EDPS Newsletter

EUROPEAN DATA PROTECTION SUPERVISOR

N° 21 | 9 OCTOBRE 2009

CONSULTATION

> Avis du CEPD sur les systèmes de transport intelligents 1
> Avis du CEPD sur des mesures restrictives concernant le réseau Al-Qaïda et les Taliban 2
> Avis du CEPD sur l'accès des services de répression à EURODAC 3

SUPERVISION

> Contrôles préalables de traitements de données personnelles 4
> Consultation sur les mesures administratives 5
> Enquêtes 7

EVENEMENTS

> Séminaire sur les conséquences de failles de sécurité (Bruxelles, 23 octobre 2009) 7
> Conférence internationale des Commissaires à la protection des données et de la vie privée (3-6 Novembre, Madrid) 8
> Réunion CEPD - Délégués à la protection des données (Bruxelles, 2 Octobre 2009) 8
> Séminaire sur les lignes directrices du CEPD en matière de vidéosurveillance (Bruxelles, 30 septembre 2009) 9

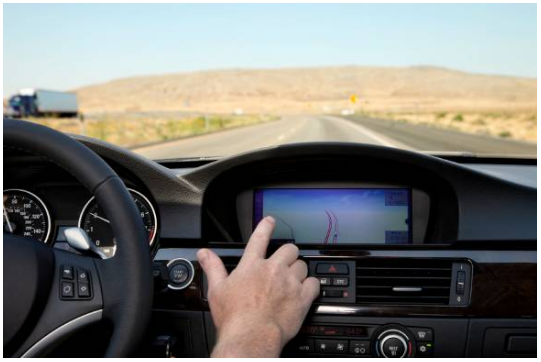
DISCOURS ET PUBLICATIONS

> Publication du Rapport annuel 2008 du CEPD 10
> Discours 11

NOUVEAUX DELEGUES A LA PROTECTION DES DONNEES 11

CONSULTATION

> Avis du CEPD sur les systèmes de transport intelligents



© iStockphoto

L'avis du CEPD, adopté en juillet, porte sur la proposition d'un plan de déploiement de la Commission européenne pour les systèmes de transport intelligents (STI) en Europe en vue d'accélérer et de coordonner leur déploiement dans les transports routiers et leur relation avec d'autres modes de transport. Le déploiement des STI a des **implications importantes en termes de protection de la vie privée**s, notamment parce que ces systèmes permettent de suivre un véhicule et de recueillir un large éventail de données relatives aux habitudes de conduite des usagers européens de la route.

Le CEPD relève que la protection des données a été prise en compte dans le projet de cadre juridique et qu'elle est également présentée comme une condition générale pour le déploiement des STI. Il souligne cependant que la proposition est **trop générale** pour répondre de façon appropriée aux questions de vie

privée et de protection des données soulevées par le déploiement des STI dans les États membres. En particulier, le cadre juridique ne définit pas clairement quand l'exécution des services STI entraînera la collecte et le traitement de données personnelles, quelles sont les finalités et les modalités selon lesquelles des traitements de données pourront avoir lieu, ou qui sera responsable du respect des obligations en matière de protection des données.

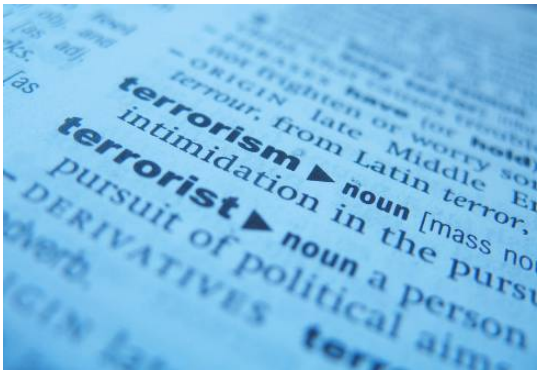
> ***Il y a un risque que le manque de clarté du cadre juridique proposé conduise à une incertitude élevée, à une fragmentation et à des incohérences en raison de différents niveaux de protection des données en Europe***
> ***Peter Hustinx, CEPD***

