Le Contrôleur européen de la protection des données

Newsletter du CEPD

No 39 | Octobre 2013

DANS CE NUMÉRO

FAITS MARQUANTS

1 Enquête de la commission LIBE sur la surveillance électronique de masse des citoyens de l'UE

1 Frontières intelligentes: la proposition clé est coûteuse, insuffisamment justifiée et intrusive

SUPERVISION

1 BEI: enregistrement des conversations téléphoniques dans les salles de sécurité et au standard téléphonique

2 Vidéosurveillance: l'EFSA doit être vigilante sur la limitation des finalités et la portée

2 Le CEPD inspecte la vidéosurveillance dans les institutions de l'UE à Luxembourg

2 Contrôle de la sécurité et de la fiabilité au CCR

2 Demandes d'accès aux documents de la BCE – mise en équilibre des intérêts du personnel et du public

CONSULTATION

3 Le CEPD constate des lacunes importantes dans les propositions anti-blanchiment

3 Signe des temps: la protection des données doit faire partie intégrante de la protection des marques

3 En route vers la sécurité: les garanties en matière de protection des données doivent être appliquées

3 Services financiers: les règles de l'UE en matière de protection des données doivent être prises en considération

4 Vente de contrefaçons sur l'internet

4 Se préparer à un monde audiovisuel: le dispositif doit faire une place plus large à la protection des données

AFFAIRES JUDICIAIRES

4 Affaire devant la Cour: Commission européenne/Hongrie

4 Affaire devant la Cour: conservation des données

ÉVÉNEMENTS

5 Ateliers du CEPD sur l'utilisation des appareils mobiles sur le lieu de travail et les sites web

5 Conférence annuelle 2013 de l'ERA sur la législation européenne relative à la protection des données

DISCOURS ET PUBLICATIONS

DÉLÉGUÉS À LA PROTECTION DES DONNÉES

FAITS MARQUANTS

Enquête de la commission LIBE sur la surveillance électronique de masse des citoyens de l'UE

Les trois points les plus frappants dont nous avons connaissance à ce stade sont i) l'étendue de la surveillance en cours, ii) le nombre d'acteurs privés, notamment certains géants de l'internet bien connus, qui y ont apparemment pris part, activement ou passivement, et iii) le développement de failles et de portes dérobées dans le chiffrement, qui a des effets pervers de grande ampleur et porte gravement atteinte à la confiance du public.

Peter Hustinx lors de son audition à Strasbourg, 7 octobre 2013

Audition du CEPD (pdf)

Frontières intelligentes: la proposition clé est coûteuse, insuffisamment justifiée et intrusive

Il n'est pas clairement démontré que les propositions de la Commission visant à créer un système de **frontières intelligentes** pour les frontières extérieures de l'Union européenne atteindront l'objectif poursuivi, a déclaré le contrôleur européen de la protection des données (CEPD). À la suite de la publication de son avis du 18 juillet 2013, qui met en particulier l'accent sur le système **entrée/sortie**, le CEPD note que l'un des objectifs annoncés dans les propositions est de remplacer le système existant, «lent et peu fiable», mais que les propres estimations de la Commission ne permettent pas d'affirmer que la solution de rechange sera suffisamment efficace pour **justifier** la **dépense** et les **intrusions** dans la vie privée.

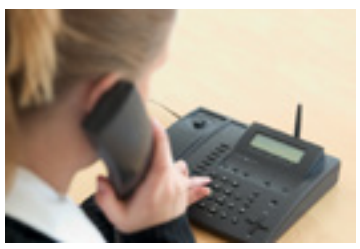
Améliorer la gestion des contrôles aux frontières est un exercice légitime. Mais il serait plus efficace de le faire lorsqu'une politique européenne claire de gestion des individus qui dépassent la durée du droit de séjour aura été établie. En l'absence d'une telle politique, la création d'une nouvelle base de données informatique pour stocker des quantités massives de données à caractère personnel est une réponse disproportionnée à un problème que d'autres systèmes créés récemment pourraient être à même de résoudre. Il serait prudent, d'un point de vue à la fois économique et pratique, d'évaluer les systèmes existants afin de garantir à tout le moins la cohérence et les bonnes pratiques

