

LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

Newsletter du CEPD

N° 43 | Octobre 2014

DANS CE NUMÉRO

FAITS MARQUANTS

- 1 Nomination prochaine des nouveaux Contrôleurs

SUPERVISION

- 1 Transferts de données internationaux: assurer la protection des données de l'UE à l'étranger
- 2 Votre messagerie est-elle ultraconfidentielle?
- 2 Répondre aux demandes d'accès à des documents
- 2 La cohérence grâce à la coopération
- 2 Conformité accrue grâce à une action ciblée
- 3 Bonne santé des normes relatives à la protection des données
- 3 Traitement des allégations de faute professionnelle
- 3 Conduire une enquête efficace

CONSULTATION

- 3 Assurer la protection des données
- 4 Espace: la dernière frontière
- 4 Étendre ses activités devient plus simple
- 4 Plateforme dédiée au partage de données en Europe
- 4 Un portail dédié à la justice dans l'ensemble de l'UE

IT POLICY

- 5 Des politiques intelligentes pour des réseaux intelligents
- 5 Préserver la mobilité des institutions de l'UE

ÉVÉNEMENTS

- 5 Atelier IPEN: technologie et respect de la vie privée
- 6 «Trois années de réforme de la protection des données dans l'UE: bilan et perspectives» (Bruxelles)
- 6 Lancement du concours de l'UE sur la protection des données
- 6 Votre avis sur la newsletter du CEPD

DISCOURS ET PUBLICATIONS

DÉLÉGUÉS À LA PROTECTION DES DONNÉES

FAITS MARQUANTS

Nomination prochaine des nouveaux Contrôleurs

Au cours des semaines à venir, une nouvelle équipe de Contrôleurs devrait être nommée au sein du CEPD. Bien que l'adoption d'une décision officielle par le Parlement européen et le Conseil puisse prendre quelques semaines, toutes les informations disponibles suggèrent que Giovanni Buttarelli, actuel CEPD adjoint, deviendra le nouveau Contrôleur, et que Wojciech Wiewiórowski, inspecteur général de la protection des données personnelles en Pologne, deviendra le nouveau CEPD adjoint. Peter Hustinx, actuel Contrôleur, quittera ses fonctions après plus de dix ans à ce poste. Une passation des pouvoirs officielle est prévue le jour de l'entrée en vigueur des nouveaux mandats.

Durant les deux mandats précédents, le CEPD a été créé, a acquis une visibilité croissante en tant qu'institution, et a développé son rôle de contrôle des institutions et organes de l'UE. Il a également conseillé la Commission, le Parlement et le Conseil sur les nouvelles politiques et la nouvelle législation, ainsi que la Cour de justice dans les cas appropriés, et a coopéré avec les autorités nationales de protection des données afin d'améliorer la cohérence

de la protection des données dans l'UE. Au cours des derniers mois, le CEPD a pris d'autres initiatives concernant le respect de la vie privée et la technologie (voir la page 6 - IPEN), ou le respect de la vie privée et la concurrence à l'ère des données massives.

La nouvelle équipe entrera en fonction à un moment critique, avec la persistance de grands défis. La priorité fondamentale consiste à soutenir l'adoption d'un nouveau cadre juridique européen de protection des données en 2015, et de préférence d'ici le printemps prochain. C'est une condition essentielle pour que le respect de la vie privée et la protection des données continuent à jouer leur rôle clé dans le marché intérieur numérique. Le CEPD devrait assurer le secrétariat du comité européen de la protection des données, qui contribuera à garantir la cohérence de la supervision et de l'application du nouveau cadre dans l'ensemble de l'UE. Ceci nécessitera dévouement et diplomatie de la part de la nouvelle équipe de contrôleurs et du personnel.

Les institutions et les organes de l'UE devront parallèlement veiller à ce que les exigences relatives à la protection

de la vie privée et des données soient inscrites dans leur utilisation de l'informatique dématérialisée et d'autres services numériques inédits. Il faudra évaluer la conformité des initiatives politiques annoncées par la nouvelle Commission avec les exigences relatives à la protection de la vie privée et des données, telles qu'énoncées dans la Charte et les cadres juridiques applicables. Les négociations entre l'UE et les États-Unis concernant les accords transatlantiques sur le commerce et l'investissement ou le partage des données relatives au respect des lois feront partie des nombreux sujets réclamant l'attention de la nouvelle équipe de contrôleurs.

Les numéros antérieurs de la newsletter ont décrit la croissance rapide et l'impact grandissant du CEPD en tant qu'institution dédiée aux bonnes pratiques en matière de protection des données et de la vie privée. Nous continuerons à vous informer, en vous exposant comment la nouvelle équipe de contrôleurs gère et développe l'héritage précieux et les ressources de notre institution dans l'intérêt des citoyens européens.

SUPERVISION

Transferts de données internationaux: assurer la protection des données de l'UE à l'étranger

Le 14 juillet 2014, le CEPD a adopté un *document d'orientation* destiné à fournir des conseils aux institutions et organes de l'UE sur l'interprétation et l'application des règles énoncées dans le règlement (CE) n° 45/2001, lors du transfert international de données à caractère personnel.

Les *institutions et organes de l'UE* ont de plus en plus besoin de transférer des informations personnelles à des pays tiers ou des organisations internationales. À titre d'exemple, les transferts de données internationaux sont nécessaires pour faciliter la coopération transfrontalière, afin de permettre la mise en œuvre réussie des projets de l'UE à l'extérieur ou de contribuer à la résolution des enquêtes de l'UE. Par ailleurs, l'UE utilise plus de services externes que jamais

auparavant, dans des domaines tels que l'informatique ou la traduction. Toutes ces activités impliquent le transfert et le partage de données, et le nouveau document d'orientation du CEPD fournit des conseils concrets sur l'interprétation des règles dans ce domaine.

