Newsletter du CEPD
LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES
N°26 | NOVEMBRE 2010

CONSULTATION

> Avis du CEPD sur la stratégie extérieure de l'UE relative aux dossiers passagers

Le 19 octobre 2010, le CEPD a adopté un avis sur la communication de la Commission européenne sur le transfert des données des dossiers passagers (*Passenger Name Record* - PNR) vers les pays tiers. La communication présente la stratégie extérieure de l'UE relative aux dossiers passagers et met en avant les principes généraux, y compris les normes en matière de protection des données, que tout accord PNR avec un pays tiers doit respecter.

Le CEPD accueille favorablement l'approche horizontale suivie par la Commission et soutient l'objectif de parvenir à un niveau élevé et harmonisé de protection des données applicable à tous les régimes PNR actuels et à venir. Il exprime toutefois ses préoccupations en ce qui concerne la **nécessité** et la **légitimité** de certains aspects importants des systèmes proposés. Il estime en particulier que l'utilisation proactive des données PNR de tous les passagers à des fins d'évaluation des risques nécessite des justifications et garanties plus explicites.

> ***Je soutiens l'approche horizontale présentée par la Commission qui représente une étape essentielle vers l'établissement d'un cadre global pour l'échange de données PNR. Néanmoins, pour être recevables, les conditions de collecte et de traitement des données PNR devraient être considérablement restreintes. Je suis particulièrement préoccupé par l'utilisation des régimes PNR pour l'évaluation des risques ou pour le profilage.*** ***Peter Hustinx, CEPD***

Le CEPD souligne également la nécessité d'assurer une **cohérence** entre les différentes initiatives directement ou indirectement liées au traitement des données PNR, y compris le cadre général européen pour la protection des données - en cours de révision, l'initiative visant à la mise en place d'un système PNR pour l'UE, et les négociations en cours pour un accord UE-États-Unis-Unis sur le partage des données pour l'application des lois.

En ce qui concerne le contenu des normes de protection des données, le CEPD demande **davantage de précision** concernant les **garanties minimales** applicables aux accords PNR. Des conditions plus strictes devraient en particulier être appliquées en matière de données sensibles, des conditions de transferts ultérieurs, et de rétention des données.

Le CEPD souligne également la nécessité pour tout accord PNR de prévoir expressément les **droits directement applicables** pour les individus concernés.

☞ Avis du CEPD (EN) (pdf)

> Avis du CEPD sur la gestion de l'information dans l'espace de liberté, de sécurité et de justice

L'avis, adopté le 30 septembre 2010, se rapporte à la communication de la Commission du 20 juillet 2010 fournissant un panorama complet des instruments européens régissant la collecte, le stockage et l'échange de données personnelles à des fins répressives ou de gestion des flux migratoires (le Système d'information Schengen, EURODAC et la «décision de Prüm» sur l'échange de données ADN sont quelques exemples de ces instruments). La communication définit également les principes fondamentaux que la Commission entend utiliser en référence lors de la préparation et de l'évaluation de propositions législatives.

Le CEPD salue et soutient pleinement les objectifs et le principal contenu de la communication, mais attire cependant l'attention sur le fait que cette initiative ne doit être considérée que comme une première étape dans le processus d'évaluation. Un tel exercice devrait être suivi par des mesures concrètes menant à la mise en place d'une politique européenne structurée, intégrée et globale en matière d'échange et de gestion de l'information.