Peter Hustinx, CEPD

Avis du CEPD
Communiqué de presse du CEPD

SUPERVISION

BEI: enregistrement des conversations téléphoniques dans les salles de sécurité et au standard téléphonique



La Banque européenne d'investissement (BEI) souhaite enregistrer occasionnellement les appels entrants et sortants de son standard téléphonique pour des raisons de sécurité. Elle nous a donc notifié sa politique en la matière. Notre avis du 20 juin 2013 en vue d'un contrôle préalable sur l'enregistrement de ces appels comporte des recommandations sur l'établissement d'une base juridique plus claire, la réduction de la période de conservation et l'amélioration de l'information des appelants et du personnel du standard téléphonique.

Avis du CEPD en vue d'un contrôle préalable

European Investment Bank

Vidéosurveillance: l'EFSA doit être vigilante sur la limitation des finalités et la portée

Les lignes directrices en matière de vidéosurveillance, adoptées par le CEPD en 2010, font obligation aux institutions de l'UE d'avertir le CEPD lorsque leurs systèmes de vidéosurveillance comprennent des installations de haute technologie invasives pour la vie privée. Étant donné que l'Autorité européenne de sécurité des aliments utilise une technologie à infrarouges dans son système de vidéosurveillance, elle a notifié sa politique de vidéosurveillance au CEPD. Conformément aux lignes directrices précitées, notre avis a porté uniquement sur les pratiques de l'Autorité qui semblaient ne pas leur être conformes – il s'agissait en sorte d'un contrôle préalable restreint. Nous avons principalement recommandé la réalisation d'une analyse d'impact de l'utilisation de la technologie à infrarouges sur la protection des données. Nous avons également profité de l'occasion pour mettre en évidence d'autres aspects de la politique de vidéosurveillance de l'EFSA, notamment la nécessité de préciser l'étendue des lieux couverts par le système de vidéosurveillance afin de respecter la limitation des finalités définies par l'Autorité, à savoir les finalités de sécurité, et d'informer le grand public de sa politique de vidéosurveillance.

Avis du CEPD

Le CEPD inspecte la vidéosurveillance dans les institutions de l'UE à Luxembourg

Le rapport de suivi du CEPD de février 2012 sur l'état de la conformité des institutions et des organes de l'UE avec nos lignes directrices de 2010 en matière de vidéosurveillance décrit plusieurs mesures de suivi, notamment des inspections thématiques. Entre juin et juillet 2012, nous avons inspecté les locaux de treize institutions et organes de l'UE à Bruxelles. Les 9 et 10 juillet 2013, nous avons mené des inspections similaires dans les locaux de quatre institutions et organes de l'UE à Luxembourg.

Comme lors de l'exercice de 2012, notre priorité était d'examiner la manière dont les institutions et les organes de l'UE à Luxembourg informent le grand public de leur politique de vidéosurveillance, et notamment:

• l'affichage, le lieu et le contenu d'un avis sur place (pictogramme accompagné des informations écrites essentielles) indiquant que la zone est soumise à une surveillance;

• un avis détaillé sur la protection des données résumant les raisons et les modalités de la vidéosurveillance;

• une description des garanties et de la manière dont les individus peuvent exercer leurs droits;

• une politique en ligne sur la vidéosurveillance détaillant l'approche de l'institution ou de l'organe de l'UE concerné.

Les résultats de l'inspection menée sur place dans les institutions et organes de l'UE sont en cours d'examen.

Contrôle de la sécurité et de la fiabilité au CCR

Conformément aux recommandations du CEPD faisant suite à une inspection effectuée au Centre commun de recherche (CCR) d'Ispra fin 2010, le CCR a décidé de remplacer sa procédure de contrôle de sécurité, qui ne serait plus liée à ses procédures de recrutement mais à l'accès des individus aux zones nucléaires et aux zones sensibles connexes. Il serait par conséquent nécessaire de déterminer et de confirmer la fiabilité des personnes ayant besoin de bénéficier d'un accès non accompagné dans les zones précitées du CCR d'Ispra.

