le traitement des données à caractère personnel par FRONTEX en ce qui concerne la «Collecte de noms et de certaines autres données pertinentes des rapatriés pour les opérations de retour conjointes».

Le but du traitement est la préparation et la réalisation d'opérations de retour conjointes assistées par FRONTEX en vertu du règlement FRONTEX (CE) n° 2007/2004 en vue:

- d'avoir une connaissance exacte du nombre et de l'identification des rapatriés prenant part à l'opération de retour;
- de fournir aux compagnies aériennes une liste des passagers;
- de connaître les risques liés aux rapatriés pour la sécurité de l'opération de retour;
- de connaître l'état de santé des rapatriés afin d'assurer une assistance médicale appropriée au cours de l'opération de retour;
- de savoir si des mineurs sont concernés par l'opération de retour.

FRONTEX a informé le CEPD que des données personnelles n'ont pas été traitées pour les activités opérationnelles à ce jour, mais que cette activité de traitement serait nécessaire dans un avenir proche: 1) pour mieux remplir et développer la tâche de l'agence dans le cadre des opérations de retour conjointes; 2) pour aider une organisation MS/SAC (Etat membre/Pays associé Schengen) dans la compilation des listes de passagers et leur mise à jour au cours de la préparation de l'opération de retour conjointe sur la base des informations reçues des États participants; 3) pour suivre en continu les Etats participants qui ont (ou n'ont pas) fourni les données nécessaires à l'Etat organisant l'opération de retour qui demande régulièrement à l'agence FRONTEX de contacter ces



Etats pour fournir les données en temps utile; 4) pour améliorer l'assistance offerte par FRONTEX dans l'organisation des opérations de retour conjointes.

Le CEPD a accordé une **attention particulière** à la **base juridique du traitement**. Le CEPD comprend que certains traitements de données personnelles peuvent être nécessaires pour la bonne exécution de la tâche de l'Agence dans le cadre de l'opération de retour conjointe; dans ce cas, l'agence devrait être considérée comme le responsable du traitement. Il estime cependant comme préférable, sinon nécessaire, d'avoir une base juridique plus spécifique que l'article 9 ("la coopération de retour") du règlement FRONTEX, en raison de la sensibilité des données et des activités concernées pour une population vulnérable.

Le CEPD estime donc que l'article 9 du règlement FRONTEX et l'article 5 (a) du règlement de protection des données 45/2001 ("licéité du traitement") ne peuvent que servir de base juridique provisoire pour l'activité de traitement envisagée, sous réserve d'un examen attentif de la nécessité d'une base juridique plus spécifique.

Le CEPD a également demandé que FRONTEX mette en œuvre les procédures nécessaires pour garantir les droits des personnes concernées et l'obligation d'informer avant la réalisation du traitement. En outre, le CEPD a demandé à l'agence FRONTEX de l'informer sur les mesures de mise en œuvre prises à cet égard.

☞ Avis du CEPD (EN) ([pdf](#))

## >> École administrative européenne - auto inventaire de perception BELBIN - Commission européenne



L'objectif du traitement est de permettre à des participants aux cours de formation de l'École administrative européenne (EAE) d'obtenir des réactions sous forme de rapport au sujet de leur rôle préféré dans une équipe. Les données ne doivent pas être utilisées pour une quelconque forme d'évaluation de la personne concernée.

Le CEPD s'est concentré sur deux aspects:

- les relations entre le responsable du traitement, le sous traitant et le sous contractant:** même si l'EAE n'a pas accès aux données traitées par le sous-contractant, ce dernier doit agir selon les instructions données par l'EAE au sous-traitant. L'EAE est le responsable du traitement des données de cette activité de traitement parce qu'elle détermine les finalités et les moyens (l'utilisation de l'outil basé sur le WEB). Les trois contractants responsables de dispenser les cours de formation pour l'EAE, ainsi que le sous-contractant responsable de l'auto évaluation basée sur le WEB (l'auto inventaire de perception BELBIN), doivent être tous considérés comme sous traitants des données à caractère personnel agissant au nom de l'EAE. Le sous-traitant n'est pas autorisé à agir au-delà de ce qu'est déterminé par l'EAE et spécifié dans le contrat entre le sous-traitant et le contractant conformément au contrat entre l'EAE et le contractant.
- la nature anonyme des données:** le rapport donné aux participants ne peut pas être considéré comme "anonyme" parce que le sous-traitant peut relier les réponses aux personnes concernées puisque les participants utilisent généralement une adresse de courrier électronique qui indique leurs nom et prénom.