> ***Une politique globale fondée sur une évaluation en profondeur est nécessaire dans le domaine. Je considère cette communication comme une première étape importante dans cette direction et je suivrai de près les développements en la matière.*** ***Peter Hustinx, CEPD***

L'avis comprend également les recommandations suivantes:

- **évaluation objective et équilibrée**: l'évaluation de la gestion de l'information ne doit pas seulement se concentrer sur les aspects positifs, mais doit aussi faire état des insuffisances et faiblesses des systèmes (par exemple, nombre de personnes arrêtées à tort ou mises dans l'embarras suite à un faux résultat positif dans le système);

- **harmonisation des droits des personnes concernées**: il convient de s'assurer que les citoyens bénéficient de droits équivalents en matière de protection des données quel que soit le système ou instrument de l'UE considéré;

- **évaluation d'impact sur la protection des données et de la vie privée**: la communication constitue une bonne occasion de mieux analyser ce que l'on entend par «évaluation d'impact sur la protection des données et de la vie privée». Des indicateurs et caractéristiques spécifiques devraient être développés à cette fin;

- **biométrie et interopérabilité des systèmes**: le CEPD invite la Commission à élaborer une politique plus cohérente sur les conditions préalables à l'utilisation de la biométrie, ainsi qu'une politique en matière d'interopérabilité des systèmes.

☞ Avis du CEPD (pdf)

> Avis du CEPD sur la décision de protection européenne et la décision d'instruction européenne en matière pénale

L'avis, adopté le 5 octobre 2010, se rapporte aux initiatives d'un certain nombre d'États membres en faveur d'une directive relative à la décision de protection européenne (EPO) (pdf) et d'une directive relative à la décision d'instruction européenne (EIO) (pdf) en matière pénale. Le but est d'améliorer au sein de l'UE la protection des victimes de la criminalité (en particulier les femmes) et la coopération transfrontalière en matière pénale en créant un instrument unique, souple et efficace – la décision d'instruction européenne – pour l'obtention de preuves situées dans un autre État membre. Les initiatives, basées toutes les deux sur le principe de reconnaissance mutuelle des jugements et décisions judiciaires, sont inscrites dans le Programme de Stockholm et prévoient l'échange de données personnelles entre les États membres.

Le CEPD est conscient de l'importance de renforcer l'efficacité de la coopération judiciaire entre les États membres, notamment dans les domaines couverts par les initiatives sur la décision de protection européenne et la décision d'instruction européenne. Il souligne toutefois que le traitement des données personnelles, en particulière dans le domaine sensible que constitue l'espace de liberté, de sécurité et de justice (ELSJ), doit être en conformité avec les règles de l'UE sur la protection des données.

> ***« Une protection efficace des données personnelles est non seulement importante pour les personnes concernées, mais elle contribue aussi au succès de la coopération judiciaire. »*** ***Peter Hustinx, CEPD***

S'agissant des initiatives relatives à la décision de protection européenne et à la décision d'instruction européenne, le CEPD recommande:

- l'inclusion de dispositions spécifiques énonçant que les instruments sont applicables sans préjudice de la décision cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (décision 2008/977/JAI);

- l'inclusion de dispositions exigeant que les États membres s'assurent que:
  - les autorités compétentes ont les **ressources** nécessaires à l'application des directives proposées;

- les agents habilités satisfont à des **normes professionnelles** et sont soumis à des procédures internes appropriées garantissant le respect voulu des dispositions prévues en matière de **confidentialité** et de **secret professionnel**;
- **des systèmes d'authentification** permettent seulement un accès autorisé à chaque base de données contenant des données personnelles ou aux locaux où se trouvent les preuves;
- **le suivi des accès et des opérations** est effectué.

Dans une perspective plus générale, le CEPD réitère la nécessité d'un **cadre juridique global pour la protection des données** couvrant tous les domaines de compétence de l'UE, y compris la police et la justice, à appliquer aux données personnelles transmises ou mises à disposition par les autorités compétentes d'autres États membres, ainsi qu'au traitement intérieur dans l'ELSJ.

☞ Avis du CEPD (EN) (pdf)

> Avis du CEPD sur les systèmes de garantie des dépôts

Les systèmes de garantie des dépôts remboursent les dépôts aux déposants à hauteur de 100 000 EUR dans le cas où une institution de crédit fait faillite. Des règles européennes relatives à de tels systèmes existent depuis 1994. Elles ont été renforcées peu après l'apparition de la crise financière en 2008. Cet été, en juillet 2010, la Commission a avancé une autre proposition visant à simplifier et harmoniser les règles nationales correspondantes en la matière.