Dans notre avis du 19 juin 2013 sur le contrôle de fiabilité de sécurité des traitements du CCR, nous avons reconnu les obligations du site d'Ispra de mettre en œuvre les recommandations de l'Agence internationale de l'énergie atomique et du plan de protection physique approuvé par décret du ministère italien de l'industrie. Nous avons insisté pour que le CCR complète cette obligation légale par la nouvelle décision de la Commission sur la sécurité et par un protocole d'accord actualisé entre les services de sécurité de la Commission et le CCR d'Ispra. Nous avons en outre recommandé de revoir la période de conservation des données déjà collectées à la lumière du nouveau traitement et de garantir que les informations soient corrigées et fournies aux différents individus concernés.

Avis du CEPD

Demandes d'accès aux documents de la BCE – mise en équilibre des intérêts du personnel et du public

Le 20 septembre 2013, le CEPD a répondu à une consultation de la Banque centrale européenne (BCE) concernant l'accès du public à un registre créé dans le cadre du code éthique de la BCE sur les dons reçus par les membres de son personnel.

Compte tenu de la décision de la BCE sur l'accès du public à ses documents et des éléments du dossier, notre analyse a pris en considération l'arrêt rendu par la Cour de justice de l'Union européenne dans l'affaire *Bavarian Lager* et le document du CEPD sur *l'accès du public aux documents contenant des données à caractère personnel après l'arrêt rendu dans l'affaire* Bavarian Lager. Le CEPD a considéré la demande d'accès aux documents comme un transfert qui doit être conforme au règlement (CE) n° 45/2001. La BCE doit mettre en balance, d'une part, les intérêts du destinataire, pour établir la nécessité du transfert des informations, et d'autre part, les intérêts de l'institution, pour déterminer s'il y a lieu de penser qu'accorder l'accès aux données à caractère personnel d'un individu pourrait mettre en péril les intérêts légitimes de celui-ci.

La mise en balance des intérêts doit également tenir compte des catégories de personnel concernées: en effet, des exigences de transparence peuvent justifier la publication des données à caractère personnel de membres de l'encadrement ou de cadres supérieurs.

Nous avons conclu que la BCE doit évaluer la nature éventuellement publique du registre des dons et bien préciser aux personnes mentionnées dans le registre dans quelle mesure le traitement est susceptible d'être divulgué au public. Par conséquent, l'intéressé doit être informé avant la première divulgation de ses données à caractère personnel et avoir le droit de s'opposer à cette divulgation pour des raisons impérieuses et légitimes conformément au règlement de l'UE relatif à la protection des données.

Réponse du CEPD

CONSULTATION

Le CEPD constate des lacunes importantes dans les propositions anti-blanchiment

Les propositions de la Commission concernant une directive du Parlement européen et du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme et concernant un règlement sur les informations accompagnant les virements de fonds doivent aller plus loin qu'une simple référence à la protection des données.

Dans notre avis du 4 juillet 2013, nous avons reconnu qu'il est légitime d'assurer la transparence de l'origine des paiements d'argent, des dépôts de fonds et des transferts afin de lutter contre le terrorisme et le blanchiment d'argent, mais nous avons insisté pour que les exigences en matière de protection des données soient incorporées aux textes législatifs transposant les normes internationales au niveau de l'UE.

Nous notons avec satisfaction que les problèmes liés à la protection des données ont été soulevés par un grand nombre d'acteurs et qu'ils figurent dans l'analyse d'impact effectuée par la Commission. Nous regrettons toutefois que les propositions de directive et de règlement ne tiennent pas suffisamment compte de ces problèmes et qu'elles ne clarifient pas l'application des règles de l'UE en matière de protection des données aux traitements en question. Dans les textes proposés, aucune disposition de fond ne traite de ces questions.

Plus particulièrement, nous nous sommes inquiétés de la quantité importante de données à caractère personnel collectées au nom de la lutte contre le blanchiment et le terrorisme, notamment par les professionnels respectant leur obligation de diligence à l'égard de leur clientèle. Nous avons recommandé de respecter scrupuleusement le principe de limitation des finalités et de donner de plus amples directives aux professionnels quant aux données qu'ils sont autorisés ou non à collecter. Nous avons également souligné que les textes devraient préciser davantage le rôle des droits individuels et sensibiliser en particulier les professionnels et les clients. En outre, nous avons estimé que la limitation des droits des individus ne se justifie que lorsque sa nécessité est prouvée.