Le CEPD a émis des recommandations concernant ces deux aspects, en particulier que le contrat entre le sous-traitant et le sous contractant devrait comprendre les clauses sur tous les articles obligatoires, notamment au regard de **la confidentialité et de la sécurité du traitement**. L'EAE doit être également informée par le sous-traitant lorsqu'il a fourni l'accès à et rectifié des données. Enfin, le choix des sous-contractants directs ou indirects du sous-traitant devrait être soumis à l'approbation de l'EAE.

☞ Avis du CEPD (EN) ([pdf](#))

## >> Système d'alerte précoce et de réaction ("EWRS") et recherche des contacts - Commission européenne

Le système d'alerte précoce et de réaction ("EWRS") est un **outil de communication** utilisé par la Commission, le Centre européen de prévention et de contrôle des maladies ("CEPCM") et les Etats membres pour **l'échange d'informations pour la prévention des maladies transmissibles** - telles que la tuberculose, la rougeole, le SRAS, le virus H1N1 et d'autres - pour permettre une action transfrontalière. Le EWRS est utilisé, entre autres, pour la "**recherche des contacts**". La recherche des contacts est une procédure utilisée pour identifier et atteindre les personnes qui ont pu entrer en contact avec une personne infectée. Une fois les contacts recherchés, ils peuvent être diagnostiqués et soignés. La recherche des contacts revêt également un intérêt général de santé publique car elle permet de réduire ou d'empêcher la propagation de la maladie.

Dans ses recommandations, le CEPD a souligné la nécessité **de déterminer plus clairement les rôles, les tâches et les responsabilités** des parties impliquées dans l'exploitation et l'utilisation du système, en particulier, le rôle de la Commission et du CEPCM. Les responsables du traitement et les sous-traitants doivent être clairement désignés d'une manière qui corresponde au rôle effectif ainsi qu'au statut juridique des organisations concernées. Il convient de préciser les responsabilités de chacun et la manière dont les personnes concernées peuvent exercer leurs droits. À court terme, **l'adoption d'un ensemble de lignes directrices de protection des données** pour l'EWRS est recommandée. La Commission est également encouragée à promouvoir une **révision du cadre juridique** pour assurer une base juridique plus sûre et une répartition claire des responsabilités.

Le CEPD a également souligné la nécessité d'appliquer le principe de **prise en compte de la vie privée dès la conception**, et d'intégrer la protection des données à la formation offerte aux utilisateurs. Un mécanisme clair doit être fourni aux personnes concernées pour exercer leur **droit d'accès**. Enfin, pour assurer la cohérence et la transparence, l'exploitant de l'EWRS devrait délivrer des **informations complètes et conviviales** aux personnes concernées sur son site Internet. Ceci devrait être complété par un avis fourni par les points de contact des Etats membres, conformément aux lois nationales sur la protection des données.

☞ Avis du CEPD ([pdf](#))

## > Lignes directrices du CEPD

Le CEPD publie des lignes directrices sur des thèmes spécifiques en vue de fournir des conseils aux institutions et organes européens dans des domaines importants tels que le recrutement, le traitement des données disciplinaires, et la vidéosurveillance. Ces recommandations ont également facilité le contrôle préalable par le CEPD des opérations de traitement des données dans les agences de l'UE. Elles ont servi de document de référence sur lequel les agences ont pu se baser pour évaluer leurs propres pratiques.