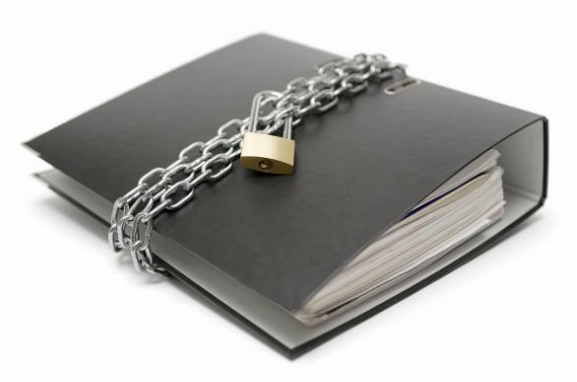
Le remboursement des dépôts via de tels systèmes de garantie exige de traiter les données des déposants. Les règles sur la protection des données sont donc applicables, pour autant que ces déposants soient des personnes physiques. Les données sont échangées entre un établissement de crédit et un système de garantie des dépôts, mais également entre les systèmes de garantie des dépôts au sein d'un État membre ou entre différents États membres.

Le 9 septembre 2010, le CEPD a publié un bref avis sur cette proposition et indiqué qu'il était généralement satisfait de la façon dont les aspects relatifs à la protection des données étaient traités dans la proposition. Par exemple, il est assuré dans la proposition que les données à caractère personnel ne seront utilisées qu'aux fins pour lesquelles elles sont échangées, à savoir le remboursement des dépôts.

Le CEPD a été particulièrement satisfait de voir que les données ne peuvent être utilisées que dans un format anonyme pour réaliser les «*stress tests*». Durant la phase de rédaction de la proposition, le CEPD s'était interrogé sur la nécessité d'utiliser des données personnelles pour effectuer de tels tests.

☞ Avis du CEPD (EN) (pdf)

> Document supplémentaire du CEPD relatif à l'accès du public aux documents et à la protection des données, après la décision dans l'affaire 'Bavarian Lager'



Le 29 juin 2010, la Cour européenne de justice a rendu sa décision dans l'affaire 'Bavarian Lager', une affaire qui a été suivie avec attention car considérée comme essentielle sur la question de la conciliation entre le droit fondamental à la protection des données personnelles et le droit fondamental d'accès du public aux documents (voir le numéro précédent de Newsletter du CEPD (pdf)).

En 2005, le CEPD a publié un document de référence sur le sujet intitulé «Accès du public aux documents et protection des données» (pdf), qui contenait des recommandations pour les institutions et organes de l'UE. Une partie de l'analyse présentée dans ce document de référence n'est plus valable à la lumière de la décision de la Cour. Le CEPD prépare donc actuellement un bref article supplémentaire sur le sujet, qui devrait être prêt pour la publication fin 2010.

Dans ce nouveau document, le CEPD mettra l'accent sur la nécessité d'une «approche proactive» en la matière. En bref, cela signifie que les institutions devraient indiquer clairement aux personnes concernées – avant, ou tout au moins au moment où elles collectent leurs données à caractère personnel – dans quelle mesure le traitement de ces données inclut ou pourrait inclure leur communication au public. La position du CEPD à cet égard est que les institutions sont obligées d'agir ainsi au titre des bonnes pratiques.

Une approche proactive réduira le nombre de situations dans lesquelles les institutions doivent décider de la communication au public dans le cadre d'une demande d'accès du public, comme dans l'affaire «Bavarian Lager». Le document supplémentaire fournira des conseils sur la façon de trouver un juste équilibre à la fois dans des situations proactives et réactives.

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.

