



CONSULTATION

- > Les règles applicables aux dispositifs médicaux respectent les données à caractère personnel mais doivent être plus strictes3
- > Révision des règles relatives aux précurseurs de drogues pour y inclure la protection des données3
- > Renforcement de la proposition relative aux essais cliniques du point de vue de la protection des données4
- > Des mesures en matière de protection des données font du dispositif eCall un service intelligent5
- > Trouver l'équilibre entre le respect de la vie privée et la transparence en matière de financement des partis politiques et des fondations européens5



SUPERVISION

- > Le SEAE démontre sa volonté de coopérer6
- > Contrôle préalable des communications électroniques...7
- > Une visite fructueuse à l'Agence Frontex7
- > Les coordinateurs de la protection des données jouent un rôle important dans le soutien aux délégués à la protection des données8



ÉVÉNEMENTS

- > L'autorité belge chargée de la protection des données publie une recommandation relative aux mesures de sécurité à respecter afin de prévenir les fuites de données8
- > Les règles d'entreprise contraignantes de l'UE et les règles transfrontalières de protection de la vie privée de la CEAP9
- > 28 janvier: Journée de la protection des données10
- > Présentation de la stratégie du CEPD pour 2013-201411
- > Atelier sur la proposition de règlement relatif à la protection des données, Varsovie, 12 décembre 201212



DISOURS ET PUBLICATIONS



DÉLÉGUÉS À LA PROTECTION DES DONNÉES

- FAITS MARQUANTS -

> Inventaire des consultations législatives pour 2013

Le 18 janvier 2013, le CEPD a fixé ses priorités pour l'année à venir en matière de **consultations législatives** et a publié un document de planification stratégique, l'Inventaire. Dans ce document, nous indiquons les questions et domaines **d'importance stratégique** qui constitueront la pierre angulaire de notre travail de consultation pour 2013.

“ Nous vivons dans un monde technologique en perpétuelle évolution. La visibilité et la pertinence de la protection des données sont dès lors plus importantes que jamais. La nécessité de prendre en compte les implications sur la protection des données et la vie privée des propositions législatives devient essentielle dans tous les domaines de la politique de l'UE, et conduit à une inflation de nouveaux champs



d'action auxquels nous sommes confrontés. Il est de plus en plus évident que le droit fondamental à la protection des données ne peut être réglé que par la seule législation en matière de protection des données, et que de nombreuses autres politiques doivent prendre en compte la protection des données. ”

Peter Hustinx, CEPD

Notre mission centrale dans le domaine de la consultation est de fournir des conseils dans trois domaines principaux: la **révision du cadre juridique pour la protection des données, les développements technologiques et l'agenda numérique, et la poursuite du développement de l'espace de liberté, de sécurité et de justice**. Nous avons en outre érigé la réforme du secteur financier et *eHealth* (la santé en ligne) en domaines d'importance stratégique pour 2013.

Par ailleurs, afin de mieux remplir notre rôle consultatif, nous envisagerons de publier des *avis prospectifs* sur des phénomènes techniques ou sociétaux importants (comme l'informatique dématérialisée) afin de mettre en avant les défis qui les caractérisent et de proposer des solutions le cas échéant.

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

> CEPD: le statut des DPD est essentiel pour la garantie des droits du personnel et des citoyens

Le 17 décembre 2012, le CEPD a publié un rapport sur le statut des délégués à la protection des données (DPD) dans le cadre de notre tâche de supervision du respect par les institutions et organes de l'UE de l'article 24 du règlement sur la protection des données, qui impose la désignation des DPD.

“ *Garantir le droit fondamental à la protection des données du personnel et des citoyens exige un engagement sans faille de la hiérarchie au sein des institutions et organes de l'UE. Cet engagement passe par la désignation et le soutien de leurs DPD, mais aussi par le statut qui leur est octroyé au sein même de l'organisation.* ”

Giovanni Buttarelli, Contrôleur adjoint

Les résultats de notre enquête montrent que la fonction de DPD est bien établie au sein de l'administration européenne, comme en attestent, par exemple, l'expérience du réseau des DPD, le rattachement administratif de la majorité des DPD au président/directeur de l'institution ou de l'organe et l'existence d'un soutien important du personnel dans le cas de nombreux DPD.