Compte tenu des transferts répétés, massifs et structurels de données à caractère personnel qui auront lieu en vertu de la directive et du règlement proposés, nous avons souligné les risques liés à ce type de transferts vers des pays tiers et recommandé d'intégrer des dispositions de fond spécifiques sur les transferts de données à caractère personnel, comme un critère de proportionnalité, afin de garantir une protection adéquate des individus lors du transfert de leurs données.

Par ailleurs, nous avons fait remarquer que les périodes de conservation des données devaient être justifiées. Nous avons également insisté sur le fait que la publication des sanctions infligées aux professionnels ne respectant pas les obligations qui leur incombent en vertu de ces textes doit être conforme au principe de proportionnalité.

Avis du CEPD

Communiqué de presse du CEPD

En route vers la sécurité: les garanties en matière de protection des données doivent être appliquées

Le 13 juin 2013, le CEPD a publié ses observations formelles sur deux projets de règlements de la Commission dans le domaine des systèmes de transport intelligents, soumis à l'examen du Parlement européen et du Conseil. Les projets d'instruments concernent la collecte et la fourniture de données à des services d'information sur la sécurité routière, l'un pour les informations sur le trafic général, l'autre sur les possibilités de stationnement pour les camions. Nous nous réjouissons d'avoir été consultés au cours du processus d'élaboration des projets de la Commission et de la prise en considération des aspects relatifs à la protection des données dans ceux-ci. À l'avenir, il est probable que les systèmes d'information sur le trafic routier utiliseront davantage des informations collectées par une multitude d'appareils mobiles installés dans les voitures ou portés par leurs conducteurs, comme les téléphones portables comportant des fonctions de localisation, les systèmes de navigation GPS connectés et d'autres systèmes de transport intelligents tels que les équipements de prise de vues capables de reconnaître les plaques d'immatriculation. Nous avons souligné l'importance de la protection des données lorsque la plupart des données collectées sur le trafic se rapportent à des personnes identifiées ou identifiables. Nous nous félicitons du fait que ces considérations sont prises en considération dans les règlements, mais avons expliqué que certaines garanties telles que l'anonymisation des données deviennent plus difficiles à mettre en œuvre lorsque des données plus précises sont collectées (d'après une *étude* sur les données de localisation, les individus peuvent être identifiés à partir d'un nombre très limité de données sur leur localisation, sans autre information). Par conséquent, la combinaison des données des systèmes d'information sur le trafic, notamment la réutilisation d'informations du secteur public (Open Data), doit toujours être effectuée en apportant les garanties appropriées en matière de protection des données.

Observations du CEPD

OFFICE FOR HARMONIZATION IN THE INTERNAL MARKET
(TRADE MARKS AND DESIGNS)

Signe des temps: la protection des données doit faire partie intégrante de la protection des marques

L'importance des marques est largement reconnue et leur protection garantie par le droit de l'Union. Une *marque* est un signe (comportant des éléments distinctifs tels que des mots, des logos, des éléments figuratifs, etc.) qui sert à distinguer les biens et services d'une organisation de ceux d'une autre. Les marques influencent les décisions des consommateurs au quotidien et, par conséquent, leur enregistrement est l'une des manières les plus efficaces de les protéger.

Le 11 juillet 2013, le CEPD a rendu un avis sur les propositions de la Commission concernant une directive rapprochant les législations des États membres sur les marques et un règlement modifiant le règlement sur la marque communautaire.

Dans notre avis, nous avons souligné que la collecte et le traitement de données à caractère personnel par les services centraux de la propriété industrielle dans les États membres et par l'Office de l'harmonisation dans le marché intérieur (OHMI) doivent être conformes à la législation applicable en matière de protection des données. Nous avons également recommandé d'établir clairement les modalités d'échange d'informations à travers des bases de données et des portails communs ou connectés, notamment en déterminant les destinataires autorisés à recevoir les données à caractère personnel, les types de données, les finalités de ces échanges et la durée de conservation des données dans ces systèmes informatiques. En outre, nous avons recommandé que si les échanges d'informations entre l'OHMI et les services nationaux comportent des données à caractère personnel, cet aspect soit clarifié, de même que les types de données concernées.

