



## CONSULTATION

- > Renforcement de la proposition relative au plan d'action pour la santé en ligne du point de vue de la protection des données.....3
- > Garanties plus concrètes nécessaires en matière de protection des données pour les procédures d'insolvabilité .....3
- > L'intégration des principes de protection des données dès la phase de conception doit figurer dans la stratégie numérique .....4
- > La limitation des données personnelles favorisera l'établissement des comptes rendus d'événements dans l'aviation civile.....5
- > La proposition en matière d'équipement hertzien doit être peaufinée.....5
- > Équilibrer vie privée des investisseurs et transparence réglementaire .....6



## SUPERVISION

- > Des garanties plus rigoureuses pour la protection du JRC .....7
- > EACI: analyse et transfert d'informations frauduleuses à l'OLAF.....7
- > Renforcement nécessaire des contrôles de conformité en matière de lutte contre le blanchiment d'argent et le financement d'activités terroristes .....8
- > Mesures à prendre: il convient que l'ERA modifie radicalement sa politique en matière de messagerie électronique .....8
- > Aider à recadrer la politique de surveillance d'Internet.....9



## EVENEMENTS

- > ICO: le bureau du commissaire à l'information (Royaume-Uni) se félicite des avancées des réformes envisagées pour l'Union européenne .....9
- > Formation des délégués à la protection des données (DPD) à Bruxelles.....10
- > Rencontre des DPD, Lisbonne.....10
- > Table ronde du CEPD: train de mesures sur les frontières intelligentes et leurs implications sur la protection des données .....11
- > Réunion du groupe de coordination du contrôle du VIS.....12
- > Réunion de coordination du contrôle EURODAC.....12



## DISCOURS ET PUBLICATIONS



## NOUVEAUX DELEGUES A LA PROTECTION DES DONNEES

## - FAITS MARQUANTS -

### Dernières informations concernant la réforme de la réglementation en matière de protection des données

Le 15 mars 2013, le CEPD a transmis au Parlement, à la Commission et au Conseil européens des observations complémentaires sur la réforme de la législation européenne en matière de protection des données. Nos observations portaient sur des points spécifiques qui demandaient à être clarifiés et répondaient aux amendements proposés par les commissions compétentes du Parlement européen.

Dans nos observations, nous avons réaffirmé que les données pseudonymisées demeurent des données à caractère personnel dont la protection s'impose. Les définitions des données anonymes ou pseudonymisées doivent, par conséquent, être en parfaite adéquation avec la définition des

données à caractère personnel et ne pas exclure certaines catégories de données personnelles du champ d'application de la protection des données. Nous avons également déconseillé l'exclusion de certains secteurs du champ d'application du cadre européen relatif à la protection des données et la restriction du périmètre territorial de la législation générale proposée en matière de protection des données. Nous sommes favorables aux amendements supprimant la possibilité globale d'un traitement supplémentaire à des fins incompatibles et avons insisté sur le fait que la définition d'un consentement explicite devait être maintenue.

Nous soutenons également la définition et les responsabilités des responsables et préposés au traitement des données telles que proposées par la Commission, ainsi que le principe de responsabilité, qui doit s'appliquer à l'ensemble de ce train de mesures. Si nous sommes d'accord avec certains éléments de l'«approche fondée sur les risques», nous avons néanmoins souligné que la protection complète prévue par le règlement doit s'appliquer à l'ensemble des opérations de traitement et pas uniquement aux plus risquées. Nous avons également demandé davantage de mesures d'incitation concernant le recours aux délégués à la protection des données. Concernant les transferts internationaux, nous prônons une clarification du règlement et nous félicitons des amendements qui introduisent un nouvel article sur les transferts interdits au regard du droit européen.

Pour ce qui est de la proposition de directive sur la protection des données en matière d'application du droit pénal, nous soutenons les amendements qui tendent à une meilleure adéquation de la directive et du règlement à des fins d'harmonisation. Nous nous félicitons également des amendements qui introduisent des conditions et garanties spécifiques concernant l'accès des données initialement traitées à d'autres fins par les autorités chargées de l'application du droit. Nous avons également souligné que la diffusion des données à des services non répressifs ou à des tiers doit être strictement limitée.