L'avis du CEPD inclut les principales recommandations suivantes:

- **clarification des responsabilités**: il est essentiel de clarifier les rôles des différents acteurs impliqués dans les STI afin de déterminer qui a la responsabilité de s'assurer que les systèmes fonctionnent correctement du point de vue de la protection des données (qui est le responsable du traitement ?);
- **garanties pour l'utilisation des technologies de localisation**: des mesures de protection appropriées (précisions sur les circonstances spécifiques pour lesquelles les mouvements d'un véhicule seront suivis et limitation stricte de l'utilisation de systèmes de localisation à ce qui est nécessaire, notamment) doivent être mises en œuvre par les responsables du traitement qui fournissent des services STI pour que l'utilisation des technologies de localisation ne soit pas intrusive en termes de vie privée;
- ***"privacy by design"***: le CEPD recommande d'envisager la vie privée et la protection des données à un stade précoce de la conception des STI afin de définir l'architecture, le fonctionnement et la gestion des systèmes. La protection de la vie privée et les exigences de sécurité doivent être incorporées dans les normes, les meilleures pratiques, les spécifications techniques et les systèmes.

☞ Avis du CEPD (EN) (pdf)

> Avis du CEPD sur des mesures restrictives concernant le réseau Al-Qaïda et les Taliban



© iStockphoto

Le CEPD a adopté fin juillet un avis sur la proposition de la Commission européenne visant à amender un règlement du Conseil instituant des mesures restrictives à l'encontre de certaines personnes et entités liées à Oussama ben Laden, au réseau Al-Qaïda et aux Taliban. Cette proposition modifie l'un de ces instruments communautaires, les "listes noires de terroristes", adoptés en vue de lutter contre le terrorisme en prenant des mesures restrictives (gel des avoirs, par exemple) en ce qui concerne les personnes physiques et morales soupçonnées d'être associées à des organisations terroristes.

Dans son avis, le CEPD se félicite de l'intention de la Commission de renforcer la procédure d'établissement de listes noires, tout en prenant en compte le droit à la protection des données

personnelles et l'applicabilité du règlement sur la protection des données (règlement (CE) No 45/2001). Tout en reconnaissant pleinement l'objectif de lutte contre le terrorisme par le traitement et l'échange de données personnelles, le CEPD est convaincu que la protection des données personnelles est un facteur essentiel afin d'assurer la légitimité et l'efficacité des mesures restrictives prises par la Commission.

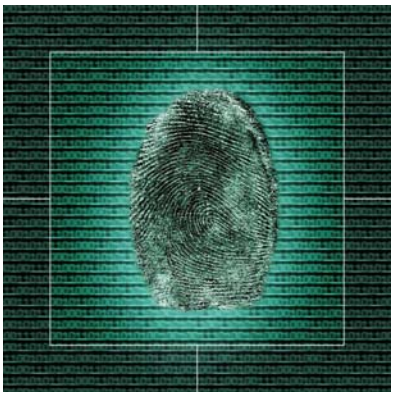
Dans ce contexte, le CEPD recommande:

- de **modifier l'article 7d** - qui soumet la divulgation de documents confidentiels au consentement de l'auteur - de manière à préserver le droit de la personne concernée d'avoir accès à ses données personnelles. L'amendement devrait également garantir la possibilité pour le CEPD et la Cour de justice d'avoir accès aux données personnelles contenues dans les informations confidentielles afin de pouvoir s'acquitter efficacement de leurs tâches respectives;
- de veiller à ce que les données traitées soient utilisées à des **fins précises** et que les éventuels transferts de données vers des pays tiers et organisations internationales garantissent une **protection adéquate** de ces données, éventuellement par l'intermédiaire d'arrangements spécifiques avec les Nations Unies;
- d'examiner si la question des **obligations des responsables du traitement** et la **responsabilité** encourue en cas de traitement illicite ou de divulgation de données personnelles doit être considérée et précisée en plus amples détails dans la proposition.