Il subsiste cependant des points de préoccupation que nous avons soulignés dans notre rapport. L'article 24 du règlement sur la protection des données prévoit que les personnes exerçant la fonction de DPD doivent être nommées pour une période minimale de deux ans. Nous avons cependant constaté une forte rotation des personnes exerçant cette fonction et, dans certains cas, des mandats plus courts, ce qui peut





être lié à la situation contractuelle de ce personnel. En outre, nous avons constaté d'éventuels conflits d'intérêts pour les personnes combinant les fonctions de DPD avec d'autres responsabilités et, parfois, le manque de ressources adéquates pour permettre aux DPD de s'acquitter de leur mission.

Comme les institutions sont entièrement responsables quant au respect des règles de protection des données, il est impératif qu'elles répondent à ces préoccupations de manière adéquate; nous avons d'ailleurs la ferme intention de suivre de près l'évolution en la matière et d'adresser les recommandations nécessaires.

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



CONSULTATION

> Les règles applicables aux dispositifs médicaux respectent les données à caractère personnel mais doivent être plus strictes



Les propositions de règlements de la Commission relatifs aux dispositifs médicaux et aux dispositifs médicaux in vitro prévoient le traitement et le stockage de volumes considérables d'informations à caractère personnel, pouvant nécessiter la sauvegarde de données sensibles, comme des informations sur la santé des patients, dans une base de données européenne centrale (Eudamed).

Dans notre avis du 8 février 2013, nous avons pris acte de l'attention particulière accordée à la protection des données dans ces propositions de règlements et nous en sommes félicités. Nous estimons cependant que des améliorations et des clarifications supplémentaires sont nécessaires, par exemple, en ce qui concerne les types de catégories d'informations à caractère personnel à traiter, en particulier lorsque des données sensibles relatives à la santé sont susceptibles d'être traitées et stockées. Nous recommandons, d'une part, que ces propositions de règlements précisent les circonstances dans lesquelles les données à caractère personnel relatives à la santé peuvent être insérées dans la base de données Eudamed et, d'autre part, que les mesures de protection en matière de traitement et de stockage soient décrites.

☞ Avis du CEPD ([pdf](#))

> Révision des règles relatives aux précurseurs de drogues pour y inclure la protection des données



Le 18 janvier 2012, nous avons publié un avis sur les propositions de la Commission en vue de modifier les réglementations relatives au commerce de précurseurs de drogues au sein de l'UE et avec les pays tiers. Nous nous sommes félicités des références, faites dans ces propositions, à l'application de la législation européenne en matière de protection des données, et nous nous sommes réjouis du fait que de nombreuses catégories d'informations



à traiter étaient précisées et du fait que le principe de limitation des finalités était mentionné dans la proposition relative au commerce extérieur.

Nous avons cependant recommandé que les principaux textes législatifs indiquent tous les éléments essentiels des opérations de traitement, comme l'exclusion du traitement des données sensibles. En outre, toutes les catégories d'informations à traiter doivent être précisées au minimum dans des actes délégués mais également de préférence dans les propositions.

Nos autres recommandations concernent les points suivants:

- la proposition relative au commerce au sein de l'UE doit préciser que les informations à caractère personnel relatives à des transactions suspectes ne peuvent être utilisées qu'en vue d'éviter le détournement de substances classées;
- il convient de fixer des périodes maximales de conservation pour toutes les opérations de traitement;
- il convient de prévoir des mesures de protection appropriées en matière de transferts internationaux d'informations à caractère personnel;
- il convient de préciser qui a accès à la nouvelle base de données européenne sur les précurseurs de drogues;
- il convient de garantir un contrôle coordonné de la base de données européenne par le CEPD et les autorités nationales chargées de la protection des données, similaire à ce qui est prévu pour le système d'information du marché intérieur;
- il convient d'interdire l'interconnexion de la base de données européenne avec d'autres bases de données créées à des fins différentes.

