ISSN: 1977-9135

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Newsletter du CEPD

No. 41 | Avril 2014

DANS CE NUMÉRO

FAITS MARQUANTS

Un ensemble unique de règles pour tous: la réforme de la protection des données en Europe peut à la fois soutenir les entreprises et protéger les citoyens

La réforme des règles européennes en matière de protection des données stimulera la reprise encore fragile de l'économie européenne, a déclaré le Contrôleur européen de la protection des données après la présentation de son rapport annuel d'activités pour 2013 à la Commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen. La réforme de ces règles devrait être synonyme de clarté et de cohérence partout en Europe : les mêmes règles s'appliqueront à toutes les entreprises qui exercent leur activité dans l'Union européenne et les citoyens seront rassurés pour ce qui concerne le traitement de leurs informations personnelles.

Le Parlement européen a massivement voté en faveur du train de réformes qui proposera un ensemble de règles uniformes plus simples - et plus économiques - pour les entreprises traditionnelles et en ligne. Il incombe à présent au Conseil de soutenir ce train de réformes dans son ensemble en garantissant aux citoyens le droit de contrôler l'usage qui est fait de leurs informations personnelles ainsi que le droit de recours s'ils sont injustement pris pour cible ou discriminés.

Peter Hustinx, CEPD

Rapport annuel CEPD 2013

Communiqué de presse du CEPD

Rétablir la confiance entre l'UE et les États-Unis passe nécessairement par le respect du droit européen à la protection des données

L'application stricte des lois communautaires existantes en matière de protection des données est un élément essentiel pour rétablir la confiance entre l'Union européenne et les États-Unis, a déclaré le Contrôleur européen de la protection des données 5CEPD) après la publication de son avis le 20 février 2014.

Les droits des citoyens européens à la protection de leur vie privée et de leurs données personnelles sont ancrés dans le droit de l'UE. La surveillance massive des citoyens européens par les agences de renseignement américaine et autres ne tient pas compte de ces droits. En plus de soutenir de nouvelles avancées législatives en matière de vie privée aux États-Unis, l'Europe doit insister sur l'application stricte de la législation européenne en vigueur, promouvoir des standards internationaux de respect de la vie privée et adopter rapidement la réforme en cours du cadre législatif de l'UE sur la protection des données. Un effort concerté pour rétablir la confiance est nécessaire.

Peter Hustinx, CEPD

Avis du CEPD

Communiqué de presse du CEPD

Un contrôle efficace du CEPD pour garder les institutions européennes sur la voie de la protection des données

Les institutions européennes sont plus performantes que jamais pour assurer le respect des principes de protection des données. C'est le message adressé par le CEPD dans son dernier état des lieux, publié le 24 janvier 2014.

Je me réjouis des progrès accomplis par les institutions européennes. Dix ans de supervision active ont mené à une hausse substantielle du niveau de conformité avec les obligations en matière de protection des données au sein de l'administration de l'UE. C'est un signal fort : les institutions européennes reconnaissent qu'elles sont responsables de la mise en œuvre des règles de protection des données.

Peter Hustinx, CEPD

Rapport du CEPD

Communiqué de presse du CEPD

SUPERVISION

Une erreur humaine entraîne une violation de la sécurité

Le 27 novembre 2013, le CEPD a été informé que le règlement (CE) n° 45/2001 semblait avoir été violé, entraînant la divulgation de l'adresse électronique de candidats impliqués dans la procédure de recrutement d'une agence de l'Union européenne. Il est apparu qu'un assistant RH avait envoyé un courrier électronique à 205 candidats non sélectionnés pour les informer que leur candidature n'avait pas été retenue. Dans ce cas précis, une erreur manuelle a été commise par un assistant de l'équipe RH : au lieu de copier toutes les adresses dans le champ « copie cachée » du courrier électronique, il les a copiées par inadvertance dans le champ « à ». Lorsque l'incident est survenu, l'agence avait heureusement instauré des mesures de prévention efficaces destinées à limiter les risques qui pèsent sur les données à caractère personnel. À la suite de cet incident, des mesures supplémentaires ont été (ou seront) mises en œuvre afin de limiter tout autre risque de divulgation. Nous avons reconnu que cette violation de la sécurité était le résultat d'une erreur humaine qui ne semblait pas être le fruit d'une négligence de l'agence en matière de sécurité des données.