>> Enquête sur les fraudes – Banque européenne d'investissement

Le 14 octobre 2010, le Contrôleur européen de la protection des données a publié un avis de contrôle préalable concernant les opérations de traitement des données qui se déroulent dans le contexte des procédures liées aux enquêtes de fraudes à la Banque européenne d'investissement (BEI) sur des allégations crédibles de pratiques frauduleuses dans des opérations financées par la BEI.

Pour mener des enquêtes, la division Enquêtes sur les fraudes de la BEI (IG/IN) a totalement accès à l'ensemble des membres du personnel concernés et à la totalité des informations, documents et

données pertinentes y compris les données électroniques au sein de la BEI. Au terme de l'enquête, le chef de la division IG/IN déterminera si une plainte ou allégation est dûment motivée et adressera l'affaire aux autorités compétentes au sein et/ou à l'extérieur de la BEI en vue d'une action appropriée. Si, après une enquête raisonnable, la division IG/IN détermine qu'une plainte ou une allégation n'est pas motivée, elle documentera les résultats dans une note relative au dossier et clôturera l'affaire.

Après un examen attentif de l'opération de traitement, le CEPD a émis un certain nombre de recommandations. Entre autres choses, le CEPD a recommandé l'adoption par la BEI d'un protocole officiel pour conduire les investigations numériques légales; préconisé l'harmonisation des périodes de conservation; et recommandé la fourniture d'informations aux personnes concernées conformément au règlement relatif à la protection des données.

☞ Avis du CEPD (EN) (pdf)

>> Traitement des données liées aux grèves – Banque centrale européenne

Le 28 septembre 2010, le CEPD a publié un avis de contrôle préalable concernant le traitement des données personnelles dans le cadre des retenues sur salaire en cas de grève à la Banque centrale européenne (BCE). Selon les règles applicables au personnel de la BCE, les membres du personnel ont le droit de faire la grève et, sauf décision contraire du conseil d'administration, la période totale de la grève sera déduite du paiement du salaire des membres du personnel participant à la grève. Dans la mesure où la participation à une grève entraîne automatiquement une déduction du salaire et d'autres rémunérations, le traitement des données personnelles liées à cette déduction est soumis au contrôle préalable du CEPD, car il implique une opération qui vise à exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat.

Après examen de la notification, le CEPD a formulé des recommandations notamment en ce qui concerne les périodes de conservation de tout document stocké dans le système de gestion des enregistrements et documents électroniques de la BCE, et les informations à fournir aux personnes concernées.

☞ Avis du CEPD (EN) (pdf)

>> Système européen de surveillance (TESSy) - Centre européen de prévention et de contrôle des maladies

Le 3 septembre 2010, le CEPD a publié un avis de contrôle préalable concernant les aspects liés à la protection des données de TESSy. TESSy est un outil de communication conçu pour assurer un échange rapide et efficace de données en matière de surveillance épidémiologique entre les États membres.

L'avis du CEPD explique que les données statistiques continueront d'être considérées comme des «données à caractère personnel» et seront par conséquent couvertes par le règlement relatif à la protection des données aussi longtemps que des personnes pourront être indirectement identifiées. Le simple fait que «des techniques d'anonymisation ont été utilisées» ne signifie pas que les données sont considérées comme étant «rendues anonymes» au sens du considérant 8 du règlement, et cessent donc d'être considérées comme des «données personnelles».

Dans son avis, le CEPD recommande également que les responsables du traitement et les sous-traitants soient clairement indiqués d'une façon qui corresponde au rôle effectif et au statut légal des

organisations concernées. Il convient de mentionner qui est responsable de quoi ainsi que la façon dont les personnes concernées peuvent exercer leurs droits. Le CEPD préconise aussi d'adopter une série de lignes directrices en matière de protection des données introduites dans TESSy. Parmi les autres recommandations figurent la fourniture d'informations complètes et accessibles aux personnes concernées sur le site web de l'opérateur, à laquelle devrait s'ajouter la diffusion d'une déclaration de protection des données par les points de contact des États membres conformément à leur législation nationale applicable en matière de protection des données. Une politique de sécurité spécifique devrait être adoptée dans les plus brefs délais afin de contribuer à garantir la sécurité de TESSy ainsi que de vérifier et de démontrer que le système est correctement administré.