Le CEPD est également en train d'examiner les propositions adoptées par la Commission concernant des mesures restrictives analogues à l'égard de la Somalie, du Zimbabwe et de la Corée du Nord.

☞ Avis du CEPD (EN) (pdf)

> Avis du CEPD sur l'accès des services de répression à EURODAC



Le CEPD a adopté un avis sur deux propositions de la Commission visant à établir la base selon laquelle les services répressifs peuvent, sous conditions, avoir accès à la base données EURODAC. Ces deux propositions autorisent l'accès au système EURODAC à des fins de prévention, de détection et d'enquête relatives à des infractions terroristes et autres infractions graves, selon les conditions exposées dans les propositions.

Le CEPD a analysé les propositions sous l'angle de leur légitimité, en prenant comme point de départ la nécessité de trouver un juste équilibre entre les exigences de sécurité publique et le droit fondamental à la vie privée et à la protection des données, conformément à l'article 8 de la Convention européenne sur les droits de l'homme (CEDH). **L'analyse a abouti à la conclusion que la nécessité et la proportionnalité des propositions, éléments impératifs pour justifier la légitimité de l'intrusion à la vie privée, ne sont pas démontrées.** En conséquence, le CEPD exprime de sérieuses réserves sur la légitimité des propositions et sur le fait que des instruments législatifs doivent être adoptés sur cette base.

> ***Pour être valable, la nécessité de l'atteinte à la vie privée doit être justifiée par des éléments clairs et indéniables, et la proportionnalité du traitement des données personnelles doit être démontrée. Cela est d'autant plus essentiel dans le cas d'une intrusion dans les droits d'individus constituant un groupe vulnérable et devant être protégés parce qu'ils fuient la persécution***
> ***Peter Hustinx, CEPD***

Le CEPD recommande d'évaluer la légitimité des propositions dans un contexte plus large, notamment:

- la tendance d'accorder aux autorités policières et judiciaires l'accès aux données personnelles d'individus qui ne sont soupçonnés d'aucun crime et dont les données ont été recueillies à d'autres fins;
- la nécessité d'une évaluation au cas par cas de chaque proposition de ce type et d'une vision cohérente, globale et prospective, de préférence en lien avec le prochain programme-cadre en matière de justice et affaires intérieures ("programme de Stockholm");
- la nécessité de procéder en premier lieu à la mise en œuvre et à l'évaluation d'instruments européens nouveaux, tels que la "décision Prüm", qui permettent la consultation par un État membre des empreintes digitales et autres données policières détenues par un autre État membre;
- la possibilité de retarder l'examen des propositions, à la lumière de l'évolution de l'environnement juridique et politique (entrée en vigueur du traité de Lisbonne et discussions en cours sur la refonte des règlements EURODAC et Dublin, par exemple).

Le CEPD souligne également que la nécessité des propositions doit être démontrée au moyen de preuves solides quant au lien entre les demandeurs d'asile et le terrorisme et/ou les formes graves de criminalité.

☞ Avis du CEPD (EN) (pdf)

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.

Base de données EudraVigilance - Agence européenne des médicaments

L'Agence européenne des médicaments (EMEA) héberge et gère la base de données EudraVigilance, qui contient des **rapports sur les effets indésirables suspectés de médicaments à usage humain** ("Individual Case Safety Reports" - Rapports de sécurité sur des cas individuels ou "ICSRs"). Ces informations sont fournies à l'EMEA par les autorités nationales compétentes, les détenteurs d'autorisation de mise sur le marché, et les sponsors d'essais cliniques et autres.

La base de données vise à permettre aux autorités nationales compétentes et à l'EMEA de rendre compte et d'évaluer les ICSRs pendant le développement et après l'autorisation de commercialisation des médicaments.