## >> Lignes directrices du CEPD sur les enquêtes administratives et les procédures disciplinaires

Le 23 avril 2010, le CEPD a publié des lignes directrices concernant le traitement des données à caractère personnel dans les enquêtes administratives et les procédures disciplinaires menées par les institutions et organes européens. Ces lignes directrices font partie de l'approche thématique horizontale du CEPD en vue d'**harmoniser les bonnes pratiques** dans les institutions, agences et organes européens, et de faciliter le respect des dispositions du règlement sur la protection des données (45/2001).

Les lignes directrices présentent les résultats des positions et recommandations du CEPD concernant chaque principe fondamental, tels qu'ils ont été analysés dans les avis de contrôle préalable sur les opérations de traitement effectuées par la plupart des institutions et organes européens. Le CEPD souligne par ailleurs la nécessité de procéder à une **réflexion plus approfondie sur la question spécifique de l'interception des communications**, avec un accent particulier sur la base juridique de la mise sur écoute des communications vocales et la possibilité de le faire sans mandat ou autorisation judiciaire.

Conformément à la procédure suivie dans le cadre d'une approche thématique, les délégués à la protection des données de toutes les agences ont été invités à utiliser les lignes directrices comme référence pratique. Ils sont également invités à communiquer au CEPD les procédures concernées pour contrôle préalable, incluant une lettre mettant en lumière les aspects spécifiques en rapport à la position du CEPD dans le domaine. Le CEPD présentera ensuite un avis commun.

☞ Lignes directrices du CEPD (EN) ([pdf](#))

## >> Lignes directrices du CEPD sur la vidéosurveillance



Le CEPD a publié un ensemble de lignes directrices à destination des institutions et organes européens sur la façon d'**utiliser la vidéosurveillance de manière responsable** et assortie de la mise en place de **garanties efficaces**. Les lignes directrices énoncent les principes destinés à évaluer la nécessité de recourir à la vidéosurveillance et à fournir des orientations sur la façon d'en minimiser l'impact sur la vie privée et autres droits fondamentaux.

Les lignes directrices s'appliquent aux systèmes existants et futurs: chaque institution a jusqu'au 1<sup>er</sup> janvier 2011 pour mettre ses pratiques existantes en conformité. Un processus de consultation, lancé juillet 2009, a suscité des commentaires visant à améliorer le projet de lignes directrices et a permis de renforcer la collaboration avec les parties prenantes.

**“ Il y a des droits fondamentaux en jeu, tels que le droit à la vie privée sur le lieu de travail. Les décisions sur l'opportunité d'installer des caméras et la manière de les utiliser ne devraient donc pas être uniquement fondées sur des considérations de sécurité. La sécurité doit plutôt être mise en balance avec**



### *les droits fondamentaux de l'individu.*

**Giovanni Buttarelli, Contrôleur adjoint**



Dans les limites prévues par la législation sur la protection des données, chaque institution et organe européen dispose d'une marge d'appréciation sur la manière de concevoir son propre système. Les lignes directrices sont conçues pour être adaptées à chaque cas. Cette **souplesse** devrait empêcher qu'une interprétation rigide ou bureaucratique des règles de protection des données ne constitue une entrave à la nécessité de sécurité ou à d'autres objectifs légitimes.

Dans le même temps, chaque institution doit également **démontrer** que des procédures sont en place afin d'assurer la **conformité avec les exigences de protection des données**. D'un point de vue organisationnel, les pratiques recommandées comprennent l'adoption d'une série de garanties en matière de protection des données devant être décrites dans la politique de vidéosurveillance de l'institution et des audits périodiques pour vérifier la conformité. Les analyses d'impact effectuées par les institutions sont encouragées, tandis que le contrôle préalable du CEPD demeure nécessaire pour les systèmes de vidéosurveillance comportant des risques significatifs (une surveillance dissimulée ou des systèmes complexes de surveillance préventive).

La protection des données ne devrait pas être considérée comme un fardeau réglementaire ou une case de bonne conformité devant être "cochée". Elle devrait au contraire faire partie de la culture organisationnelle et de la bonne gouvernance au sein desquelles les décisions sont prises par la direction de chaque institution sur base des conseils de leurs délégués à la protection de données et des consultations avec les parties prenantes.