☞ Avis du CEPD (EN) (pdf)

>> Inspections de sécurité – Commission européenne (CCR à Ispra)

Le 6 septembre 2010, le CEPD a adopté un avis de contrôle préalable concernant les inspections relatives à la sécurité au Centre commun de recherche à Ispra. Il concerne les opérations de traitement de données effectuées aux fins de maintenir et d'améliorer les normes de sécurité applicables.

Le CEPD a reconnu que la «*Procedura in caso d'infortunio*» implique le traitement de données relatives à la santé par plusieurs parties dans le but de réduire au minimum les conséquences et de prévenir des incidents de sécurité similaires sur le site d'Ispra.

En conséquence, le CEPD a publié des recommandations visant à garantir la limitation de la finalité du transfert des données, ainsi que la conformité aux principes de qualité des données applicables au stockage et à la poursuite du traitement des données personnelles dans ce contexte.

Une révision correspondante de la déclaration de confidentialité existante a été suggérée.

☞ Avis du CEPD (EN) (pdf)

> Mise en application

>> Politique de suivi de la conformité et de mise en application

Le CEPD élabore actuellement une politique de suivi de la conformité et de mise en application qui devrait être disponible d'ici fin 2010.

La politique décrira de quelle manière le CEPD entend suivre, mesurer et assurer la conformité au règlement (CE) n°45/2001 relatif à la protection des données. Elle expliquera également la nature des différents pouvoirs d'exécution à la disposition du CEPD, et soulignera les éléments moteurs et déclenchants de toute action formelle qui pourrait être entreprise. En encourageant la responsabilisation, la mise en conformité de manière volontaire et l'adoption des meilleures pratiques, la politique mettra largement l'accent sur la responsabilité, et s'efforcera de cibler les agences et institutions affichant les statistiques les plus médiocres en termes de conformité. Enfin, la politique définira également l'approche adoptée par le CEPD à l'égard de la transparence et de la publicité en rapport avec ses activités en matière de mise en application.

> 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.

>> Demande d'accès à l'identité d'un informateur – Médiateur européen

Le médiateur européen a consulté le CEPD sur une question soulevée dans le cadre d'une plainte déposée à l'encontre de l'Office européen de lutte antifraude (OLAF). La consultation a inclus un certain nombre de questions, à savoir notamment:

- si l'identité des personnes qui fournissent des renseignements à l'OLAF, en tant qu'informateurs ou dénonciateurs, ne devrait pas être divulguée à d'autres personnes que les autorités judiciaires;

- si la protection des informateurs et dénonciateurs doit aussi être garantie après la clôture d'une enquête classée sans suite et, le cas échéant, de quelle façon et dans quelles proportions.

Le CEPD a formulé des commentaires au niveau réglementaire ou politique, plutôt qu'au niveau de l'affaire. Dans cette perspective, le CEPD soutient la position suivante: en règle générale, l'identité d'un dénonciateur ou informateur ne devrait pas être divulguée, sauf lorsque cela enfreint les règles nationales sur les procédures judiciaires et/ou lorsqu'ils font une fausse déclaration dans l'intention de nuire. Dans ces cas, ces données personnelles pourraient être seulement divulguées aux autorités judiciaires.

S'agissant de la seconde question, on considère qu'il y a de bonnes raisons de penser que la protection des dénonciateurs et informateurs devrait être la même après la clôture d'une enquête, classée ou non sans suite. La vulnérabilité du rôle de dénonciateur ou d'informateur et, par conséquent, les risques pour leur vie privée et leur intégrité ne varient pas en fonction de la poursuite ou du classement d'une affaire.