L'avis du CEPD souligne que l'EMEA, les autorités nationales compétentes, les détenteurs d'autorisation de mise sur le marché et les sponsors **partagent les responsabilités** en ce qui concerne les droits des personnes concernées, selon des cadres juridiques différents en fonction de leurs attributions (règlement (CE) n° 45/2001 pour l'EMEA, législation nationale d'application de la directive 95/46/CE pour les autres acteurs). En conséquence, une partie des recommandations adressées à l'EMEA met l'accent sur la **nécessité de coordination** et d'efforts conjoints entre les différents acteurs.

Le CEPD a émis des recommandations, notamment en matière de **respect avec le principe de qualité de données**. En particulier, il a demandé à l'EMEA:

- de procéder à un examen de la possibilité d'anonymiser ou de pseudoanonymiser les informations personnelles contenues dans les ICSRs, ainsi que de minimiser les données personnelles enregistrées ;
- d'engager un dialogue avec les autorités nationales compétentes, les détenteurs d'autorisation de mise sur le marché et les sponsors afin de rédiger un formulaire de notification type à fournir aux personnes concernées. Ce formulaire devrait contenir une référence EudraVigilance;
- de procéder à une évaluation des motifs juridiques pour le transfert des données hors de l'UE; d'évaluer si les autorités destinataires assurent un niveau approprié de protection ; ou si une exception s'applique en raison de l'irrégularité des transferts. Dans l'alternative, envisager d'introduire des dispositions contractuelles;
- d'examiner si une période de conservation limitée permettrait d'atteindre les objectifs recherchés par le traitement des données;
- d'adopter certaines des mesures de sécurité présentées dans l'avis.

☞ Avis du CEPD (EN) (pdf)

> Consultation 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.

Transferts des données à caractère personnel à des pays tiers : "adéquation" des signataires de la Convention 108 du Conseil de l'Europe - consultation de l'OLAF

L'Office européen de lutte antifraude (OLAF) a posé la question de savoir si trois groupes de pays identifiés peuvent être considérés avoir un **niveau approprié de protection** des données, à la lumière de leur relation à la Convention 108 du Conseil de l'Europe et à son protocole additionnel.

Dans le cas où un ou plusieurs de ces groupes n'était pas considéré comme ayant un niveau approprié de protection au sens du règlement sur la protection des données (article 9.1 du règlement (CE) n° 45/2001), OLAF a également demandé si les engagements qu'ils avaient pris dans le cadre de la Convention et/ou des accords d'aide administrative mutuelle dans le domaine douanier pouvaient eux être considérés comme des "garanties appropriées" (article 9.7 du règlement).

Suite à son analyse, le CEPD a conclu qu'il n'avait pas reçu d'éléments de preuve suffisants quant à la mise en œuvre satisfaisante de la Convention 108 et de son protocole additionnel, selon le cas, dans les pays mentionnés dans la consultation. Les trois groupes de pays **ne peuvent donc pas être considérés**, en principe, **avoir un niveau de protection approprié**.

Le CEPD a ajouté que l'OLAF pouvait néanmoins envisager de conduire une **évaluation** afin de confirmer qu' un transfert - ou un ensemble de transferts - pouvait être fait, dans la mesure où celui-ci serait limité à des finalités et bénéficiaires spécifiques dans le pays de destination, dans le cas où ce pays fournit un niveau approprié de protection. Cette évaluation impliquerait un examen du droit interne qui met en œuvre la Convention et son protocole et de leur application effective.

Le CEPD a également indiqué qu'une **troisième ligne de conduite**, qui peut offrir davantage de certitudes et améliorer la protection de la vie privée et des données personnelles, pouvait représenter une alternative possible pour OLAF et les destinataires de présenter les garanties appropriées. À cet égard, les engagements pris jusqu'ici par ces groupes de pays ne peuvent pas être considérés, *en tant que tel*, comme une "garantie appropriée", compte tenu du fait que le responsable du traitement n'a pas mentionné l'existence de mesures qui compenseraient l'absence de preuves d'un niveau général de protection.