☞ Avis du CEPD ([pdf](#))

> Renforcement de la proposition relative aux essais cliniques du point de vue de la protection des données

Le 19 décembre 2012, nous avons adopté un avis sur la proposition de la Commission relative aux essais cliniques de médicaments à usage humain. Nous nous sommes réjouis de l'attention spécifique accordée à la protection des données dans cette proposition de règlement, mais avons constaté qu'il était possible d'y apporter des améliorations.

Nous avons recommandé que cette proposition de règlement fasse explicitement référence au traitement d'informations à caractère personnel relatives à la santé; qu'elle précise si les informations à caractère personnel relatives à la santé seront ou non traitées dans les bases de données européenne relatives aux essais cliniques et, dans l'affirmative, à quelle fin; qu'elle mentionne le droit des personnes concernées de bloquer les informations à caractère personnel les concernant et qu'elle introduise une période maximale de conservation pour le stockage des informations à caractère personnel.

☞ Avis du CEPD ([pdf](#))

> Des mesures en matière de protection des données font du dispositif eCall un service intelligent

eCall est un système qui envoie automatiquement un message aux services d'urgence à la suite d'un accident de la route; ce message contient entre autres la localisation précise de l'accident. Le dispositif embarqué eCall émet un appel d'urgence (appel E112 sans fil) généré soit manuellement par les occupants du véhicule en appuyant sur un bouton soit automatiquement via l'activation après l'accident de détecteurs placés dans le véhicule.



Le 19 décembre 2012, nous avons publié des observations officielles concernant un règlement délégué complétant la directive STI (directive 2010/40/UE) en ce qui concerne la mise à disposition harmonisée d'un service d'appel d'urgence (eCall) interopérable dans toute l'UE. Ce règlement délégué, adopté par la Commission le 26 novembre 2012, définit les spécifications relatives à la mise à niveau nécessaire de l'infrastructure des centres de réception des appels d'urgence (PSAP).

Nous nous sommes félicités des nombreuses références faites dans ce texte à la législation en matière de protection des données, en particulier celles qui définissent les règles en matière de protection des données et de respect de la vie privée, en vertu desquelles les PSAP et les autres acteurs concernés sont responsables devant les autorités nationales chargées de la protection des données en ce qui concerne le traitement des informations à caractère personnel. Nous avons constaté avec plaisir que les PSAP (et les services d'urgence ou partenaires appropriés) ont mis en place les mesures de protection suivantes:

- pas de pistage continu des véhicules équipés du système eCall intégré;
- protection contre l'utilisation abusive ou la perte de toute donnée;
- définition des modalités appropriées pour stocker et traiter les données;
- limitation de l'accès aux informations concernant le véhicule stockées dans les bases de données nationales ou ailleurs aux cas dans lesquels cela est approprié et conforme à la législation nationale, et indication des types d'informations auxquelles il est possible d'avoir accès.

Nous avons également constaté avec satisfaction que les États membres doivent informer la Commission quant aux protocoles en matière de respect de la vie privée et de protection des données mis en place dans le cadre de ce règlement délégué.

↳ Observations du CEPD ([pdf](#))

> Trouver l'équilibre entre le respect de la vie privée et la transparence en matière de financement des partis politiques et des fondations européens

Dans notre avis du 13 décembre 2012 sur le statut et le financement des partis politiques européens et des fondations européennes, nous avons rappelé que le respect de la vie privée et la protection des données n'ont pas pour rôle d'empêcher l'accès du public aux informations dès que des données à caractère personnel sont concernées ni de limiter excessivement la transparence. Le respect de la



vie privée et la protection des données devraient garantir que les informations à caractère personnel ne sont publiées que lorsque cela est justifié et que les différents intérêts des personnes concernées ont été mis en balance.