Cette approche n'exclut pas bien sûr, dans la pratique, qu'il peut y avoir des situations où les demandes légitimes d'autres personnes seraient à privilégier par rapport à la protection des dénonciateurs et informateurs. Le temps qui passe peut s'avérer un facteur important dans ce contexte, mais il est de toute évidence difficile de spéculer sur une hypothèse.

☞ Avis du CEPD (EN) (pdf)

>> Transferts internationaux de données à caractère personnel - Agence européenne de la sécurité aérienne

L'Agence européenne de la sécurité aérienne (AESA) réalise des activités (par exemple, en matière de certification) qui donnent lieu au paiement de droits et de taxes par les demandeurs. Ces activités de certification peuvent être effectuées, partiellement ou totalement, en dehors du territoire des États membres. Dans certains cas, les candidats demandent à l'Agence de leur fournir les noms et la date de voyage des experts, afin de pouvoir procéder au paiement de la facture.

Le délégué à la protection des données de l'AESA a sollicité l'avis du CEPD sur l'application de l'article 9 du règlement relatif à la protection des données (Transfert de données à caractère personnel à des destinataires autres que les institutions et organes communautaires et ne relevant pas de la directive 95/46/CE) pour le cas en question.

Selon l'article 9.1 du règlement, le transfert de données à caractère personnel à des destinataires autres que les institutions et organes communautaires, et qui ne sont pas soumis à la législation nationale adoptée en application de la directive 95/46/CE, ne peut avoir lieu que pour autant qu'un niveau de protection adéquat soit assuré dans le pays du destinataire.

Le CEPD souligne que si le pays tiers en question – en dehors de l'EEE – n'assure pas un niveau de protection adéquat, d'autres conditions mentionnées à l'article 9 devraient être prises en compte. L'article 9, paragraphe 6, précise en effet que «par dérogation aux paragraphes 1 et 2, l'institution ou l'organe communautaire peut transférer des données à caractère personnel si: (...) (d) le transfert est nécessaire ou rendu juridiquement obligatoire pour des motifs d'intérêt public importants (...)».

Étant donné que la prestation des services décrits ci-dessus est l'une des principales activités de l'AESA, les transferts effectués pour le paiement de ces services pourraient être considérés, en principe, comme nécessaires pour le fonctionnement de cet organe, de façon à remplir les conditions exigées pour une dérogation au titre de l'article 9.6, alinéa (d).

Le CEPD note également que dans le cas présent, il s'agit apparemment de transferts ponctuels destinés à différents bénéficiaires de divers pays, et non pas de transferts «répétés, de masse ou structurels». Quant aux risques pour les personnes concernées, la lettre du DPD n'a fait état d'aucun risque spécifique. Les catégories de données à transférer (le nom et la date de voyage des experts en question) ne semblent pas non plus susciter d'inquiétude particulière.

Le CEPD souligne toutefois qu'aucune garantie n'est donnée dans les cas où une exception est appliquée. Pour cette raison, il recommande l'introduction d'une clause précisant que le bénéficiaire est légalement autorisé à demander ces données, et de limiter l'usage des données aux seules fins motivant leur transfert.

☞ Avis du CEPD (EN) (pdf)

EVENEMENTS

> Evénements à venir

>> Conférence de presse du CEPD sur l'avenir du cadre juridique de l'UE pour la protection des données (Bruxelles, 15 novembre 2010)

Le CEPD tiendra une conférence de presse le lundi 15 novembre 2010 sur l'avenir du cadre juridique de l'UE pour la protection des données. La conférence de presse fournira l'occasion d'entendre les perspectives du CEPD concernant la vaste révision imminente des règles de l'UE sur la protection des données et de la vie privée, et sur certains sujets dans des domaines connexes.