☞ Analyse du CEPD (EN) (pdf)

Consultation sur le traitement des données à caractère personnel dans le cadre de la procédure de pandémie - Banque centrale européenne

Le CEPD a été consulté sur la question du traitement des données à caractère personnel par la Banque centrale européenne (BCE) en cas de pandémie. Outre le traitement des données à caractère personnel par les services médicaux de la BCE, la pandémie exigerait également d'informer la gestion locale qu'une personne spécifique est soupçonnée d'être infectée de sorte que les membres concernés de l'équipe puissent être avertis.

Le CEPD a considéré qu'en l'absence de toute obligation légale nationale, l'article 5(a) du règlement (CE) n° 45/2001 peut servir de **base juridique** pour le traitement des données dans le cadre de la procédure de pandémie. Néanmoins, comme cela est exceptionnel, il serait souhaitable que la **direction de la BCE** adopte une **décision formelle** sur base de laquelle toute communication destinée à la direction peut être adressée. Une **procédure de crise spéciale** pourrait en effet être établie pour garantir la protection des droits et des libertés des personnes concernées, et notamment leur droit à la vie privée. Cette procédure pourrait notamment s'appuyer sur les recommandations de l'Organisation Mondiale de la Santé qui n'ont aucune valeur juridique contraignante, mais qui pourraient servir de base à toute décision interne à ce sujet.

Le CEPD a par ailleurs souligné que, puisque le traitement concerne des **données relatives à la santé**, le traitement de ce type de données est interdit, à moins que des exceptions puissent être trouvées, conformément à l'article 10 du règlement. Le traitement des données relatives à la santé pourrait être basé sur une obligation légale pour les employeurs de se conformer aux obligations sur la santé et la sécurité au travail. Le CEPD a également considéré que, dans le dossier examiné, des **raisons d'"*intérêts publics substantiels*"** pouvaient également **justifier le traitement** de données sanitaires dans le cadre de cette procédure, mais que des **sauvegardes appropriées** devaient être mises en place pour protéger les intérêts des personnes concernées. Ces sauvegardes devraient notamment inclure des

dispositions selon lesquelles les données ne peuvent être utilisées pour d'autres finalités et ne peuvent être transférées à aucun tiers. Elles devraient également comprendre la fixation de délais appropriés pour la conservation des données et des dispositions permettant de garantit les droits à la protection des données des personnes concernées.

☞ Analyse du CEPD (EN) (pdf)

> Enquêtes

Le CEPD effectue des enquêtes de sa propre initiative ou sur la base d'une plainte. Il dispose de compétences étendues lui permettant d'avoir accès aux données à caractère personnel, aux informations et aux documents utiles à ses enquêtes, ainsi qu'aux locaux s'il est nécessaire d'enquêter sur place. Le CEPD effectue également des inspections sur place afin de vérifier dans la pratique le respect du règlement (CE) n° 45/2001 sur la protection des données par l'ensemble des institutions et organes communautaires.

Procédure et politique d'inspection du CEPD adoptées

Le 23 juillet 2009, le CEPD a adopté son **manuel d'inspection interne** et publié sur son site internet le résumé de la procédure suivie par les membres de son personnel lors de la procédure d'inspection. La procédure d'inspection est basée essentiellement sur le cadre juridique existant, les principes généraux du droit européen, et les bonnes pratiques administratives communes aux institutions et aux organes communautaires. Un document stratégique sur le rôle des inspections dans les activités de supervision et sur les critères pour mener une inspection sera élaboré et rendu public en temps utile.

Les règles reflètent les expériences actuelles du CEPD. Le manuel d'inspection est un document évolutif, et donc soumis à modifications en fonction de la progression des pratiques et des expériences du CEPD. La politique d'inspection du CEPD contribue à l'effort visant à **mesurer la conformité** avec le règlement (CE) n° 45/2001 selon différents types de contrôles dans les institutions et les organes communautaires.