Consultation du CEPD

Le nouveau statut des fonctionnaires de l'Union européenne et le traitement ultérieur des évaluations du personnel

Le nouveau *statut* des fonctionnaires européens modifie quelque peu la procédure d'évaluation annuelle ou le système d'évaluation du personnel centré sur l'évolution de carrière. Au titre de ce statut, une évaluation insatisfaisante constitue un frein à la promotion bisannuelle, trois évaluations insatisfaisantes consécutives entraînent le passage à une catégorie inférieure et cinq évaluations insatisfaisantes consécutives ont pour effet le licenciement de la personne concernée.

Le délégué à la protection des données (*DPD*) de la Commission a informé le CEPD de la première utilisation de l'évaluation dès que les modalités d'exécution ont été adoptées.

Dans notre lettre du 28 janvier 2014, nous avons insisté sur le fait que les personnes concernées sont *informées* de la finalité du traitement des informations collectées dans le cadre des évaluations annuelles ainsi que du droit de recours.

En vertu de l'article 110 du nouveau statut du personnel qui assure l'applicabilité de principe des modalités d'exécution générales de la Commission aux 44 agences, le CEPD a décidé de partager ses recommandations avec tous les DPD afin qu'ils soient suffisamment informés à cet égard.

Lettre du CEPD

ARACHNE : aucun réseau d'observation citoyen en matière de protection des données

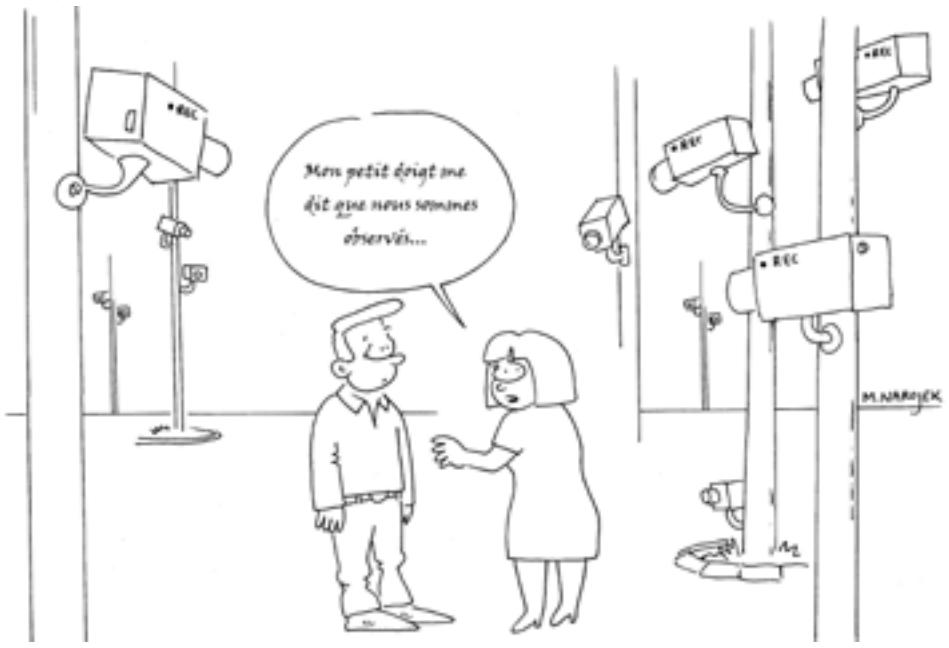
Le système ARACHNE fait partie de la stratégie de prévention et de détection de la fraude de la Commission dans le domaine des Fonds structurels (Fonds social européen et Fonds européen de développement régional) Il complète une base de données existante avec des informations accessibles au public afin d'identifier les projets les plus risqués sur la base d'une série d'indicateurs de risque utilisés pour aider les auditeurs à identifier et sélectionner de futurs candidats pouvant faire l'objet d'un contrôle. Contrairement à d'autres procédés de détection de la fraude, le système ARACHNE n'a pas pour objectif d'évaluer le comportement individuel des bénéficiaires des fonds ou de priver des bénéficiaires de ces fonds.

Les recommandations formulées dans notre avis du 17 février 2014 évoquent notamment la nécessité d'assurer la qualité des données et d'informer les personnes concernées. Étant donné que le système ARACHNE contiendra, par exemple, des informations portant sur des individus sous le coup de sanctions, nous préférons adopter une base juridique plus spécifique autorisant le traitement de certaines catégories de données à caractère personnel en vertu de l'article 10, paragraphe 5, du règlement.