Avis du CEPD

Services financiers: les règles de l'UE en matière de protection des données doivent être prises en considération

«La proposition de directive de la Commission sur la comparabilité des frais est *liée aux comptes* de paiement, au changement de compte de paiement et à l'accès à un compte de paiement assorti de prestations de base

Les mesures sur la comparabilité des frais liés aux comptes de paiement permettent aux consommateurs d'avoir une vue d'ensemble complète des offres sur le marché, tandis que les mesures sur le changement de compte leur permettent de changer plus facilement de compte lorsqu'une meilleure offre est disponible. Tous ces éléments visent à renforcer la concurrence sur le marché des services financiers au bénéfice des consommateurs. Toutefois, pour garantir que le plus grand nombre possible de consommateurs puissent réellement profiter des avantages de ces améliorations, il est essentiel de faire en sorte que tout citoyen de l'UE ait le droit d'accéder aux prestations de base liées à un compte de paiement.

Dans nos observations formelles du 27 juin 2013 sur cette proposition, nous nous sommes félicités du fait que tout échange de données à caractère personnel du consommateur par les fournisseurs du service de paiement dans la phase de «changement» soit conditionné au consentement préalable, écrit et explicite, du consommateur. Nous avons également salué le fait que la proposition de directive rappelle spécifiquement le principe de nécessité lors du partage d'informations entre fournisseurs de services de paiement. Nous avons cependant souligné que la proposition devrait mentionner que la législation de l'UE en matière de protection des données reste pleinement applicable en ce qui concerne les obligations introduites par la directive.

Observations du CEPD

Vente de contrefaçons sur l'internet

Le 18 avril 2013, la Commission a publié un rapport sur le fonctionnement du protocole d'accord (MoU) concernant la vente de contrefaçons sur l'internet. Le rapport comporte une évaluation détaillée des meilleures pratiques et des mesures concrètes qui préviennent efficacement la vente de contrefaçons en ligne, protégeant ainsi les consommateurs à la recherche de produits authentiques sur le marché intérieur numérique. Le protocole d'accord a été rédigé à la suite d'un *dialogue* entre des entreprises et des associations commerciales représentant 39 sites internet différents, notamment les principales plates-formes de commerce électronique (comme eBay, Amazon, Allegro et Rakuten/PriceMinister).

Dans nos observations formelles du 11 juillet 2013, nous avons salué la publication de ce rapport, qui fournit des informations sur la manière dont les plates-formes électroniques parties prenantes au protocole ont mis en œuvre des procédures de notification et de retrait, mais aussi sur les mécanismes qu'elles ont mis en place pour coopérer et partager des informations – y compris les données à caractère personnel des contrevenants présumés – avec les titulaires des droits. Nous avons pris acte du rôle joué par la Commission pour reconnaître l'importance de ces problèmes et faciliter le dialogue entre les sociétés et les associations professionnelles afin de veiller à ce que toute mesure adoptée soit conforme au droit applicable et respecte pleinement les droits des individus à la vie privée et à la protection des données. Nous avons également exprimé le souhait d'être associés au dialogue en cours.

Observations du CEPD

Se préparer à un monde audiovisuel: le dispositif doit faire une place plus large à la protection des données

Le 24 avril 2013, la Commission a publié un *livre vert* intitulé *Se préparer à un monde audiovisuel totalement convergent: croissance, création et valeurs*. Le livre vert engage une consultation publique sur les implications de la transformation actuelle du paysage audiovisuel: les services audiovisuels ne sont plus fournis uniquement par des moyens traditionnels et par les radiodiffuseurs traditionnels, mais par des téléviseurs ou des ordinateurs de bureau ou portables connectés (souvent qualifiés d'«intelligents») ou par des tablettes et des appareils mobiles tels que les téléphones intelligents.

Dans nos observations du 30 août 2013, nous avons souligné que ces nouveaux modes de distribution et de consommation des œuvres audiovisuelles engendrent de nouvelles formes de collecte et de traitement des données à caractère personnel des utilisateurs. Ceux-ci ne comprennent pas toujours clairement que leur consommation d'œuvres audiovisuelles et leurs interactions avec les services connexes entraînent le traitement de leurs données à caractère personnel à différents niveaux du service fourni (par exemple, par leur appareil, leur FAI ou le radiodiffuseur), ni dans quelle mesure un tel traitement a lieu, de sorte que les utilisateurs ne contrôlent plus leurs données.