Le Contrôleur européen de la protection des données, Peter Hustinx, et son adjoint, Giovanni Buttarelli, évoqueront en particulier la récente communication de la Commission sur sa stratégie pour renforcer les règles de l'Union en matière de protection des données. Ils rappelleront les implications

d'une réforme qui aura un impact sur le développement d'une société de l'information où le droit fondamental des citoyens à la protection des données à caractère personnel devrait être assuré de manière efficace.

La conférence de presse offrira également l'occasion de présenter le rapport annuel 2009 du CEPD et de souligner les principales caractéristiques des activités menées en 2009 en ce qui concerne les tâches du CEPD en matière de supervision, de consultation et de coopération.

☞ Pour plus d'informations, veuillez contacter: press@CEPD.europa.eu

> Compte rendu d'événements passés

>> L'évènement de l'OCDE et la 32ème Conférence internationale des commissaires à la protection des données et à la vie privée (Jérusalem, 26-29 octobre 2010)

Au cours de la dernière semaine d'octobre 2010, deux grands évènements dans le domaine de la protection des données se sont déroulés à Jérusalem dans le cadre de la semaine d'activités sur le thème du respect de la vie privée, organisée par l'Organisation de coopération et de développement économiques (OCDE) et par l'ILITA, l'Autorité israélienne pour le Droit, l'Information et la Technologie.

L'évènement de l'OCDE, marquant le 30e anniversaire des lignes directrices de l'OCDE régissant la protection de la vie privée, a mis l'accent sur l'évolution du rôle des individus dans ce domaine. Ils ne sont plus de simples personnes concernées mais traitent eux-mêmes désormais activement des données personnelles, par exemple en participant à des réseaux sociaux. En outre, la technologie actuelle permet d'enregistrer tous les comportements humains, en garantissant qu'aucun élément ne soit oublié. Ce sont justement ces deux raisons qui incitent l'OCDE à envisager une révision de ses lignes directrices, vieillissantes.

La 32ème Conférence internationale des commissaires à la protection des données et à la vie privée, organisée par l'ILITA, a continué de travailler sur ces développements et sur les perspectives des différentes générations sur la protection des données et de la vie privée. La conférence s'est largement intéressée à la façon dont les lois et les mécanismes d'autorégulation influencent la technologie et vice versa. Là aussi, l'usage grandissant des réseaux sociaux a été au centre de cette conférence.

Au nom du CEPD, le Contrôleur Peter Hustinx, le Contrôleur adjoint Giovanni Buttarelli et la conseillère juridique Rosa Barcelo ont donné des présentations et présidé différentes sessions de la Conférence.

Lors de la session à huis clos des commissaires, diverses résolutions ont été adoptées, la principale concernant l'appel à organiser une conférence intergouvernementale afin d'élaborer un instrument international à caractère contraignant sur la vie privée et la protection des données personnelles.

La 33e Conférence internationale se déroulera au Mexique en novembre 2011.

☞ Plus d'information sur le site Internet de la conférence

>> Réunion des délégués à la protection des données (Londres, 15 octobre 2010)

Le 15 octobre 2010, le CEPD a tenu une réunion semestrielle avec les délégués à la protection des données des institutions et organes de l'Union européenne, dans les bureaux de l'Agence européenne des médicaments à Londres.

Après un tour d'horizon général des récentes évolutions dans le domaine de la protection des données, le CEPD a présenté une nouvelle structure et nouvel organigramme. Il a ensuite évoqué la politique de conformité et de mise en application qu'il compte finaliser d'ici la fin de l'année (voir la section Mise en application de cette newsletter). Il a également profité de l'occasion pour mettre en lumière les principaux points de son avis conjoint imminent sur le traitement des données liées à la santé dans les agences.