☞ Communiqué de presse du CEPD ([pdf](#)) et observations ([pdf](#))

## Formation sur mesure à l'ETF

La promotion d'une culture de protection des données au sein des institutions et organes de l'Union européenne figure parmi les objectifs stratégiques du CEPD. A cette fin, nous avons coordonné plusieurs formations et activités de sensibilisation. Nous avons ainsi poursuivi notre coopération avec le réseau de délégués à la protection des données (DPD) en proposant une session de formation dans nos bureaux le 17 avril 2013 et avons participé à la rencontre bi-annuelle réunissant le CEPD et le réseau de DPD, et qui s'est tenue à Lisbonne. Pour en savoir plus, consultez notre section Événements.



Le 25 février 2013, dans le cadre de nos activités de sensibilisation, nous avons suivi une journée de formation sur la protection des données que nos collègues des services de supervision et d'application des textes, et de réglementation en matière de technologies de l'information du CEPD ont dispensée dans leurs locaux de la Fondation européenne pour la formation (ETF) à Turin (Italie).

Parallèlement à une présentation du rôle du CEPD, nous avons proposé une étude de cas et avons, à la demande de l'ETF, organisé des sessions portant sur des problèmes spécifiques comme les droits des personnes, les questions liées aux ressources humaines et les problèmes relatifs aux marchés publics.

Cette formation a constitué un excellent terrain d'échange, notamment sur la mise en œuvre pratique de nos orientations, et a permis au personnel du CEPD de tirer parti des expériences d'une agence.

Nous sommes très heureux que cette formation ait répondu aux attentes de l'ETF. Dans un souci d'efficacité et d'efficience, nous envisageons de proposer des formations du même genre aux autres agences, notamment par vidéoconférences.



## CONSULTATION

### > Renforcement de la proposition relative au plan d'action pour la santé en ligne du point de vue de la protection des données



Dans notre avis du 27 mars 2013 sur la communication de la Commission «Plan d'action pour la santé en ligne 2012-2020 – des soins de santé innovants pour le XXIe siècle», nous nous sommes félicités de l'attention portée à la protection des données dans cette communication. Cependant, les informations personnelles traitées dans le cadre de la santé en ligne et du bien-être au moyen d'applications et de solutions TIC (technologies de l'information et des communications), sont souvent des données ayant trait à la santé qui imposent un niveau de

protection accru. Nous demandons instamment à cette industrie, aux États membres et à la Commission d'examiner avec la plus grande attention les implications en matière de protection des données qui peuvent naître de la mise en œuvre de programmes dans le domaine de la santé en ligne. Nous recommandons, par ailleurs, que la Commission consulte le CEPD avant de prendre toute autre mesure législative ou non comme indiqué dans la communication.

☞ Avis du CEPD ([pdf](#))

### > Garanties plus concrètes nécessaires en matière de protection des données pour les procédures d'insolvabilité

Dans notre avis du 27 mars 2013 sur la proposition de la Commission en faveur d'une modification du règlement (CE) No 1346/2000 du Conseil relatif aux procédures d'insolvabilité, nous avons salué les références faites à l'applicabilité de la législation européenne en matière de protection des données.

Nous recommandons toutefois une plus grande clarté des dispositions de fond concernant les modalités d'application concrètes des principes de protection des données aux procédures d'insolvabilité, notamment en ce qui concerne les informations échangées entre parties prenantes qui sont parfois également publiées.

Nous avons exprimé nos inquiétudes concernant la publication des informations relatives à l'ouverture et à la clôture des procédures d'insolvabilité dans les registres afférents, librement accessibles sur Internet.

Nous reconnaissons que la volonté d'encourager la transparence et la communication entre les parties prenantes est légitime. Cependant, nous estimons que ce mode de publication engendre des risques spécifiques et porte atteinte à la vie privée. Nous avons souligné que la proportionnalité de cette mesure n'était pas prouvée puisque, contrairement ce que conseille la décision Schecke, aucune alternative, à savoir aucun autre mode de publication entravant moins les droits de leurs bénéficiaires en matière de vie privée, n'a été envisagée.

Entre autres choses, nous conseillons que des responsables du traitement des données soient désignés, que les mises à jour des données échangées ou publiées soient organisées, que la période de conservation des données traitées soit spécifiée et que des procédures soient mises en place afin d'informer les personnes du traitement de leurs informations personnelles.