Avis du CEPD

Vidéosurveillance : le CEPD se félicite des améliorations constatées dans les pratiques des organes de l'Union européenne

Depuis la publication des lignes directrices en matière de vidéosurveillance en 2010, et tel qu'annoncé dans notre rapport de suivi de 2012, le CEPD a enquêté en 2012 sur la conformité de 13 institutions et de 12 organes de l'UE basés à Bruxelles et a effectué quatre inspections similaires au Luxembourg en 2013 . Ces inspections étaient axées sur la manière dont les informations portant sur la vidéosurveillance sont transmises au grand public. Le rapport d'inspection des inspections effectuées au Luxembourg a été publié le 13 janvier 2014. Le règlement



(CE) n° 45/2001 oblige les institutions et organes de l'UE à informer le CEPD lorsqu'elles élaborent des mesures administratives relatives au traitement de données à caractère personnel. Les résultats positifs de ces récentes inspections laissent à penser que nos conseils ont été pris en compte - un bon exemple d'institutions et d'organes de l'UE appliquant le principe de responsabilité.

Communiqué de presse du CEPD

Fiche d'information du CEPD sur les CCTV

CONSULTATION

Progrès concernant le train de réformes en matière de protection des données

Sous la présidence grecque, le Conseil continue de débattre du règlement général sur la protection des données. Dans une lettre envoyée au président du Conseil de l'Union européenne le 14 février, nous avons fait part de notre point de vue concernant **trois points essentiels** de la réforme qui sont encore en suspens.

Premièrement, nous avons souligné la nécessité de s'assurer que le **secteur public demeure dans le champ d'application du règlement général sur la protection des données**. En effet, prévoir une dérogation, comme semblent le préconiser certains États membres, constituerait un recul par rapport au système actuel de protection des données, étant donné que ni la directive 95/46/CE relative à la protection des données ni la convention 108 du Conseil de l'Europe ne font de distinction entre le secteur privé et le secteur public. Plus important encore, de nombreuses activités telles que la prestation de soins de santé, peuvent être pratiquées par des entités privées ou publiques qui devraient être soumises aux même règles.

Nous sommes également intervenus dans le débat portant sur le sujet qui fait l'objet d'un vif débat : **le guichet unique**. Nous avons souligné l'importance de ce principe dans la proposition d'harmonisation du cadre relatif à la protection des données. En la matière, nous estimons que le principe du guichet unique ne restreint pas indûment les droits des personnes concernées à un recours juridictionnel efficace ni à un procès équitable et qu'il est compatible avec un niveau élevé de protection des droits fondamentaux des citoyens, y compris ceux garantis par l'article 47 de la Charte des droits fondamentaux.

En conclusion, nous avons présenté nos observations sur le **principe de responsabilisation** et sur « l'approche fondée sur le risque », soulignant la nécessité de critères clairs permettant de réaliser une évaluation des risques afin que les efforts déployés pour respecter les règles soient dirigés directement vers les zones principalement concernées.

Paiements dans le marché intérieur

Le 5 décembre 2013, nous avons publié un Avis portant sur l'ensemble des dispositions législatives relatives aux *services de paiement dans le marché intérieur et aux commissions interbancaires relatives aux opérations de paiement par carte*. La directive a pour but de donner une série de nouveaux droits aux consommateurs tandis qu'un règlement connexe plafonnera les commissions que les distributeurs paient aux banques en cas de paiement par carte de débit et de crédit et réduira également les coûts qui incombent aux consommateurs. En la matière, nous avons salué l'introduction d'une disposition importante en vertu de laquelle le traitement des données à caractère personnel organisé dans le cadre de la directive proposée se fera dans le respect intégral des législations nationales transposant la directive 95/46/CE, la directive 2002/58/CE et le règlement n° 45/2001.

Nous avons recommandé que les références à la loi sur la protection des données en vigueur soient précisées par des garanties concrètes qui s'appliqueront à toutes les situations dans lesquelles le traitement des données est envisagé ; il faudrait, par ailleurs, expressément préciser que le traitement des données à caractère personnel n'est autorisé que dans la mesure où il est nécessaire aux services de paiement. Nous avons également attiré l'attention sur d'autres questions relatives à la protection des données, par exemple dans le cadre de l'échange d'informations, l'accès de tiers à des informations comptables et à la transmission d'informations sécuritaires.