L'une des principales préoccupations en matière de protection des données liées à cette proposition concerne la publication d'informations sur les dons et contributions apportés aux partis politiques européens et aux fondations européennes. Nous avons reconnu que l'objectif de l'accroissement de la transparence et de la confiance dans le processus démocratique est légitime. Cependant, nous avons indiqué que la publication d'un seuil pour les dons et les contributions, tel que recommandé dans l'arrêt rendu dans l'affaire *Schecke*, contribuerait à parvenir à un juste équilibre. Il convient également de fournir une justification de ce seuil.

🔗 Avis du CEPD ([pdf](#))



SUPERVISION

> Informations sur le contrôle préalable par le CEPD du traitement des données à caractère personnel

Le traitement des données à caractère personnel par l'administration de l'UE qui est susceptible de présenter des risques particuliers pour les personnes concernées fait l'objet d'un contrôle préalable par le CEPD. Cette procédure sert à déterminer si le traitement est conforme ou non au règlement (CE) n° 45/2001 sur la protection des données, qui définit les obligations des institutions et des organes de l'UE en matière de protection des données.

> Le SEAE démontre sa volonté de coopérer

Le 1^{er} février 2013, nous avons publié notre premier avis de contrôle préalable concernant une opération de traitement du Service européen pour l'action extérieure (SEAE). Ce contrôle préalable portait sur des enquêtes de sécurité effectuées par la division «Sécurité et politique de sécurité» du SEAE. La notification initiale du SEAE couvrait plusieurs mesures en matière de sécurité que nous avons précisées et dont nous avons limité la portée.



Dans nos conclusions, nous avons recommandé de modifier le projet de proposition de décision sur la politique de sécurité. Le SEAE a déjà confirmé qu'il sera modifié. Une autre recommandation que nous avons formulée portait sur les transferts de données – étant donné qu'il s'agit d'un service extérieur, cela pourrait inclure les transferts vers des pays tiers et des organisations internationales – et nous avons renvoyé à notre document suivant sur les transferts de données.

🔗 Avis du CEPD ([pdf](#))



> Contrôle préalable des communications électroniques...

Le CEPD a été consulté sur les données de contrôle des appels du système de communication unifié (UniComm) de l'Agence des droits fondamentaux de l'Union européenne (FRA). Dans notre réponse du 1^{er} février 2013, nous avons précisé les cas de communications électroniques nécessitant des notifications de contrôle préalable.

En principe, nous considérons que les communications électroniques (et en particulier le traitement des enregistrements téléphoniques) doivent être soumises à un contrôle préalable dans les trois situations suivantes:

- 1) s'il y a violation de la confidentialité de la communication, ou
- 2) si le traitement a trait à des suspicions ou à des mesures de sûreté, ou
- 3) si le traitement vise à évaluer des aspects de la personnalité des personnes concernées.



Dans ce cas, il est apparu que les informations à caractère personnel en question ne sont traitées que pour assurer le bon fonctionnement, l'identification et le traitement des menaces de sécurité contre le système UniComm. Parallèlement, le traitement ne semble pas violer la confidentialité des communications, dans la mesure où certaines informations relatives au trafic ne sont traitées que pour permettre aux personnes d'identifier leurs appels privés, sans interférer avec le contenu de leurs communications. Nous en avons dès lors conclu que ces opérations de traitement ne nécessitent pas de contrôle préalable.

☞ Consultation du CEPD ([pdf](#))

> Une visite fructueuse à l'Agence Frontex

Dans le cadre de notre rôle de contrôle, nous avons organisé une visite à l'Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des États membres de l'UE (Frontex) en décembre 2012. La visite est un instrument de conformité dont l'objectif est de faire en sorte que les dirigeants d'une institution ou d'une agence de l'UE s'engagent à favoriser le respect du règlement en matière de protection des données. Plusieurs raisons peuvent justifier une visite dans une institution ou une agence. En l'occurrence, nous étions préoccupés par l'absence de coopération entre Frontex et le CEPD.



Cette visite incluait une réunion entre le contrôleur européen adjoint de la protection des données et le directeur exécutif de Frontex ainsi que des réunions avec le délégué à la protection des données et les personnes chargées des opérations de traitement. Nous avons également présenté notre approche en matière de contrôle et de garantie du respect de la réglementation au sein des institutions de l'UE.