☞ Avis du CEPD ([pdf](#))

## > L'intégration des principes de protection des données dès la phase de conception doit figurer dans la stratégie numérique

Dans sa communication sur *Une stratégie numérique pour l'Europe: faire du numérique un moteur de la croissance européenne*, la Commission a identifié plusieurs domaines politiques sur lesquels elle souhaite concentrer ses efforts afin de favoriser et de stimuler le développement de l'économie numérique: le marché unique du numérique, l'offre et la demande de l'Internet ultrarapide, l'informatique en nuage, et la confiance et la sécurité.



Dans notre avis du 10 avril 2013, nous insistons sur le fait que la conception et le déploiement de nouvelles applications et solutions ICT (technologies de l'information et des communications) pour l'environnement numérique doivent respecter les principes de protection des données, étant donné que la recommandation d'intégration des principes de protection des données dès la phase de conception prendra un caractère obligatoire en vertu de la proposition de règlement sur la protection des données. Nous avons également rappelé à la Commission que l'usage de l'interopérabilité dans le but de favoriser le partage de données entre bases de données doit s'appuyer sur une base juridique adéquate et sur des garanties appropriées en matière de protection des données.

En matière d'informatique en nuage, nous nous sommes référés aux nombreuses orientations portant sur l'application du droit actuel dans le domaine de la protection des données et sur l'incidence de la proposition de réglementation en la matière qui ont été proposées par les autorités de protection des données et par le CEPD. Nous demandons instamment à la Commission de s'appuyer sur ces orientations afin d'inciter les personnes et les consommateurs à s'impliquer dans ces nouvelles technologies dans la mesure où ils en garantiront à leur tour le bon déploiement.

☞ Avis du CEPD ([pdf](#))



## > La limitation des données personnelles favorisera l'établissement des comptes rendus d'événements dans l'aviation civile

La proposition de règlement de la Commission sur l'établissement de comptes rendus des événements dans l'aviation civile vise à améliorer les systèmes existants en la matière dans ce secteur tant sur le plan national qu'europpéen. Par «événement», on entend tout événement susceptible de porter atteinte à la sécurité aérienne, notamment les accidents, défauts, défaillances et les autres problèmes liés à l'exploitation des avions. Afin d'établir des comptes rendus plus complets et de meilleure qualité, la proposition insiste, entre autres choses, sur l'utilisation d'un système de déclaration volontaire complétant le système obligatoire et encourage les organisations, et pas seulement les États membres, à établir des comptes rendus sur les événements. La proposition offre également une protection harmonisée contre les sanctions hiérarchiques ou la poursuite des personnes signalant de tels événements, et tend à assurer un accès adéquat aux informations stockées dans la banque de données centrale européenne.

Dans notre avis du 10 avril 2013, nous avons salué l'attention que porte cette proposition à la protection des données à caractère personnel, plus particulièrement au travers de l'engagement pris pour *dépersonnaliser* une majeure partie des données traitées. Nous avons toutefois souligné que la proposition revient, au mieux, à une anonymisation partielle et que les données traitées demeureront des données à caractère personnel soumises à la législation européenne en matière de protection des données. Nous souhaitons donc que plusieurs points de ce texte soient clarifiés pour favoriser au plus vite une meilleure protection des données et leur anonymisation complète. Nous souhaitons également que le responsable des différentes bases de données soit clairement identifié, que les durées de stockage des données dans les bases de données soient précisées, que les droits des personnes et les mesures de protection à mettre en œuvre soient précisés. Nous recommandons également que des garanties supplémentaires soient prises pour le transfert des données vers des pays tiers et en matière de traitement des données sensibles.



☞ Avis du CEPD ([pdf](#))

## > La proposition en matière d'équipement hertzien doit être peaufinée

La proposition de la Commission pour une directive harmonisant les législations des États membres sur la disponibilité des équipements hertziens sur le marché remplacera la directive 1999/5/CE concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité (appelé directive R&TTE).