Nous pensons que tout choix politique dans ce domaine doit respecter pleinement le cadre juridique de l'UE en matière de protection des données. Nous avons notamment souligné qu'une *transparence intégrale* doit être garantie aux utilisateurs quant aux types de données à caractère personnel qui sont collectées et aux personnes qui les recueillent, que le consentement de l'utilisateur doit être obtenu, le cas échéant, avant de traiter ses données et qu'une attention particulière doit être accordée à la *protection de la vie privée et aux données à caractère personnel d'enfants*, notamment dans le domaine de la publicité. Des outils techniques devraient aider à protéger la vie privée et les données à caractère personnel des enfants, notamment pour ce qui est de la configuration du service et du terminal de l'utilisateur.

Observations du CEPD

AFFAIRES JUDICIAIRES

Affaire devant la Cour: Commission européenne/Hongrie

Lors d'une audience devant la Cour de justice de l'Union européenne le 15 octobre 2013, le CEPD a soutenu la position de la Commission européenne dans l'affaire C-288/12, *Commission/Hongrie*.

Le 1er janvier 2012, une nouvelle constitution est entrée en vigueur en Hongrie, en vertu de laquelle une nouvelle autorité chargée de la protection des données a été créée et le mandat du directeur de l'autorité existante a pris fin. Le CEPD a fait valoir que la Hongrie n'avait pas garanti une indépendance d'action totale à l'autorité nationale chargée de la protection des données, comme l'article 28 de la directive 95/46/CE l'exige. Il a également soutenu que le mandat du directeur de l'autorité doit être protégé de manière à ce qu'il n'y soit pas mis fin prématurément sans justification adéquate et sans les garanties procédurales appropriées. Des dispositions transitoires adéquates auraient dû être prévues. En outre, une modification de la législation ne peut justifier en soi une cessation prématurée du mandat.

Les conclusions de l'avocat-général Wathelet sont attendues pour le 10 décembre.

Il s'agit de la troisième affaire portée devant la Cour au sujet de l'indépendance des autorités nationales chargées de la protection des données. Veuillez lire nos précédents articles sur les affaires *Commission/Allemagne* et *Commission/Autriche*.

Plaidoirie du CEPD

Affaire devant la Cour: conservation des données

Le 9 juillet 2013, le CEPD a présenté des observations orales à l'audience devant la grande chambre de la Cour de justice dans les demandes jointes de décision préjudicielle C-293/12 et C-594/12, *Digital Rights Ireland et autres*. Ces deux affaires concernent la validité de la directive 2006/24/CE sur la conservation des données. C'est la première fois que la Cour a décidé, sur la base de l'article 24 de ses statuts, d'inviter le CEPD à une audience (dans une procédure de décision préjudicielle) afin de répondre à certaines questions spécifiques. Dans sa plaidoirie, le CEPD a souligné la nécessité d'opérer une distinction entre l'article 7 (*respect de la vie privée et familiale*) et l'article 8 (*protection des données à caractère personnel*) de la Charte des droits fondamentaux de l'UE. Si ces deux dispositions sont bien entendu étroitement liées, leur nature est différente. Par conséquent, lorsqu'elle statue sur la validité des actes juridiques adoptés en vertu de la Charte, la Cour doit procéder à un double contrôle, en évaluant si les exigences distinctes des articles 7 et 8 sont respectées. L'avocat général P. Cruz Villalón présentera ses conclusions le 7 novembre 2013.

Plaidoirie du CEPD

ÉVÉNEMENTS

Ateliers du CEPD sur l'utilisation des appareils mobiles sur le lieu de travail et les sites web

Le 19 septembre 2013, nous avons organisé deux ateliers sur l'utilisation des appareils mobiles sur le lieu de travail et les sites web gérés par les institutions et organes de l'UE. Plus de 60 participants ont assisté à chaque atelier, notamment des délégués à la protection des données (DPD), des coordinateurs de la protection des données (CPD) et des experts en informatique et en communication. Avant la réunion, nous avions demandé à ces collègues des institutions de l'UE de participer à notre enquête et de faire part de leurs propres pratiques. Nous avons ainsi obtenu des informations spécifiques précieuses sur les expériences et les opinions en la matière, qui ont été ensuite débattues, comme l'utilisation de témoins de connexion (cookies) et d'appareils mobiles privés sur le lieu de travail.