Cette visite s'est révélée être une évaluation préliminaire très utile du respect du règlement (CE) n° 45/2001 par Frontex et fut l'occasion de sensibiliser l'agence à la question de la protection des données.



> Les coordinateurs de la protection des données jouent un rôle important dans le soutien aux délégués à la protection des données

Au cours de ces dernières années, certaines des plus grandes institutions de l'UE ont créé des réseaux de coordinateurs de la protection des données (CPD) afin de servir de relais pour les délégués à la protection des données (DPD) au niveau local. En juin 2012, le CEPD a lancé une enquête sur la fonction de CPD et les mécanismes mis en place par les directions générales (DG) de la Commission européenne pour se conformer au règlement (CE) n° 45/2001. En janvier 2013, nous avons publié un rapport général contenant les conclusions de cette enquête.

Les résultats de l'enquête montrent une grande disparité dans les ressources allouées à la fonction par les DG, par exemple, entre 5 % et 100 % du temps du CPD sont consacrés à la fonction. Les CPD partagent cependant un socle commun de tâches dont ils doivent s'acquitter peu importe le temps dont ils disposent. Une de nos conclusions est dès lors qu'il est nécessaire d'établir des critères minimums à remplir par les DG afin de préserver l'utilité de la fonction.

Notre rapport salue aussi certaines des bonnes pratiques développées dans certaines DG, comme créer une boîte fonctionnelle pour la consultation du CPD, développer une page intranet dédiée à la protection des données, assurer la visibilité du CPD dans l'organigramme ou structurer son accès à la hiérarchie et assurer son information effective.

Enfin, nous avons souligné dans notre rapport le fait que la fonction de CPD s'inscrit aussi dans la réforme actuelle de la protection des données: le rapport entre le rôle joué par le CPD et la responsabilité de la DG, d'une part, et sa mission concernant la documentation des opérations de traitement, d'autre part, joue un rôle majeur dans le soutien à la fonction de DPD.

☞ Rapport du CEPD ([pdf](#))



ÉVÉNEMENTS

> L'autorité belge chargée de la protection des données publie une recommandation relative aux mesures de sécurité à respecter afin de prévenir les fuites de données



Une série de fuites de données commentées dans les médias belges début janvier a incité l'autorité belge chargée de la protection des données à élaborer une recommandation relative aux mesures de sécurité à prendre afin de prévenir de tels incidents portant atteinte à la sécurité. Ce document a pour but de sensibiliser les individus à la sécurité des informations et de souligner certains éléments fondamentaux en vue d'aider les organisations à établir les fondements d'une politique de sécurité appropriée.

Les deux conditions de base nécessaires à la mise en place d'une politique de sécurité efficace sont la responsabilité du management et l'information des



employés. Le management doit prendre l'initiative d'élaborer une politique de sécurité et de la communiquer dans tous ses aspects aux employés. Une politique de sécurité bien documentée, soutenue par l'ensemble des membres de l'organisation, est à la base de la réussite d'une telle politique. D'un point de vue pratique, l'autorité belge chargée de la protection des données recommande les points suivants:

- des couches de sécurité, à savoir différents niveaux d'accès pour différentes zones du réseau ainsi qu'une segmentation logique et/ou physique des zones;
- des analyses de la vulnérabilité, soutenues par un système de détection et de prévention d'intrusion.

☞ Pour de plus amples informations, lire la recommandation, qui est disponible sur le site internet de l'autorité belge chargée de la protection des données en [français](#) et en [néerlandais](#).

> Les règles d'entreprise contraignantes de l'UE et les règles transfrontalières de protection de la vie privée de la CEAP

Les 21 pays de la Coopération économique Asie-Pacifique (CEAP), dont les États-Unis, le Canada, le Japon, la Chine, la Russie, la Corée du Sud et l'Australie, ont récemment mis au point un système de règles transfrontalières de protection de la vie privée (CBPR) en vue de protéger la vie privée et d'apporter des garanties aux transferts de données.