Hormis quelques exceptions, tous les équipements utilisant les ondes hertziennes ou des fréquences de télécommunication entreraient dans le champ d'application de ces règles, notamment les voitures équipées de cartes SIM (comme le dispositif embarqué [eCall](#), dont nous avons parlé dans notre dernière newsletter) et qui exploitent des équipements hertziens. Etant donné que cette technologie permet de géolocaliser un véhicule (et donc, un individu), son utilisation n'est pas sans incidence sur la vie privée des personnes.

Dans nos observations formelles du 27 février 2013, nous avons fait remarquer que la directive R&TTE incitait les fabricants de tels équipements à appliquer l'intégration des principes de protection

des données dès la phase de conception. Nous sommes, par conséquent, heureux de constater que la proposition s'appuie sur l'approche de ladite directive en termes de respect de la vie privée et de protection des données, ces deux notions demeurant essentielles pour la conception de tout équipement hertzien. Nous saluons également le fait que la proposition oblige clairement les fabricants à s'assurer que les équipements hertziens commercialisés ont été conçus et fabriqués de manière à intégrer, entre autres choses, des garanties visant à assurer la protection des données à caractère personnel et de la vie privée des consommateurs.

Nous regrettons, toutefois, que les équipements de terminaux fixes échappent désormais au champ d'application de la directive, ce qui a pour conséquence de limiter les incitations existantes visant à favoriser l'intégration des principes de protection des données dès la phase de conception de ces équipements. Ce point est particulièrement regrettable dans la mesure où les équipements terminaux jouent un rôle de plus en plus important en matière de protection de la vie privée et qu'il n'existe actuellement aucun règlement équivalent en matière de protection des données personnelles et le respect de la vie privée dans les autres instruments législatifs applicables aux équipements terminaux non hertziens. Nous recommandons, par conséquent, que la Commission s'engage dans le cadre de cette proposition à superviser la conformité des équipements terminaux avec les exigences en matière de protection des données et de respect de la vie privée, et qu'elle envisage des mesures appropriées, le cas échéant.

↳ Observations du CEPD ([pdf](#))

## > Équilibrer vie privée des investisseurs et transparence réglementaire

Dans son plan d'action Droit européen des sociétés et gouvernance d'entreprise relatif à l'équilibrage de la confidentialité des investisseurs et la transparence et surveillance réglementaires, la Commission dévoile ses projets pour moderniser le droit des sociétés et le cadre de gouvernance d'entreprise en Europe.



Dans notre lettre du 27 mars 2013, nous avons rappelé à la Commission que les propositions de loi visant à *accroître la visibilité* des participations doivent tenir dûment compte des droits des actionnaires à protéger leurs informations personnelles. Les décideurs doivent évaluer et articuler avec le plus grand soin les objectifs des politiques publiques qui renforcent cette visibilité, et les équilibrer au regard des risques pesant sur les droits des actionnaires au respect de leur vie privée.

Le *renforcement de la surveillance des politiques de rémunération par les actionnaires* est un autre point de la proposition pour lequel la transparence doit être adaptée aux droits des individus en matière de respect de leur vie privée et de protection de leurs données personnelles. En ce qui concerne la divulgation des données à caractère personnel, nous encourageons l'examen d'autres méthodes, modalités et niveaux de granularité afin que les mesures adoptées soient parfaitement adaptées aux différents cas autorisant la libre consultation des informations sur la rémunération des membres de la direction/des conseils de surveillance.

↳ Lettre du CEPD ([pdf](#))



## SUPERVISION

### > Des garanties plus rigoureuses pour la protection du JRC

Le 19 mars 2013, nous avons adopté un avis sur le traitement des opérations menées dans le cadre des enquêtes de sécurité au centre commun de recherche (JRC) de Petten.

Nous avons examiné cette notification au regard de la révision de la décision de la Commission sur la sécurité qui définit les tâches générales du service de sécurité et l'adoption prochaine d'un protocole d'accord entre la Direction générale des ressources humaines et de la sécurité de la Commission européenne et le JRC afin de mener certains types d'enquêtes de sécurité.

L'opération de traitement a pour but d'obtenir des informations sur les incidents de sécurité comme les accidents de la route, les violations de stationnement et le vandalisme qui sont intervenus dans les installations du JRC de Petten, et qui seront à terme répertoriés dans un rapport décrivant l'événement.