Avis du CEPD

Déjouer les trafics illicites d'armes à feu et protéger les données à caractère personnel

Dans notre avis du 17 février 2014 portant sur la Communication de la Commission sur *les armes à feu et la sécurité intérieure dans l'Union européenne : protéger le citoyens et déjouer les trafics illicites*, nous avons souligné les exigences en matière de protection des données qui s'appliquent en particulier aux priorités et aux tâches exposées dans la Communication.

Nous avons souligné l'importance d'aborder ces questions au début du processus législatif si possible lors de la consultation des parties prenantes, et d'inclure dans chaque texte réglementaire une référence à la loi sur la protection des données en vigueur.

Plus précisément, nous avons abordé les questions portant sur :

- le marquage des armes à feu ;
- la possibilité d'exiger des examens médicaux et vérifications judiciaires comme une condition d'achat et de détention licites de toute arme à feu ;
- l'installation de capteurs biométriques sur les armes à feu ; et
- le partage d'informations entre les autorités répressives et les autorités douanières, à travers des systèmes informatisés de grande envergure.

Avis du CEPD

Le recoupement de données pour lutter contre la fraude et les erreurs dans le domaine de la coordination transfrontalière des systèmes de sécurité sociale

La Commission a sollicité l'avis du CEPD concernant une proposition à l'examen pour modifier le règlement portant sur la *coordination des systèmes de sécurité sociale* pour lutter contre la fraude et les erreurs dans le contexte de la coordination transfrontalière des systèmes de sécurité sociale entre les États membres.

Le recoupement de données consiste à comparer deux ensembles de données à caractère personnel afin d'identifier les informations contradictoires. Par exemple, un État membre A sur le territoire duquel résident un certain nombre de retraités ressortissants d'un État membre B communique à ce dernier des données sur les décès. Ainsi, l'État membre B peut comparer ces données avec sa liste de retraités vivant sur son territoire afin de détecter tout anomalie entre les deux séries de données, à savoir si des pensions sont versées à des personnes décédées.

Dans nos observations du 17 janvier 2014, nous avons accueilli favorablement l'intention de la Commission de modifier le cadre juridique actuel afin de fournir des éclaircissements sur l'échange de données en masse sous la forme d'un « recoupement de données ». Outre qu'il faille insister sur la nécessité et la proportionnalité du recoupement de données, nous avons souligné qu'il est particulièrement important de :

- faire en sorte que la notion de recoupement des données soit transparente ;
- garantir l'absence de refus automatique d'octroi de prestations sur la base des résultats de la procédure de recoupement des données ; et
- garantir l'existence de procédures équitables permettant aux personnes physiques de contester toute décision prise sur la base de procédures automatiques de recoupement des données.

Observations du CEPD

Protection des données personnelles dans la chaîne agroalimentaire

Une proposition de règlement concernant les *contrôles officiels et les autres activités officielles servant à assurer le respect de la législation sur les denrées alimentaires et les aliments pour animaux* est actuellement en première lecture au Parlement et au Conseil. La proposition porte sur le traitement de deux ensembles généraux de données, à savoir des données liées aux opérateurs (par exemple, les noms de personnes ou d'entreprises, le lieu d'établissement, les sites Internet, les classements, etc.) et des données liées aux avoirs des opérateurs (par exemple, les animaux et les biens). En outre, des informations seront échangées entre autorités nationales compétentes au moyen d'un réseau informatisé à l'échelle européenne, l'IMSOC.

Dans nos observations du 20 février 2014, nous avons précisé que :

- les données liées aux biens et aux animaux peuvent être considérées comme relatives à un individu identifié ou identifiable, et qu'elles relèvent donc du concept de « données à caractère personnel » ;
- les règles de protection des données s'appliquent au traitement des données tel qu'envisagé par le règlement. Partant, les opérateurs qui exercent leurs activités professionnelles en tant que personnes physiques sont des personnes concernées au sens des règles applicables à la protection des données. En outre, même les opérateurs qui agissent comme personnes morales peuvent être considérés comme des personnes concernées si « le nom légal de la personne morale identifie une ou plusieurs personnes physiques » ou si d'autres informations sur les personnes morales peuvent aussi être considérées comme « concernant » des personnes physiques, ou encore si le droit national, y compris celui transposant la directive 95/46/CE au niveau national, étend la protection des données à caractère personnel aux personnes morales ;
- l'IMSOC appliquera les principes du respect de la vie privée dès la conception ou par défaut et les informations devront être fournies par la Commission pour la partie du traitement dont elle est responsable. Cela nécessite de la Commission qu'elle fournisse une première « couche » de notification relative à la protection des données et d'autres informations pertinentes aux personnes concernées sur son site Internet multilingue, y compris « pour le compte » d'autorités compétentes.