Les CBPR sont similaires aux règles d'entreprise contraignantes (REC) qui s'appliquent aux transferts européens de données.

Ainsi, ces deux types de règles s'appliquent aux transferts internationaux conçus par les entreprises et sont revus, a priori, par les autorités chargées de la protection des données ou par des tiers autorisés.

Par conséquent, le groupe de travail «Article 29» a décidé qu'il était nécessaire d'œuvrer en vue d'une double «certification» pour les procédures de respect des CBPR-REC.

À cette fin, des représentants de la CNIL (Commission nationale française de l'informatique et des libertés), le commissaire fédéral allemand à la protection des données et à la liberté de l'information (BfDI), le CEPD et la Commission européenne se sont réunis fin janvier à Jakarta pour la première fois avec le comité REC et les membres de la CEAP responsables des CBPR afin de partager leurs points de vue sur ce projet.

Cette réunion fructueuse a débouché sur un accord en vue de concevoir des outils qui pourraient être utilisés par les multinationales actives tant au sein de l'UE que dans la région de la CEAP. Une feuille de route sera probablement adoptée au cours des prochains mois par les membres du groupe de travail «Article 29» et la CEAP en vue de poursuivre cette coopération et de mettre ces outils en œuvre.

☞ [Communiqué de presse](#) de la CNIL

> 28 janvier: Journée de la protection des données

Le 28 janvier 2013, les 47 pays membres du Conseil de l'Europe ainsi que les institutions, agences et organes de l'UE ont célébré la septième Journée européenne de la protection des données. Cette date marque l'anniversaire de la Convention 108 du Conseil de l'Europe pour la protection des données à caractère personnel, le premier instrument international juridiquement contraignant dans le domaine de la protection des données.

Cet événement annuel a été, cette année encore, l'occasion pour le CEPD et les délégués à la protection des données des institutions de l'UE de sensibiliser le personnel des institutions de l'UE et le grand public à leurs droits et obligations en matière de protection des données. Ces droits et obligations sont établis par le règlement de l'UE relatif à la protection des données et leur mise en œuvre au sein de l'administration de l'UE est contrôlée par le CEPD.

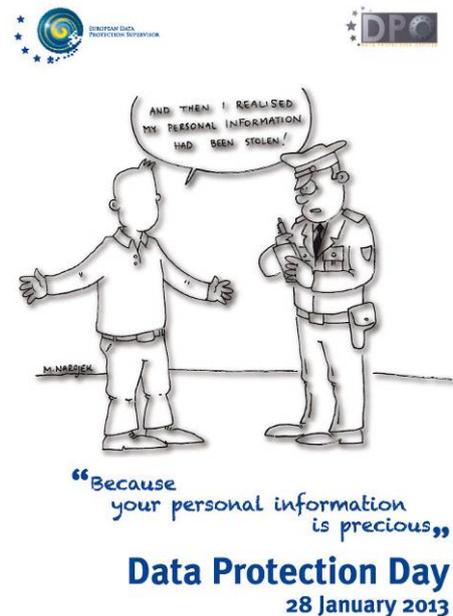
Dans le cadre de nos efforts de sensibilisation, nous avons réalisé une petite vidéo afin d'illustrer, de manière divertissante et informative, certains droits et risques liés à la protection des données dans notre vie quotidienne.

Afin de célébrer cet événement, nous avons également organisé, en coopération avec le Parlement européen (PE), une conférence commune intitulée *What will the data protection reform change for EU officials and citizens? (Quelles seront les incidences de la réforme de la protection des données pour les fonctionnaires et les citoyens de l'UE?)*. Cette conférence a rencontré un franc succès, seules quelques places debout étaient encore disponibles quelques minutes avant le début du discours de bienvenue prononcé par le secrétaire général du PE, Klaus Welle. Après quelques brèves présentations, Peter Hustinx, Contrôleur, Giovanni Buttarelli, contrôleur adjoint, et M. Paul De Hert, professeur à la *Vrije Universiteit Brussel* ont participé à un débat.