☞ Politique et procédure d'inspection du CEPD (EN) (pdf)

E V E N E M E N T S

>> Evénements à venir

> Séminaire sur les conséquences de failles de sécurité (Bruxelles, 23 octobre 2009)

Le CEPD, conjointement avec l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), organise un séminaire sur les conséquences des failles de sécurité, le 23 octobre, au Parlement européen.

Le séminaire sera divisé en trois parties correspondant aux grandes étapes du cycle de vie d'une faille de sécurité, à savoir:

- le partage et l'analyse des meilleures pratiques de **prévention** et de réduction des risques de failles de sécurité du point de vue du responsable du traitement;

- offrir un lieu d'échanges des meilleures pratiques développées par les autorités nationales de protection des données, ainsi que par les institutions et le secteur privé pour **la gestion** des failles de sécurité, y compris l'instauration de procédures d'investigation des incidents;
- recueillir les expériences en matière de **notification** des failles de sécurité dans d'autres secteurs et dans les pays hors Union européenne.

☞ **Pour vous inscrire à ce séminaire, veuillez envoyer un email à: EDPS-Events@edps.europa.eu**.
☞ Programme du séminaire

> Conférence internationale des Commissaires à la protection des données et de la vie privée (3-6 Novembre, Madrid)

Une délégation du CEPD participera à la conférence. Peter Hustinx présidera une session consacrée aux thèmes de la loi applicable et de la mondialisation, durant laquelle les conséquences de phénomènes nouveaux tels que les services d'hébergement et d'accueil, et le "cloud computing" seront abordées.

La Conférence prévoit l'adoption d'une résolution sur les normes internationales en matière de vie privée. La préparation de cette résolution a été coordonnée par l'autorité espagnole de protection des données suite à une résolution de la conférence internationale de 2008 à Srasbourg. Le CEPD a activement participé à sa préparation.

La résolution se félicite de la proposition commune en faveur d'un projet de normes internationales sur la protection de la vie privée en ce qui concerne le traitement de données personnelles. Cette proposition commune prévoit un ensemble de principes, droits, obligations et procédures que tout système juridique en matière de protection des données et de vie privée devrait s'efforcer d'atteindre. Le traitement des données personnelles dans les secteurs public et privé pourrait ainsi être effectué selon une approche plus uniforme au niveau international

☞ Plus d'informations sur: www.privacyconference2009.org

>> Evénements passés

> Réunion CEPD - Délégués à la protection des données (Bruxelles, 2 Octobre 2009)

Le 2 Octobre 2009, le CEPD a participé à la réunion semestrielle des délégués à la protection des données (DPD) des institutions et agences européennes organisée à Bruxelles par la Commission européenne et l'OLAF.

Les deux allocutions d'ouverture de Catherine Day (secrétaire générale de la Commission) et de Nicholas Ilett (chef adjoint à l'OLAF) ont réitéré l'engagement de leurs institutions envers la protection des données personnelles.

Après une introduction générale de Peter Hustinx, CEPD, sur les développements récents dans la protection des données au niveau européen et international soulignant la tendance à la responsabilisation des parties prenantes, la réunion s'est concentrée sur les développements dans le

domaine des activités de supervision du CEPD. Plusieurs membres du personnel du CEPD ont présenté les évolutions récentes du CEPD dans des domaines tels que les inspections dans les institutions et agences, le traitement des plaintes, le contrôle préalable des opérations de traitement et les consultations sur des mesures administratives. La réunion a également été l'occasion de tirer des conclusions préliminaires relatives au séminaire de travail du CEPD sur la vidéosurveillance (voir ci-dessous).

Les questions ouvertes à de nouvelles discussions entre les DPD et le CEPD comprennent l'établissement de normes professionnelles pour les DPD, les formulaires de notification pour contrôle préalable et la question des opérations de traitement interinstitutionnelles.