☞ Lignes directrices du CEPD (EN) ([pdf](#))

## > Consultations sur les mesures administratives

Le règlement (CE) n° 45/2001 prévoit que le CEPD a le droit d'être informé des mesures administratives qui se rapportent au traitement de données à caractère personnel. Il peut rendre son avis soit à la demande de l'institution ou de l'organe concerné, soit de sa propre initiative. Le terme "mesure administrative" doit être entendu comme une décision d'application générale de l'administration qui concerne un traitement de données personnelles effectué par l'institution ou l'organe concerné.

### >> Accès des administrateurs IT - Banque Européenne d'Investissement

Le 26 mars 2010, le CEPD a répondu à une consultation de la Banque européenne d'investissement (BEI) en formulant des recommandations concernant la gestion des accès des administrateurs IT aux données personnelles contenues dans les systèmes et applications informatiques. Le CEPD a souligné la nécessité d'appliquer le **principe de la séparation des tâches**. Le degré de séparation devrait être défini en fonction du niveau de risque identifié pour le processus concerné.

La gestion des droits d'accès des administrateurs IT devrait être abordée selon une **approche équilibrée entre les mesures organisationnelles et techniques**. Le CEPD a également recommandé que ces mesures soient bien documentées dans une politique de sécurité détaillée établie par l'institution.

☞ Recommandations du CEPD ([pdf](#))



## >> Enregistrement des activités - Comité économique et social

Le dossier se rapporte à une consultation au sujet d'une mesure administrative relative à un projet de règlement sur l'enregistrement des activités au sein du Comité économique et social européen (le «Comité»). Le traitement s'applique à tous les enregistrements sonores, visuels ou de radiodiffusion du Comité, quelle que soit leur support.

Les enregistrements ont lieu, en principe, dans les cas suivants: les activités des organes et structures de travail du Comité et les activités au sein du Secrétariat du Comité. L'objectif est d'assurer la transparence des modalités d'enregistrement des activités au sein du Comité.

Différents échanges de lettres a eu lieu entre le CEPD et le délégué à la protection des données du Comité. Une lettre finale a été envoyée par le CEPD en mars 2010, qui souligne les différentes observations formulées par le CEPD dans son analyse:

- la finalité du traitement doit être mieux définie par le Comité, conformément à l'article 4 (1) (b) ("qualité des données") du règlement relatif à la protection des données personnelles. Ce n'est qu'une fois la finalité définie qu'une évaluation du principe de la qualité des données peut être réalisée;
- la différence entre les enregistrements conservés pour des raisons historiques et des enregistrements utilisés à des fins de transcription devrait être mieux déterminée, en ce qui concerne la période de rétention.
- le Comité devrait clarifier la situation concernant le stockage des enregistrements en tant que moyen de preuve, en précisant par exemple les situations dans lesquelles la conservation peut avoir lieu.
- la question du consentement est également une préoccupation du CEPD. Ce consentement doit être libre et explicite

☞ Lettre du CEPD ([pdf](#))

## >> Dispositions d'application concernant le délégué à la protection des données

Le Règlement (CE) N°45/2001 prévoit l'adoption par chaque institution ou organe de l'UE de **dispositions** concernant les tâches, fonctions et compétences du **délégué à la protection des données (DPD)**. À ces règles concernant la **fonction** de DPD, le projet de document soumis par l'Agence exécutive du Conseil européen de la recherche (ERCEA) propose d'ajouter une section consacrée **au rôle du responsable du traitement** et une autre à **la manière dont les personnes concernées peuvent exercer leurs droits**. Le CEPD accueille favorablement cette approche, d'autant plus que le document contient également certaines **bonnes pratiques** recommandées par le CEPD ces dernières années, à savoir:

- la constitution d'un inventaire anonyme des demandes écrites des personnes souhaitant exercer leur droit (accès, rectification, verrouillage, etc.);
- la collaboration du DPD avec les services IT et ceux de la sécurité de l'information afin de compléter ses sources d'information.