DISCOURS ET PUBLICATIONS

- La déclaration (pdf) de Peter Hustinx sur la réforme du règlement 1049/2001 relatif à l'accès du public aux documents, commission des pétitions, Parlement européen (Bruxelles, 9 novembre 2010)
- «Government access to private sector data», intervention (pdf) de Giovanni Buttarelli lors de la 32ème Conférence internationale des commissaires à la protection des données et à la vie privée (Jérusalem, 28 octobre 2010)
- «Promoting Dialogue Between NGOs and DPAs», notes d'allocution (pdf) de Giovanni Buttarelli à la réunion de la société civile de «Public Voice»: «Next Generation Privacy Challenges and Opportunities» [réunion tenue conjointement à la 32ème Conférence internationale des commissaires à la protection des données et à la vie privée (Jérusalem, 25 octobre 2010)]
- Notes (pdf) de Giovanni Buttarelli à la conférence sur le thème «Justice pénale en Europe: défis, principes et perspectives» (Luxembourg, 22 octobre 2010)
- Notes (pdf) de Peter Hustinx à la Table ronde de haut niveau sur «l'avenir de la protection des données à caractère personnel», Commission européenne (Bruxelles, 5 octobre 2010)
- Notes (pdf) de Giovanni Buttarelli à la Table ronde mensuelle de l'agenda Sécurité et défense sur le thème «Fine-tuning EU border security» (Bruxelles, 29 septembre 2010)
- Notes (pdf) de Giovanni Buttarelli à l'audition de la Commission des libertés civiles, de la justice et des affaires intérieures (LIBE) sur la lutte contre les abus sexuels, l'exploitation sexuelle des enfants et la pédopornographie, Parlement européen (Bruxelles, 28 septembre 2010)
- «Protection des enfants sur l'Internet», (pdf), article de Peter Hustinx publié dans Information Bulletin of Czech Office for Personal Data Protection, nr 1/2010, p. 1-2 (2 septembre 2010)
- «Privacy and data protection - legal lessons?», contribution du CEPD (pdf) («Expert Think Piece») à la conférence HiiL Law of the Future 2011 (30 juillet 2010)

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:

- M. Alfonso **SCIROCCO**, DPD, et M^e^ Sylvie **PICARD**, DPD adjoint – Contrôleur européen de la protection des données
- M. Alain **LEFÈBVRE**, Agence européenne des produits chimiques

☞ Voir la liste complète des DPD.

> Le CEPD nomme une nouvelle équipe de DPD

Le 1er septembre 2010, le CEPD a nommé une nouvelle équipe de DPD, composée d'Alfonso Scirocco, DPD, et de Sylvie Picard, DPD adjoint. Tous deux ont beaucoup d'expérience dans le domaine de la protection des données: Alfonso dans l'équipe de consultation et d'élaboration de politiques du CEPD, et Sylvie dans l'équipe de supervision.

Ces nominations montrent que le CEPD est désireux d'investir de nouvelles ressources et de l'énergie dans ce domaine afin de progresser rapidement vers un meilleur niveau de conformité.

La fonction de DPD au CEPD présente de nombreux défis: être indépendant au sein d'une institution indépendante, répondre aux attentes importantes des collègues qui sont particulièrement bien informés et sensibilisés aux questions de protection des données, et apporter des solutions qui peuvent servir de référence pour les autres institutions.

Les modalités d'application (pdf) reflètent ces spécificités, tout en tenant compte à la fois du document de référence du CEPD (pdf) et de l'article du réseau de DPD sur les normes professionnelles pour les délégués à la protection des données (pdf).

Une page DPD est désormais disponible sur le site Internet du CEPD; elle sera développée au cours du prochain mois en vue d'inclure de nouvelles fonctionnalités.

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 abonnez / désabonnez à cette newsletter sur notre site web.**

COORDONNEES
www.edps.europa.eu
Tel: +32 (0)2 283 19 00
Fax: +32 (0)2 283 19 50
NewsletterEDPS@edps.europa.eu

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