Nous avons également co-sponsorisé l'exposition *A look inside*, une exposition d'œuvres d'art originales axée sur le respect de la vie privée et la surveillance, en collaboration avec la *Vrije Universiteit Brussel* et la Commission belge de la protection de la vie privée. Se tenant au parc des expositions «De Markten» à Bruxelles, cette exposition présentait les œuvres de jeunes artistes européens, qui ont mis à profit leur expression artistique pour provoquer un débat sur le respect de la vie privée et son importance dans la vie quotidienne moderne.

⇨ [Discours](#) de Peter Hustinx prononcé lors de la réception à l'occasion de l'exposition d'œuvres d'art relatives au respect de la vie privée, 28.1.2013

⇨ [Message vidéo du CEPD](#) à l'occasion de la Journée de la protection des données 2013





Chaque année, la conférence CPDP réunit des responsables politiques, des universitaires, des informaticiens, des consultants, des praticiens et des activistes du monde entier afin de leur permettre d'échanger leurs idées et de discuter de questions qui se posent dans les domaines des technologies de l'information, du respect de la vie privée, de la protection des données et de la législation. Cette année, la conférence était intitulée «Computers, Privacy and Data Protection (CPDP) 2013: Reloading Data Protection». Ce forum a permis d'aborder des sujets comme la guerre de l'information, la liberté sur l'internet et l'introduction de drones dans l'espace aérien civil de l'UE. D'importants débats sur la proposition de règlement relatif à la protection des données ont également eu lieu lors de cette conférence. Plusieurs collègues du CEPD ont participé aux débats. Giovanni Buttarelli a pris la parole au sujet de la proposition de règlement relative à la protection des données lors du débat d'ouverture, tandis que Peter Hustinx a prononcé le discours de clôture de la conférence.

☞ [Site internet de la conférence CPDP](#)

> Présentation de la stratégie du CEPD pour 2013-2014

Le 22 janvier 2013, le CEPD a présenté un rapport décrivant notre **stratégie pour 2013-2014** à une série de hauts représentants des institutions européennes. Tant les contrôleurs que le directeur ou encore les membres du conseil d'administration ont décrit le processus, les objectifs et les résultats d'une analyse approfondie, y compris les grandes lignes de la stratégie 2013-2014. La présentation du CEPD a été suivie d'une allocution de la vice-présidente de la Commission, **Viviane Reding**, de la commissaire **Cecilia Malmström**, de la vice-présidente de la commission LIBE du Parlement, **Sophie in't Veld**, et du coordinateur de l'UE pour la lutte contre le terrorisme, **Gilles de Kerchove**.



Notre stratégie 2013-2014 repose sur une révision stratégique entamée en juillet 2011. L'objectif de cette révision était d'identifier les priorités et de répondre à la **charge de travail croissante** ainsi qu'à **l'élargissement du champ des activités** auxquels le CEPD devra faire face dans les années à venir. Par notre expertise, notre autorité et nos pouvoirs formels, nous avons pour objectif de continuer à renforcer la **sensibilisation** à la protection des données comme un droit fondamental et un élément essentiel de la bonne politique et administration publiques des institutions européennes. En agissant **de manière sélective et proportionnelle**, nous voulons nous assurer que la protection des données fera partie intégrante de l'élaboration des politiques et de la législation, dans tous les domaines de compétence de l'UE.

En particulier, nous avons identifié les activités qui mettent l'accent sur la **responsabilisation** des décideurs et des responsables du traitement, ainsi que les activités qui s'appuient sur le rôle crucial des **délégués à la protection des données (DPD)**. Ces activités sont des éléments clés des réformes législatives proposées et indiqueront la manière d'élever les niveaux de conformité dans une période de restrictions budgétaires.



Nous continuerons à développer et à construire notre stratégie en vue de répondre efficacement au défi consistant à **atteindre l'excellence en matière de protection des données** au niveau européen au-delà de 2014.