Observations du CEPD

Les concepteurs de l'internet réfléchissent aux moyens d'améliorer les connaissances en matière de sécurité et de respect de la vie privée

L'Internet Engineering Task Force (IETF) est l'organe à but non lucratif qui conçoit et promeut les normes de fonctionnement de l'internet, en particulier pour le protocole internet (TCP/IP, etc.). Lors de la réunion de l'IETF organisée en mars dernier à Londres, des concepteurs de l'internet ont présenté le suivi des résultats de leur précédente réunion organisée à Vancouver en novembre dernier (cf. notre rapport dans la *newsletter* du CEPD de décembre 2013). Ils avaient convenu que la surveillance massive des communications internet représentait une menace et que cette menace, à l'instar d'autres, devait être combattue au moyen de mesures techniques. La réunion de Londres a été l'occasion d'organiser des séminaires sur le respect de la vie privée et de débattre de la meilleure manière d'ancrer le respect de la vie privée dans la toile de l'internet, par le biais de ses protocoles. La réunion de l'IETF a été précédée d'un *séminaire* spécialisé réunissant plus de cent spécialistes de l'internet qui ont passé en revue plus de 60 documents portant sur la manière de renforcer l'internet contre l'omniprésence de la surveillance.

Pour la plupart des spécialistes, il convient d'abord de faire bon usage des outils cryptographiques correctement mis en œuvre (algorithmes codés de bas niveau fréquemment utilisés pour concevoir les systèmes de sécurité informatiques) afin de renforcer la sécurité des réseaux et des communications. Des experts du respect de la vie privée ont déjà signalé que d'autres principes du respect de la vie privée, tels que la limitation de données, l'anonymisation et l'agrégation de données, devraient également être pris en compte. La mise au point de solutions techniques utiles destinées à mettre ces principes en œuvre nécessitera une large coopération. Le CEPD lance une *initiative* pour surmonter les problèmes de communication entre les experts du respect de la vie privée et les concepteurs et pour les amener à développer de concert des outils techniques destinés à renforcer le respect de la vie privée au niveau des outils et des applications internet et il invite les concepteurs de l'internet à exprimer leur point de vue.

La sécurité mobile représentera-t-elle un défi majeur pour le respect de la vie privée?

Les moyens de communication mobiles sont en passe de devenir le principal moteur de notre monde interconnecté. De plus en plus d'appareils sont équipés de Wi-Fi, Bluetooth, 4G ou d'autres interfaces qui permettent de se connecter directement à l'internet ; on peut également s'y connecter au moyen de téléphones intelligents ou de réseaux domestiques. Des dispositifs mobiles, tels que des appareils de contrôle des activités sportives, équipés de la technologie de navigation par satellite enregistrent des données biométriques, la position et les mouvements de leur utilisateur et les transmettent aux serveurs de leurs fabricants dès qu'ils sont connectés. Des appareils domestiques peuvent communiquer avec des réseaux locaux et des voitures peuvent enregistrer et transmettre des données relatives à leurs fonctions, leur position et le comportement de leurs conducteurs.

Les géants de l'internet investissent de manière significative dans les technologies mobiles et intégrées : ils ont récemment acheté plusieurs entreprises de messagerie mobile, d'automatisation domestique ou de robotique. Par ailleurs, ils investissent massivement dans la recherche et le développement pour la mobilité (p. ex. voitures autonomes).

Alors que ces tendances sont susceptibles d'amplifier la collecte et la transmission de données à caractère personnel sur les réseaux,

d'aucuns craignent que la sécurité ne soit pas suffisante. Le nombre de failles de sécurité détectées dans les systèmes les plus répandus est également en hausse. Une *erreur de programmation* récemment corrigée a accru la vulnérabilité aux attaques de type intermédiaire de certains appareils mobiles très populaires, ce qui pourrait permettre aux pirates d'intercepter des communications apparemment cryptées. Peu de temps après cet incident, un problème lié à un logiciel ouvert a également été détecté. Une partie du code présent dans de nombreux systèmes Linux présentait une *faille importante* qui aurait permis aux pirates de contourner certaines protections du TLS (Transport Layer Security). Par conséquent, les programmes utilisant ce système sont vulnérables aux attaques et leurs communications cryptées sont susceptibles d'être décodées. Dans les deux cas, la mise à jour des logiciels a permis de corriger ces erreurs de programmation. De plus, il est apparu récemment qu'un téléphone intelligent utilisant un système d'exploitation androïde était lui aussi vulnérable : la puce responsable des communications sur le réseau pouvait contourner les restrictions protégeant la partie « intelligente » du téléphone et, par conséquent, accéder à toutes les informations stockées dans le téléphone intelligent. Les personnes qui parviendraient à prendre le contrôle de ce module de communication de données pourraient utiliser cette porte dérobée dans le téléphone de l'utilisateur. Une solution a été développée pour cette configuration spécifique, mais tous les téléphones concernés n'en bénéficieront peut-être pas rapidement.