Nos principales préoccupations face à ce traitement portent sur l'utilisation des données transférées par leurs destinataires, notamment des institutions ou organes de l'Union européenne ou autorités nationales (policières ou judiciaires, par exemple). Nous avons donc proposé qu'une information sur la limitation des objectifs soit fournie aux destinataires. Nous avons également insisté sur la nécessité d'évaluer et de documenter dûment tout transfert d'informations avant sa réalisation.

☞ Avis du CEPD ([pdf](#))

### > EACI: analyse et transfert d'informations frauduleuses à l'OLAF



Le traitement réalisé par l'Agence exécutive pour la compétitivité et l'innovation (EACI) a pour but d'analyser et de transférer des informations à l'Office européen de lutte antifraude (OLAF) dans les cas de fraudes et d'irrégularités financières présumées dans la gestion des fonds de l'Union européenne. L'EACI a été la première agence à soumettre une notification dans ce domaine au CEPD.

Dans notre avis de contrôle préalable, nous avons insisté sur la nécessité de définir une période de conservation des données personnelles adaptée dans les cas non transmis à l'OLAF. Nous avons également insisté sur le fait que seules les données strictement nécessaires doivent être transférées au destinataire adéquat sur la base de la réalisation légitime de leurs tâches et sur le fait que l'EACI se doit de garantir un droit d'accès et de rectification aux personnes dont les informations sont conservées, notamment aux dénonciateurs, informateurs ou témoins, en précisant les limites prévues à l'article 20 du règlement.

☞ Avis du CEPD ([pdf](#))

## > Renforcement nécessaire des contrôles de conformité en matière de lutte contre le blanchiment d'argent et le financement d'activités terroristes

La proposition de la Banque européenne d'investissement visant à appliquer des contrôles de lutte contre le blanchiment de capitaux et le financement du terrorisme a pour objectif d'appliquer les meilleures pratiques bancaires dans ce domaine et de réduire les risques en termes d'intégrité et de réputation.



Dans notre avis de contrôle préalable, nous avons instamment demandé à la Banque européenne d'investissement de renforcer le socle juridique existant. Nous avons également insisté sur la nécessaire introduction d'un certain nombre de garanties afin d'améliorer la qualité des données personnelles traitées. Les informations de cette nature ne présentant aucun intérêt pour l'objectif sous-jacent ne doivent par conséquent pas être traitées. Les rumeurs, articles de presse et autres allégations non vérifiés doivent être traités avec la plus grande prudence. Enfin, la Banque européenne d'investissement doit mettre en place des procédures afin de vérifier que les informations utilisées sont exactes et à jour.

☞ Avis du CEPD ([pdf](#))

## > Mesures à prendre: il convient que l'ERA modifie radicalement sa politique en matière de messagerie électronique



En réponse à une notification pour un contrôle préalable émise par l'Agence ferroviaire européenne (ERA), nous avons procédé à un examen minutieux de la politique de surveillance des messageries électroniques de cet organe afin de l'aider à prévenir les interruptions et utilisations erronées causées par le personnel, et avons insisté sur la nécessité d'apporter des modifications dans un certain nombre de domaines.

Nous avons mis l'ERA en garde contre le fait que la surveillance des messageries électroniques doit être nécessaire et proportionnée, et qu'elle doit, en priorité, être automatisée et anonyme. L'examen de messages électroniques comportant l'identification de l'utilisateur doit être réservé aux seuls cas pour lesquels il existe une suspicion raisonnable d'irrégularités corroborée par une première preuve concrète; il doit, en outre, être mené dans le cadre d'une enquête administrative.

Entre autres choses, nous avons également invité l'ERA à exclure les comptes de messagerie personnels du champ d'application des politiques en matière de messagerie électronique et à exclure, ou tout au moins limiter considérablement, le droit de l'ERA à intervenir dans les communications personnelles.

☞ Avis du CEPD ([pdf](#))



## > Aider à recadrer la politique de surveillance d'Internet

La surveillance électronique opérée par l'Agence ferroviaire européenne (ERA) a pour but de vérifier si l'utilisation qui est faite d'Internet est conforme aux critères définis dans ses documents de politique interne.

Dans notre avis de contrôle préalable, nous avons appliqué l'analyse et les orientations proposées dans nos précédents avis.