## ÉVÉNEMENTS

### > Événements à venir

#### >> Troisième atelier sur la protection des données dans les organisations internationales (Florence, 27-28 mai 2010)



Le CEPD, en coopération avec l'Institut Universitaire Européen (IUE), organise un troisième atelier sur la protection des données dans les organisations internationales les 27 et 28 mai 2010 au Théâtre Badia Fiesolana de l'IUE.. Cet atelier, réunissant diverses organisations internationales ainsi que des professeurs dans une session académique distincte, vise à aborder certaines questions actuelles concernant la protection de la vie privée et des données à caractère personnel.

☞ [Informations complémentaires](#)

#### >> Conférence bisannuelle sur la protection des données et l'application des lois (Trèves, 31 mai - 1er Juin 2010)

Cette conférence bisannuelle, organisée par l'Académie de droit européen (ERA) à Trèves, en coopération avec le CEPD, est intitulée cette année "Data protection in the age of SWIFT, PNR, Prüm and e-justice". Cette conférence offrira l'occasion de discuter d'un certain nombre de questions d'actualité concernant la protection, l'utilisation et l'échange de données à caractère personnel, telles que:

- la technologie pour la collecte et l'échange de données, également sous le "modèle d'échange d'informations de l'UE";
- l'avenir de l'échange de données UE-Etats-Unis (SWIFT, PNR, accord général sur la protection des données);
- l'impact de la Cour européenne de justice sur l'indépendance des autorités de protection des données en Allemagne, et de l'arrêt de la Cour constitutionnelle allemande sur la conservation des données;
- l'échange de données au titre du "mécanisme de Prüm";
- le cadre juridique de l'UE pour la protection des données sous le traité de Lisbonne.

Des experts du monde académique et/ou ayant une expérience pratique dans les Etats membres et les institutions européennes s'exprimeront lors de la Conférence. La participation du CEPD est assurée par Peter Hustinx, Contrôleur, qui prononcera le discours d'ouverture, et par Anne-Christine Lacoste et Hielke Hijmans qui interviendront dans d'autres sessions.

☞ Programme de la conférence ([pdf](#))

#### >> Transparence et protection des données personnelles: éléments complémentaires ou conflictuels de la bonne gouvernance? (Maastricht, 3-4 juin 2010)



Le CEPD organise en collaboration avec l'Institut européen d'administration publique (IEAP) un séminaire sur la "Transparence et protection des données personnelles: éléments complémentaires ou conflictuels de la bonne gouvernance?", qui se tiendra à Maastricht les 3 et 4 juin 2010.

Au cours du séminaire, des experts des institutions européennes ainsi que des ONG et du monde académique discuteront sur les principaux aspects et les développements des cadres juridiques de l'UE en matière de transparence et de protection des données, ainsi que sur la façon dont ces deux droits interagissent.

Le premier jour portera essentiellement sur la transparence, alors que la deuxième journée se penchera sur le droit à la protection des données à caractère personnel, en particulier le droit d'accès à ses données personnelles.

Le séminaire abordera également certains thèmes récents, tels que les nouvelles perspectives juridiques et politiques après le traité de Lisbonne, la refonte de la réglementation de l'accès aux documents ainsi que l'évolution de la jurisprudence dans ces domaines.

☞ Informations complémentaires sur le [site Internet de l'IEAP](#)

### >> Conférence de clôture du CSEE sur le cyber-harcèlement (Bratislava, 7-8 juin 2010)

Les 7 et 8 juin 2010, le Comité Syndical Européen de l'Education (CSEE) accueillera la conférence de clôture sur le cyber-harcèlement des enseignants. La conférence se tiendra à Bratislava, et réunira des participants d'organisations membres du CSEE dans l'UE/AELE et des pays candidats. Les résultats des deux enquêtes du CSEE sur le cyber-harcèlement des enseignants seront présentés lors de la conférence, et les participants discuteront des nouvelles mesures et politiques nécessaires pour prévenir et traiter le phénomène du cyber-harcèlement dans les écoles.