Alors que les logiciels de la plupart des ordinateurs et de nombreux appareils mobiles sont fréquemment mis à jour pour limiter leur vulnérabilité aux attaques, il n'en va pas de même pour d'autres dispositifs équipés de moyens de communication intégrés tels que des téléviseurs ou des appareils domestiques. Bien souvent, les mises à jour des logiciels de ces appareils ne sont plus disponibles peu de temps après la vente des appareils, c'est-à-dire bien avant qu'ils ne rendent l'âme. Les vulnérabilités de leurs « anciens » systèmes d'exploitation et de leurs « anciennes » fonctions demeurent en place et peuvent servir de porte d'entrée aux pirates qui misent sur les faiblesses bien connues des anciennes versions des logiciels. Parfois même, il est apparu que certains routeurs donnant accès au réseau présentaient des faiblesses.

Cette situation est une véritable gageure pour les fabricants, les distributeurs et les prestataires de services qui veulent créer l'internet des objets. Il convient de développer des appareils sûrs capables de garantir leur propre sécurité au moyen de mises à jour périodiques du système d'exploitation. Si l'on ne solutionne pas ce problème, la mise sur le marché d'appareils connectés pourrait être sérieusement limitée en raison de problèmes de sécurité tout à fait justifiés.

ÉVÉNEMENTS

Le laboratoire du CEPD sera opérationnel au printemps

En 2013, afin de renforcer ses propres moyens de surveillance technologiques et d'évaluer dans quelle mesure certains produits ou systèmes utilisés dans le cadre de ses travaux de contrôle respectent la vie privée, le CEPD a envisagé la création d'un laboratoire informatique. Ce laboratoire aidera le CEPD à évaluer les effets des derniers développements technologiques sur le respect de la vie privée et à s'assurer que les sites internet respectent les règles en matière de protection des données. Le laboratoire du CEPD devrait être opérationnel au printemps 2014.

Le laboratoire pourrait également permettre de tester des plateformes nouvelles ou modifiées pertinentes en matière de protection des données, telles que des résultats de projets de recherche universitaires ou de nouveaux produits.

À l'avenir, nous pourrions inviter les diplômés en informatique qui suivent notre programme de stage ou les étudiants postuniversitaires qui mènent une partie de leurs recherches au CEPD à utiliser le laboratoire pour y développer des projets de recherche et développement. Ils pourraient y mener à bien des projets de recherche et développement et y conduire des expériences.

À cet effet, nous promouvons activement le *programme de stage* du CEPD auprès des étudiants en informatique et des personnes qui souhaitent étudier les aspects technologiques de la protection des données et du respect de la vie privée. Le CEPD offre un stage rémunéré de cinq mois aux diplômés universitaires ainsi que la possibilité d'effectuer un stage non rémunéré aux étudiants postuniversitaires qui bénéficient déjà du soutien d'autres programmes et qui souhaitent poursuivre leurs travaux de recherche à Bruxelles.

DÉLÉGUÉS À LA PROTECTION DES DONNÉES

DISCOURS ET PUBLICATIONS

- Discours (*pdf*) de Peter Hustinx à Bruxelles, «Opportunities and challenges in the digital era: big data and moral hazard» (1er avril 2014)
- Discours (*pdf*) de Peter Hustinx à Bruxelles, « Observations sur le contrôle de la protection des données à Europol » (12 février 2014)
- Discours (*pdf*) de Peter Hustinx à Bonn, « Passation de fonction : cérémonie de départ et d'accueil » (4 février 2014)
- Discours (*pdf*) de Peter Hustinx à Bonn, « La proposition visant à créer un marché intérieur de l'UE pour le secteur des communications électroniques : champ de tension entre protection des données, neutralité du réseau et liberté économique » (13 janvier 2014)

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 site Internet.

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-14-001-FR-C