- ☞ [Stratégie 2013-2014](#)
- ☞ [Communiqué de presse](#) sur la stratégie 2013-2014
- ☞ [Vidéo](#): Faits marquants de la présentation de la stratégie du CEPD 2013-2014

> Atelier sur la proposition de règlement relatif à la protection des données, Varsovie, 12 décembre 2012

Le contrôleur adjoint et plusieurs collègues ont participé à un atelier organisé par l'autorité polonaise chargée de la protection des données afin de débattre avec les fonctionnaires polonais des conséquences de la proposition de règlement relatif à la protection des données.



Un certain nombre de questions et de préoccupations ont été soulevées quant aux incidences de cette proposition de règlement pour les questions intérieures et certains participants ont souligné la nécessité d'apporter des améliorations à cette proposition. Les participants ont, entre autres, abordé les thèmes suivants: la collecte d'informations à caractère personnel à des fins statistiques et les limites que la proposition prévoit à cet égard, les incidences sur le traitement des informations à caractère personnel par les juridictions nationales, le manque de clarté en matière de droit à un recours juridictionnel, et le traitement des données relatives aux enfants.

Le fait qu'il puisse être nécessaire de modifier certaines législations sectorielles existantes qui prévoient actuellement des solutions efficaces en raison de certaines dispositions de la proposition de règlement suscite une crainte générale sur le plan national. Par exemple, la législation polonaise du travail contient une disposition limitant le traitement des données par les employeurs.



Nous avons tiré une double conclusion de cet atelier très productif: un dialogue accru avec les États membres (et les administrations nationales) est nécessaire afin de discuter d'une corrélation entre la proposition de règlement et les lois nationales qui laisse une marge de manœuvre permettant le maintien des législations sectorielles nationales.

En outre, cette proposition de règlement pourrait être améliorée sur certains points: l'étendue de son application aux juridictions, la définition de l'exemption domestique, l'harmonisation des règles du forum en matière de protection des données avec d'autres types de demandes, les règles en matière de statistiques pour permettre la reconnaissance de règles sectorielles spécifiques en vigueur définies au niveau national.



DISCOURS ET PUBLICATIONS

- "Le respect de la vie privée doit devenir un automatisme", interview de Peter Hustinx ([pdf](#)) dans De Tijd (22 février 2013)
- "The role of data protection legislation" (Le rôle de la législation en matière de protection des données) ([pdf](#)), contribution écrite de Peter Hustinx à l'occasion de la conférence «Security of e-Government» (La sécurité de l'administration en ligne), Parlement européen, Bruxelles (19 février 2013)
- "A Look Inside" ([pdf](#)), discours prononcé par Peter Hustinx lors de la réception à l'occasion de l'exposition organisée en collaboration avec la *Vrije Universiteit Brussel* (VUB) et la Commission belge de la protection de la vie privée (CBPL-CPVP), Bruxelles (28 janvier 2013)
- "Présentation des rapports sur la proposition de règlement général sur la protection des données et sur la proposition de directive sur le traitement des données à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière" ([pdf](#)), schéma d'intervention de Giovanni Buttarelli, réunion de la commission des libertés civiles, de la justice et des affaires intérieures, Parlement européen, Bruxelles (10 janvier 2013)
- "Loi européenne relative à la protection des données – situation actuelle et perspectives d'avenir" ([pdf](#)), discours prononcé par Peter Hustinx lors de la conférence de haut niveau "Dimensions éthiques de la protection des données et de la vie privée", Centre pour l'éthique, Université de Tartu / Inspection de la protection des données, Tallinn (9 janvier 2013).



DÉLÉGUÉS À LA PROTECTION DES DONNÉES

Chaque institution ou organe européen doit nommer au moins une personne en tant que délégué à la protection des données (DPD). La tâche de ces délégués est d'assurer de manière indépendante la mise en œuvre des obligations de protection des données établies par le règlement (CE) n° 45/2001 au sein de leur institution ou organe.

☞ 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 et GIODO

 **Suivez-nous sur Twitter: @EU_EDPS**

COORDONNEES

www.edps.europa.eu

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

Fax: +32 (0)2 283 19 50

NewsletterEDPS@edps.europa.eu

ADRESSE POSTALE

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 personnelles