> Séminaire sur les lignes directrices du CEPD en matière de vidéosurveillance (Bruxelles, 30 septembre 2009)

Le 30 Septembre 2009, le CEPD a organisé un séminaire sur la vidéosurveillance à Bruxelles. Près d'une centaine de délégués à la protection des données, responsables de sécurité, spécialistes en vidéosurveillance et technologies de l'information, et représentants du personnel, provenant de plus de 40 institutions et organes communautaires ont participé au séminaire. Le séminaire s'appuyait essentiellement sur le **projet de lignes directrices du CEPD sur la vidéosurveillance**, publiée le 7 Juillet 2009.

Dans son **discours d'ouverture**, le Contrôleur adjoint, Giovanni Buttarelli, a souligné que des "droits fondamentaux étaient en jeu", notamment le droit à la vie privée sur les lieux de travail, le droit d'être libre de toute discrimination, la liberté d'expression et la liberté de réunion. Par conséquent, les décisions sur l'opportunité d'installer des caméras et la manière de les utiliser ne devraient pas être uniquement fondées sur les exigences de sécurité. Ces dernières doivent plutôt être mises en balance avec le respect des droits fondamentaux.

Le discours d'ouverture a été suivi d'un **aperçu du cadre de conformité** proposé dans les lignes directrices. Cet aperçu a mis l'accent sur la nécessité de passer d'une perception de la protection des données en tant que charge administrative à une approche basée sur la vie privée dès la conception ("privacy by design"), sur une prise de décision transparente impliquant toutes les parties prenantes, sur le rôle actif des délégués à la protection des données, et sur la responsabilité de l'institution responsable de l'exploitation du système de vidéosurveillance. Pour assurer un cadre de procédure plus efficace sans être trop contraignant, il n'est pas nécessaire, dans la plupart des cas, que le CEPD opère un contrôle préalable des systèmes de vidéosurveillance avant leur mise en œuvre.

Le séminaire a atteint ses deux objectifs, à savoir susciter des **commentaires afin d'améliorer le projet** de lignes directrices et **renforcer la coopération** pour assurer le respect des principes de protection des données. De manière générale, la réaction des participants au projet de lignes directrices a été positive. Dans un climat de préoccupation croissante face à la vidéo-surveillance, les participants ont favorablement accueilli le fait que les lignes directrices fournissent des **conseils pratiques** sur la

décision d'installer ou d'utiliser des équipements de vidéo-surveillance et, lorsqu'il s'agit de leur utilisation, sur la meilleure manière d'aborder les questions de protection des données.

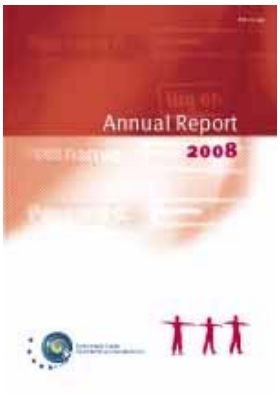
Pendant les discussions, des **préoccupations** ont été soulevées au sujet de la responsabilisation, de la prise de décision et de la valeur juridique des lignes directrices. Les intervenants ont demandé des éclaircissements sur les principaux "outils de conformité" tels que la politique de vidéo-de surveillance, l'audit interne, et les évaluations d'impact. Ils ont aussi émis des commentaires sur des questions de fond, notamment sur ce qui peut être considéré comme objectifs légitimes et proportionnels pour utiliser la vidéo-surveillance et combien de temps les images peuvent être conservées.

Les lignes directrices seront formellement publiées avant la fin de cette année.

☞ La documentation relative au séminaire est disponible sur notre site web.

DISCOURS ET PUBLICATIONS

> Publication du Rapport annuel 2008 du CEPD



Le CEPD a publié son Rapport annuel qui couvre 2008, quatrième année complète d'activité du CEPD en tant que nouvelle autorité indépendante de supervision. Ce rapport conclut également le premier mandat du CEPD et donne l'occasion de dresser un bilan des développements intervenus depuis le départ.