Il s'agissait là de la deuxième édition d'une série d'ateliers qui nous aideront à formuler des lignes directrices sur ces questions et d'autres liées aux technologies, comme l'utilisation des communications électroniques sur le lieu de travail et l'informatique en nuage, qui sont en cours d'élaboration. Les discussions menées dans les ateliers confirment la nécessité d'une approche commune pour protéger les données à caractère personnel et confirment que les institutions et les organes de l'UE ont intérêt à échanger leurs expériences sur les bonnes pratiques en matière de protection des données, surtout dans des domaines aussi complexes qui évoluent rapidement.

Conférence annuelle 2013 de l'ERA sur la législation européenne relative à la protection des données

Les 18 et 19 novembre 2013, l'Académie de droit européen (ERA) établie à Trèves tiendra sa conférence annuelle sur la législation européenne relative à la protection des données. La conférence de cette année se focalisera sur le rôle des services d'informatique en nuage et des réseaux sociaux dans l'application du droit de l'UE en matière de protection des données. Ce sera aussi l'occasion d'informer les participants sur l'état d'avancement de la réforme de la législation de l'UE relative à la protection des données et sur la jurisprudence la plus récente de la Cour de justice de l'UE. Le panel d'orateurs distingués sera composé d'avocats, de défenseurs de la vie privée, d'universitaires, de représentants de la Commission européenne et du CEPD, ainsi que de Peter Hustinx, qui prononcera une allocution majeure. Comme les principaux thèmes porteront sur la souveraineté de l'UE en matière de données, le transfert transfrontalier de données à des pays tiers ainsi que PRISM et la protection des données, les discussions seront probablement animées.

Programme de la conférence

DÉLÉGUÉS À LA PROTECTION DES DONNÉES

Nominations récentes

- M[me] Christina Karakosta, par intérim, Médiateur européen, depuis le 15 octobre 2013.

DISCOURS ET PUBLICATIONS

- Contribution (*pdf*) de Peter Hustinx lors de l'enquête de la Commission LIBE sur la surveillance électronique de masse des citoyens de l'Union européenne, audience publique, Strasbourg (7 octobre 2013).
- Conclusions (*pdf*) de Peter Hustinx lors de la 35[e] conférence internationale des commissaires chargés de la protection des données et de la vie privée, Vie privée: une boussole dans un monde turbulent, Varsovie (23-26 septembre 2013).
- Discours d'orientation (*pdf*) de Peter Hustinx lors du Digital Enlightenment Forum, *Données à caractère personnel et citoyenneté dans la société numérique*, Bruxelles (19 septembre 2013).
- *Interaction (future) entre les autorités chargées de la protection des données et les institutions de défense des droits de l'homme*, article (*pdf*) de Peter Hustinx publié dans *National Human Rights Institutions in Europe – Comparative, European and International Perspectives*, Jan Wouters et Katrien Meuwissen (éd.), Cambridge 2013, pp. 157-172 (17 juillet 2013).
- *Une période intéressante pour la protection des données en Europe*, éditorial (*pdf*) de Peter Hustinx paru dans *L'Observateur de Bruxelles*, n° 93, pp. 5-6 (15 juillet 2013).

À propos de cette newsletter

Cette newsletter 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 à caractère personnel dans les institutions et organes de l'UE;
- conseiller les institutions européennes sur la législation en matière de protection des données;
- coopérer avec les autorités similaires afin de promouvoir la cohérence de la protection des données à caractère personnel.

Vous pouvez vous abonner à cette newsletter ou vous en désabonner sur notre web

COORDONNÉES

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

ADRESSE POSTALE

CEPD
Rue Wiertz 60 – Bât. MTS
B-1047 Bruxelles
BELGIQUE

ADRESSE BUREAUX

Rue Montoyer 30
B-1000 Bruxelles
BELGIQUE

Suivez-nous sur Twitter: @EU_EDPS

CEPD – Le Contrôleur européen de la protection des données

QT-AC-13-002-FR-N