☞ [Informations complémentaires](#)

### >> Premier débat de la table ronde européenne de la sécurité sur le *cloud computing* (Bruxelles, 8 juin 2010)

Le 8 juin 2010, la Table ronde européenne sur la sécurité (ESRT) entamera une série de débats sur le *cloud computing*. Au cours de cette première rencontre, les possibilités et les considérations de sécurité pour le développement de technologies dématérialisées dans les administrations locales, les municipalités et les villes seront analysées dans le cadre d'un débat intitulé **"Moving to the Cloud: Risks and Opportunities - Assessment for Local Entities"**.

La Table ronde européenne sur la sécurité est





une plate-forme neutre entre les institutions de l'UE, l'OTAN et d'autres parties prenantes pour discuter de la sécurité européenne et des questions de défense.

☞ Information complémentaires et programme ([pdf](#))

## >> La Conférence sur le Traité de Lisbonne - Evaluation de l'impact sur la législation et la politique du Royaume-Uni (Londres, 15 juin 2010)

La conférence vise à fournir une analyse exhaustive des implications du traité de Lisbonne sur le droit au Royaume-Uni. Elle abordera les modifications législatives importantes, la jurisprudence pertinente et les nouveaux mécanismes de saisine, et examinera les domaines politiques que l'UE a identifiés pour l'action future dans le "Programme de Stockholm" (programme de travail Justice et Affaires intérieures pour 2010 à 2014).

L'événement permettra également d'aborder les questions suivantes:

- Est-ce que le droit communautaire s'appliquera dans davantage de cas?
- Comment la Charte européenne des droits fondamentaux changera l'approche de l'UE en faveur des droits de l'homme?
- Quelles sont les implications pour des domaines tels que la protection des données, l'immigration, la criminalité transfrontalière et le droit de la famille?

Giovanni Buttarelli, Contrôleur adjoint, apportera une contribution à la session sur "la vie privée et l'accès aux données à caractère personnel".

☞ [Informations complémentaires](#)

## > Compte rendu d'événements passés

### >> Conférence européenne des commissaires à la protection des données (Prague, 29-30 avril 2010)

Cette année, la conférence de printemps des commissaires à la protection des données a été organisée par l'Office tchèque de protection des données personnelles, sous l'intitulé "Peser le passé, en pensant à l'avenir". Les sessions de la conférence ont été consacrées à divers thèmes, notamment: 1) L'Internet des choses, la surveillance omniprésente dans l'espace et le temps - avec une présentation de Giovanni Buttarelli, Contrôleur adjoint; 2) Les enfants sur la toile des réseaux; 3) La protection des données personnelles à la croisée des chemins - avec une présentation de Peter Hustinx, CEPD et 4) Secteur public: partenaire respecté ou sous-traitant privilégié?

Sans surprise, le cadre futur de la protection des données en cours d'élaboration par la Commission européenne a été au centre des discussions. Plusieurs résolutions ont été adoptées, en particulier sur l'accord envisagé entre l'Union européenne et les Etats-Unis sur des normes de protection des données dans le domaine de la police et de la coopération judiciaire en matière pénale, sur les scanners corporels, sur la protection des enfants et sur l'avenir de la protection de la vie privée. Les résolutions seront publiées sur le site de l'Office tchèque de protection des données personnelles ([www.uoou.cz](http://www.uoou.cz)).



## >> CEPD - Réunion des délégués à la protection des données (Bruxelles, 19 mars 2010)

Le 19 mars 2010, le CEPD a participé à la réunion semestrielle des délégués à la protection des données (DPD) des institutions et organes de l'UE.

Le CEPD a saisi cette occasion pour présenter l'évolution récente de la protection des données. Le CEPD a également souligné quelques unes des implications du traité de Lisbonne pour la protection des données et des implications possibles pour le champ d'application du Règlement (CE) N° 45/2001.