Le rapport montre que des progrès significatifs ont été réalisés, tant dans le rôle de supervision du CEPD que dans sa fonction de conseil. La plupart des institutions et organes communautaires sont en bonne voie dans le respect des règles de protection des données, mais des défis importants doivent encore être relevés. Le travail de supervision entend donc mettre davantage l'accent sur l'évaluation du niveau de conformité dans la pratique, en particulier au moyen de vérifications plus systématiques sur les lieux et d'un suivi de la mise en œuvre des recommandations dans le cadre des contrôles préalables. Le CEPD a également amélioré sa fonction de conseiller des institutions européennes et a présenté des avis sur un nombre croissant de propositions législatives.

En ce qui concerne les activités de **supervision** du CEPD, le rapport souligne l'adoption d'un nombre record d'avis de contrôle préalable relatifs aux opérations de traitement de données personnelles dans les institutions et organes communautaires. Ces avis ont principalement porté sur les données relatives à la santé, le recrutement du personnel et la sélection de candidats, l'évaluation du personnel, les systèmes de gestion des identités, le contrôle des accès et les enquêtes de sécurité. Le CEPD a également procédé à l'examen de questions clés abordées pour la première fois, telles que le contrôle d'accès avec authentification de l'iris ou des empreintes digitales, le suivi de l'utilisation d'Internet par le personnel, et les systèmes de vidéo-surveillance.

Dans son rôle de **conseil**, le CEPD a mis un accent particulier sur de nouvelles initiatives dans le domaine de la liberté, de la sécurité et de la justice, en particulier l'adoption de la décision-cadre relative

à la protection des données personnelles dans le cadre de la coopération policière et judiciaire en matière pénale. D'autres thématiques telles que la révision de la directive "Vie privée et communications électroniques", l'accès du public aux documents et les soins de santé transfrontaliers ont été également très importants. Le CEPD a par ailleurs examiné des questions relatives à la mise en place de systèmes d'information et à l'accès à ces systèmes (paquet de la Commission relatif à la gestion des frontières de l'UE, échange transatlantique d'informations à des fins répressives, par exemple), la qualité des données, ainsi que l'utilisation des nouvelles technologies et les développements actuels dans la société de l'information (RFID et intelligence ambiante).

> Discours

- Allocution de bienvenue (EN) (pdf) de Giovanni Buttarelli sur "Les droits fondamentaux en jeu", séminaire du CEPD sur la vidéosurveillance dans les institutions et organes communautaires (Commission européenne, Bruxelles, 30 septembre 2009)
- Discours (EN) (pdf) prononcé par Giovanni Buttarelli à une réunion de la commission LIBE du Parlement européen sur "The use of information technology for customs purposes" (Bruxelles, 29 septembre 2009;
- "*The relation between transparency and the rights of privacy and the protection of personal data*", discours (EN) (pdf) prononcé par Peter Hustinx au séminaire "Transparency and Clear Legal Language in the EU" organisé par la Présidence suédoise (Stockholm, 8 septembre 2009)
- Discours (EN) (pdf) prononcé par Peter Hustinx à la réunion conjointe des commissions LIBE et ECON du Parlement européen sur l'accord intérimaire UE-Etats-Unis suite à un changement dans suite à l'entrée en vigueur de la nouvelle structure du réseau SWIFT (Bruxelles, 3 septembre 2009)
- *Current Challenges for Data Protection in Europe*", discours (EN) (pdf) prononcé par Peter Hustinx à la conférence de printemps de la commission autrichienne des juristes (Weissenbach am Attersee, 21 mai 2009)

NOUVEAUX DELEGUES A LA PROTECTION DES DONNEES

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 des obligations de protection des données établies par le règlement (CE) n° 45/2001.

Nominations récentes:

- **Beata HATWIG**, Executive Agency for Health and Consumers (EAHC)
- **Triinu VOLMER**, European GNSS Supervisory Authority (GSA)
- **Francesca PAVESI**, European Aviation Safety Agency (EASA)

☞ Liste complète des DPD.

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 une approche cohérente en matière de protection des données.

☞ **Vous pouvez vous inscrire/désinscrire à cette newsletter sur notre site internet.**

COORDONNÉES

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