Nous avons alors signalé qu'une surveillance générale de l'utilisation d'Internet par les individus était excessive dès lors qu'elle était menée en dehors de toute suspicion. Nous avons recommandé la mise en place d'une politique autorisant un renforcement progressif de la surveillance selon les besoins concrets et circonstances. La surveillance de l'utilisation d'Internet par des utilisateurs identifiés doit être réservée aux seuls cas de suspicion raisonnable, corroborée par une preuve, et être réalisée dans le cadre d'une enquête administrative. Avant de mettre en place toute action de surveillance, d'autres mesures moins intrusives (comme des rappels ou avertissements généraux) doivent autant que possible être envisagées.

↪ Avis du CEPD ([pdf](#))



## EVENEMENTS

### > ICO: le bureau du commissaire à l'information (Royaume-Uni) se félicite des avancées des réformes envisagées pour l'Union européenne



Au Royaume-Uni, l'année 2013 marque un tournant dans la mesure où les entreprises commencent réellement à réaliser l'importance des réformes envisagées en matière de protection des données dans l'UE, et leurs incidences directes sur le plan juridique.

Si cette perception s'accompagne d'une certaine inquiétude, le Bureau du commissaire à l'information (ICO) britannique s'attache à démontrer tout l'intérêt des

nouvelles propositions. Le droit actuel demande à être moderniser; ces réformes en sont donc le moyen, notamment en termes de renforcement des droits des personnes.

Pour beaucoup, les propositions du nouveau règlement faisaient craindre une augmentation des formalités bureaucratique, notamment pour les petites entreprises. Dans ce contexte, il était donc intéressant d'écouter les commentaires de Françoise Le Bail, Directeur général de la DG Justice de la Commission, lors de la conférence organisée le mois dernier par l'ICO.

Mme Le Bail a tenu à dissiper les craintes concernant un nouveau cadre juridique trop contraignant. Elle a notamment réaffirmé aux participants que la Commission souhaite privilégier une approche fondée sur les risques et tenir particulièrement compte de la position des PME. Cette approche, dont l'ICO se félicite, devrait limiter les incidences disproportionnées sur les entreprises.

Il reste encore beaucoup à faire avant que ces propositions prennent forme dans le cadre d'une loi applicable aux secteurs public et privé. Cela sera possible pour la prochaine décennie et au-delà, mais nous sommes convaincus que de sérieux progrès ont déjà été réalisés.

Vous pouvez découvrir le point de vue de l'ICO vis-à-vis de ces propositions [ici](#) et dans les dernières publications de son blogue en cliquant [ici](#).

## > Formation des délégués à la protection des données (DPD) à Bruxelles

Au sein du CEPD, nous sommes convaincus que le délégué à la protection des données joue un rôle majeur dans l'application des règles et principes de protection des données au sein de l'administration de l'UE. Nous avons donc été heureux d'accueillir une session de formation dans nos bureaux le 17 avril 2013. Au cours de cette journée, nous avons pu rappeler un certain nombre de points:

- Principes de base de la législation relative à la protection des données (licéité du traitement, données confidentielles et exceptions, qualité des données)
- Obligations des délégués à la protection des données (inventaire, registre et notifications au CEPD)
- Procédure de contrôle préalable (échéances, phases procédurales, suivi des recommandations émises dans les avis)
- Orientation disponible sur le site Internet du CEPD (coin du DPD, orientations par thématique)
- Outils de mesure de la mise en conformité (notamment, enquêtes)
- Qu'attendre en cas de non-conformité (visite avec feuille de route et/ou mise en œuvre des pouvoirs répressifs du CEPD).

Les questions et exemples pratiques accompagnant les présentations ont donné lieu à des échanges constructifs entre les collègues du CEPD et les DPD. Cette rencontre a reçu un accueil positif. Les commentaires reçus indiquent également que les DPD ont aussi apprécié cet événement et la possibilité qui leur était offerte d'échanger avec le personnel du CEPD.

## > Rencontre des DPD, Lisbonne

Le 1er mars 2013 s'est tenue à l'Observatoire européen des drogues et des toxicomanies (OEDT) la première de nos rencontres bi-annuelles avec les Délégués à la protection des données.