Après avoir reçu un compte-rendu de la réunion des DPD du 18 mars 2010, le CEPD a présenté les développements récents dans le domaine de la supervision, tels que les travaux sur le suivi de la conformité et la politique d'application, et les principaux points de la procédure des plaintes auprès du CEPD qui sont pertinents pour les DPD.

Les discussions ont également porté sur le principe de notification des failles de sécurité. Le principe de la notification aux autorités de protection des données et, dans certains cas, aux utilisateurs et personnes concernées, a été reconnu dans la récente réforme de la Directive 2002/58/CE "vie privée et communications électroniques". En parallèle, la Commission a adopté en mai 2009 les règles d'application de la décision de 2006 sur la sécurité des systèmes informatiques qui prévoient également la déclaration au DPD des "événements de sécurité des systèmes d'information" en matière de données personnelles. Certaines agences et entreprises communes sont tenues d'appliquer les mêmes règles par le biais de leur *Service Level Agreement* avec la Commission. Le CEPD a donc également invité les DPD à mettre en place un groupe de travail pour discuter de la mise en œuvre du principe de la notification des failles de sécurité.

## >> Case Handling Workshop (Bruxelles, 18-19 mars 2010)

L'autorité belge de la protection des données a accueilli le 21<sup>ème</sup> atelier de traitement des dossiers, les 18 et 19 mars 2010. Ces ateliers, qui se tiennent deux fois par an, ont pour but de rassembler des gestionnaires de dossiers des différentes autorités de protection des données pour échanger des idées et des bonnes pratiques sur les dossiers pertinents. Rosa Barcelo du CEPD a contribué à l'atelier par une présentation sur la publicité comportementale en ligne.

☞ [Informations complémentaires](#)



## DISCOURS ET PUBLICATIONS

- "Internet of things: ubiquitous monitoring in space and time", discours (EN) ([pdf](#)) prononcé par Giovanni Buttarelli lors de la conférence des commissaires à la protection des données et de la vie privée d'Europe (Prague, 29 avril 2010)
- "The Strategic Context and the Role of Data Protection Authorities in the Debate on the Future of Privacy", discours (EN) ([pdf](#)) prononcé par Peter Hustinx lors de la conférence des commissaires à la protection des données et de la vie privée d'Europe (Prague, 29 avril 2010)
- "Protection des données et informatique dématérialisée dans le droit européen", discours ([pdf](#)) prononcé par Peter Hustinx lors de la "Troisième journée européenne de sensibilisation à la cybersécurité" (Bruxelles, 13 avril 2010)



- "A privacy Framework for the Stockholm Programme", discours (EN) ([pdf](#)) prononcé par Peter Hustinx lors du RISE - High Level Workshop on Ethical and Policy Implications of Global Mobility and Security (Bruxelles, 26 mars 2010)
- "Pour un usage responsable de la biométrie: perspectives du Contrôleur européen de la protection des données", discours ([pdf](#)) prononcé par Peter Hustinx lors des "3èmes Rencontres parlementaires sur la Sécurité" (Paris, 23 mars 2010).

## A propos de cette newsletter

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

- superviser le traitement des données personnelles dans les institutions et organes communautaires;
- conseiller les institutions européennes sur la législation en matière de protection des données;
- coopérer avec les autorités nationales de protection des données afin de promouvoir la cohérence au niveau de la protection des données à caractère personnel.

☞ **Vous pouvez vous abonner / désabonner à cette newsletter sur notre site [web](#).**

### COORDONNÉES

[www.edps.europa.eu](http://www.edps.europa.eu)  
Tel: +32 (0)2 34234234234  
Fax: +32 (0)2 34234234234  
e-mail: see our contacts page

### ADRESSE POSTALE

EDPS – CEDP  
Rue Wiertz 60 – MO 63  
B-1047 Bruxelles  
BELGIQUE

### BUREAUX

Rue Montoyer 63  
Bruxelles  
BELGIQUE

**CEPD – Le gardien européen de la protection des données personnelles**