Outre un échange d'opinions entre le CEPD et les DPD sur le traitement des



33rd Meeting of the Data Protection Officers and the European Data Protection Supervisor - Lisbon, 1st March 2013

données à caractère personnel en relation avec l'utilisation d'Internet et des réseaux de communication, cette rencontre a donné lieu à des échanges sur les développements en matière de protection des données sur le plan européen et international, à la présentation des récentes activités du CEPD comme notre rapport sur les coordinateurs de la protection des données à la Commission européenne, les développements concernant les avis et consultations relatifs aux contrôles préalables, et l'examen stratégique du CEPD.

Cette rencontre a une nouvelle fois constitué une excellente occasion de procéder à des échanges de vues sur des problèmes communs.

## > Table ronde du CEPD: train de mesures sur les frontières intelligentes et leurs implications sur la protection des données

Le 28 février 2013, la Commission a adopté un train de mesures relatives aux frontières intelligentes. La Commission propose un système d'entrée/sortie (EES) qui enregistrera la date et le lieu d'entrée et de sortie des ressortissants de pays tiers qui se rendent dans l'UE. Ce système calculera électroniquement la durée du court séjour autorisé, remplaçant ainsi le calcul manuel, et avertira les autorités nationales en l'absence d'avis de sortie à la date butoir. Pour compléter ce système, un programme d'enregistrement des voyageurs (Registered Traveller Programme - RTP) doit permettre à certaines catégories de voyageurs fréquents provenant de pays tiers d'entrer dans l'UE après avoir fait l'objet de vérifications simplifiées aux frontières.

Le 10 avril 2013, dans le cadre de notre stratégie 2013-2014, nous avons organisé un atelier de travail regroupant des experts de différents pays, notamment de pays ayant mis en place des systèmes similaires, afin de partager leurs expériences et de débattre des implications en termes de protection des données.

Les participants ont été accueillis à cet atelier de travail par MM. Peter Hustinx, CEPD et Giovanni Buttarelli, CEPD adjoint. Etaient ainsi présents des experts de la Commission européenne, du Parlement européen (PE), de la Présidence irlandaise, de la représentation des USA auprès de l'UE, des Etats membres de l'UE, du groupe de travail Article 29, des autorités de la protection des données, ainsi que des universitaires, des ONG parmi lesquelles le Comité Meijers et le CEPS.



Au cours de ce forum, animé par M. Hielke Hijmans, chef de l'unité Politique législative et Consultation du CEPD, un certain nombre de questions et d'inquiétudes ont été soulevées à propos des implications pratiques du système d'entrée/sortie sur la protection des données, de sa compatibilité avec d'autres systèmes tels que VIS et SIS, du rôle de la biométrie, de la possibilité pour les autorités chargées de l'application des lois d'accéder au système, et du transfert des données à des pays tiers. Le groupe s'est particulièrement intéressé aux expériences des États-Unis et des membres de l'UE qui ont mis en œuvre des systèmes similaires.

Pour faire suite à la présentation de nos premières réactions sur ce train de mesures devant la commission des libertés civiles (LIBE) le 21 mars 2013, nous rédigeons actuellement un avis sur ce train de mesures qui devrait être publié dans les mois qui viennent.

## > Réunion du groupe de coordination du contrôle du VIS

Le système d'information sur les visas (VIS) est devenu opérationnel en Afrique du Nord en octobre 2011, puis a été mis en place au Proche-Orient en mai 2012, dans le Golfe en octobre 2012, et en Afrique de l'Ouest et Afrique centrale en mars 2013. Les prochains déploiements auront lieu en Amérique du Sud (septembre 2013), en Asie centrale, en Asie du Sud-Est et dans les Territoires occupés de Palestine (novembre 2013).

Conformément au règlement du VIS, le CEPD et les autorités nationales chargées de la protection des données assurent la coordination du contrôle de la protection des données du VIS. C'est pourquoi le CEPD a organisé le 11 avril 2013 la deuxième réunion du groupe de coordination du contrôle du VIS. Après adoption du règlement intérieur, M. Peter Hustinx, CEPD et Mme Vanna Palumbo, représentant l'autorité italienne chargée de la protection des données, ont été élus respectivement à la présidence et à la vice-présidence du groupe. Le Royaume-Uni et l'Irlande ont été invités à se joindre à titre d'observateurs.

Des représentants de la nouvelle agence de l'Union européenne chargée des systèmes informatiques de grande envergure, EU LISA, ont également présenté au groupe les objectifs de leur programme de travail qui vise à garantir que les caractéristiques techniques du VIS seront en mesure de soutenir une mise en place à l'échelle mondiale.

A la suite des discussions issues de la première réunion, le groupe a adopté le programme de travail du VIS pour les deux prochaines années. Les objectifs du programme se concentrent principalement sur le partage d'expériences nationales au terme d'une analyse complète des exigences du règlement VIS en matière de protection des données, ainsi que sur la réalisation possible d'études conjointes notamment sur l'externalisation de certaines tâches communes auprès d'autres prestataires.

Le groupe a pu profiter des expériences relatées par certains membres puisque plusieurs autorités chargées de la protection des données ont déjà effectué des inspections dans leurs consulats à l'étranger (aucune lacune importante n'a été identifiée jusqu'à présent). Tous les membres du groupe suivent de près les développements, tels que la mise en place continue du système, et prévoient l'inspection des systèmes VIS nationaux à l'avenir.

La prochaine réunion du groupe de coordination du contrôle du VIS se tiendra en automne.

## > Réunion de coordination du contrôle EURODAC



La 18e réunion du groupe de coordination du contrôle EURODAC s'est tenue dans la matinée du 12 avril 2013.

Lors de cette réunion, le groupe a fait le point sur les dernières avancées législatives concernant la refonte du règlement EURODAC dont les discussions touchent à leur fin, et a examiné le transfert des opérations à l'agence IT, EU-LISA à Strasbourg.

Un point a également été proposé au groupe concernant le rapport sur les empreintes digitales illisibles. Sur la base de l'analyse des 28 réponses données, il ressort des conclusions et recommandations principales que:



- Les empreintes digitales illisibles ne doivent pas avoir d'incidence défavorable sur les demandes d'asile.
- La procédure de prise d'empreintes et de gestion temporaire ou permanente des empreintes illisibles doit être claire.
- Les agents responsables de la prise d'empreintes doivent être suffisamment formés. Cette mesure doit être contraignante et uniformisée dans toute l'UE.

Le rapport est en cours de finalisation et sera adopté par le groupe dans les semaines à venir par procédure écrite.

La prochaine réunion du groupe de coordination du contrôle EURODAC aura lieu à l'automne, parallèlement à la réunion du groupe de coordination du contrôle du VIS.



## DISCOURS ET PUBLICATIONS

- «L'avenir de la réglementation des données personnelles en Europe: Un dialogue franco-italien», discours ([pdf](#)) prononcé par Giovanni Buttarelli, Paris (24 avril 2013)
- «Le partage des données à caractère personnel et le respect de la vie privée à domicile», discours ([pdf](#)) prononcé par Peter Hustinx lors de la Conférence Le Point «Maison connectée et intelligente», Paris (28 mars 2013)
- «La protection des données et la justice pénale – Le point de vue du CEPD», discours ([pdf](#)) prononcé par Peter Hustinx lors de la conférence sur le droit en matière de protection des données, Délégation des Barreaux de France, Bruxelles (15 mars 2013)
- «La protection des données à caractère personnel – désormais inscrite dans nos gènes», discours ([pdf](#)) prononcé par Peter Hustinx lors de la Conférence du CESE «Vers une utilisation plus responsable de l'Internet: Le point de vue de la société civile européenne», Bruxelles (6 mars 2013).



## NOUVEAUX DELEGUES A LA PROTECTION DES DONNEES

### > Nominations récentes

- M. Lucas CAMARENA JANUZEC, Comité économique et social européen (CESE)
- M. Stephan KARAS, Autorité européenne des marchés financiers (ESMA)
- M. Martin GARNIER, Centre de traduction des organes de l'Union européenne (CdT)

☞ Voir la 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 la cohérence au niveau de la protection des données à caractère personnel.

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

© Photos: iStockphoto/Edps, Union européenne et ICO

🐦 **Suivez-nous sur Twitter: [@EU\\_EDPS](#)**

### COORDONNEES

[www.edps.europa.eu](http://www.edps.europa.eu)

Tel.: +32 (0)2 283 19 00

Fax: +32 (0)2 283 19 50

[NewsletterEDPS@edps.europa.eu](mailto: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

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