Nos orientations se concentrent principalement sur la notion de «protection adéquate» et sur son applicabilité, et sur la manière d'évaluer l'*adéquation*. Nous analysons aussi les exceptions aux exigences d'adéquation et nous étudions la mise en place de garanties appropriées lorsque le pays bénéficiaire ne fournit pas un niveau adéquat de protection des données. Des exemples sont donnés pour faciliter la tâche des *responsables du traitement* et des *délégués à la protection des données* (DPD)

lors de l'application des règles, ainsi qu'une liste de contrôle incluant les étapes à suivre pour appliquer l'article 9 du règlement n° 45/2001. Le document fournit également des informations pertinentes sur les rôles de contrôle et d'exécution du CEPD dans le contexte des transferts de données.

[Document d'orientation du CEPD](#)



Votre messagerie est-elle ultraconfidentielle?

Le CEPD a reçu une plainte d'un ancien membre du personnel d'un organe de l'UE, qui alléguait que son adresse électronique (prénom.nom@organe.europa.eu) n'avait pas été désactivée après son départ. Son compte de messagerie électronique était resté ouvert, et tous les courriers électroniques qu'il recevait étaient transférés à la boîte aux lettres fonctionnelle générale de l'organe de l'UE concerné, devenant ainsi accessibles à de nombreux membres du personnel.

Nous avons jugé que la non-désactivation de la messagerie électronique du plaignant après son départ constituait une atteinte

aux règles de sécurité du règlement n° 45/2001. En outre, le transfert automatique subséquent des messages du plaignant à la boîte aux lettres fonctionnelle générale enfreignait les règles de sécurité, et était de plus illégal dans la mesure où il n'était pas nécessaire.

Dans notre décision du 17 juillet 2014, nous observons que le transfert de courriers électroniques depuis la messagerie d'un ancien employé ne devrait être possible que dans des circonstances exceptionnelles, s'il peut être justifié par des raisons de continuité opérationnelle. Par conséquent, l'organe de l'UE

en question aurait pu choisir des mesures moins préjudiciables au respect de la vie privée dans le cadre de cette affaire. Il aurait pu envisager les options suivantes:

1) mettre en place une réponse automatique pour la messagerie individuelle, invitant les expéditeurs à envoyer les correspondances importantes à une autre adresse électronique; ou

2) donner à une personne, en coopération avec le délégué à la protection des données (DPD), l'autorisation d'accéder à la messagerie.

De plus, l'organe de l'UE aurait dû informer le plaignant lorsqu'il a décidé de faire suivre ses cour-

riers électroniques, afin que le plaignant puisse exercer son droit d'opposition.

Nous avons demandé à l'organe de l'UE d'intervenir immédiate-

ment, et nous effectuerons un suivi en temps opportun, afin de vérifier que les mesures nécessaires ont été prises pour remédier à la situation.



Répondre aux demandes d'accès à des documents

Le CEPD a enquêté sur une demande d'accès à des documents impliquant la Commission européenne. Cette dernière avait prié le demandeur de lui communiquer son adresse postale, et il avait jugé cette demande excessive.

La collecte de ces informations personnelles nous semble toutefois légitime, pour plusieurs raisons:

- garantir une sécurité juridique concernant la date de réception de la réponse,
- rejeter les demandes d'accès sous une fausse identité,
- vérifier si la personne demandant l'accès aux documents est établie dans l'Espace économique européen (EEE).

En nous fondant sur ces raisons, nous avons décidé que demander l'adresse postale d'un demandeur ne constituait pas une exigence excessive dans le cas de

demandes d'accès à des documents. Il importe néanmoins de fournir aux demandeurs des informations expliquant pourquoi leurs coordonnées postales sont nécessaires. La Commission inclut donc désormais ces informations dans sa déclaration de confidentialité.



La cohérence grâce à la coopération

L'une des tâches du CEPD, énoncée dans le règlement relatif à la protection des données, consiste à améliorer la cohérence dans l'application des règles relatives au traitement des données à caractère personnel dans l'ensemble de l'Union européenne. Cette tâche implique notamment de coopérer et de partager des connaissances avec les autorités chargées de la protection des données (APD) dans l'UE.

À cette fin, nous rendons visite aux APD. Ces visites nous permettent de mieux comprendre le fonctionnement des autres APD et les défis qu'elles rencontrent. Elles nous aident à échanger nos connaissances et encouragent ainsi une coopération plus profitable à l'avenir. Cet aspect est d'autant plus pertinent que la nouvelle réforme de la protection des données, prévue dans

un avenir proche, signifie que tous les organes de protection des données ont intérêt à anticiper les changements à venir.

Nous avons donc rendu visite à l'APD espagnole le 18 juillet 2014, dans l'objectif principal d'échanger des expériences sur des questions précises de contrôle et d'exécution, telles que le rôle

des DPD, l'intervention dans les affaires soumises aux tribunaux, l'accès aux documents publics, et les plaintes concernant l'accès aux données personnelles. Les discussions fructueuses menées à cette occasion faciliteront incontestablement l'adaptation aux nouvelles règles.



Conformité accrue grâce à une action ciblée

Dans certains cas, le CEPD utilise les visites en tant qu'outils de conformité. Elles nous permettent de prendre des mesures ciblées en incitant une institution ou une agence à respecter le règlement. Dans le passé, les visites se sont révélées particulièrement utiles pour sensibiliser les institutions et les aider à assumer leurs responsabilités en matière de protection des données: la quasi-totalité des huit organes de l'UE inspectés en 2012 et 2013 ont connu depuis une amélioration considérable de leur taux de conformité.

Dans ce contexte, nous avons rendu visite en juillet 2014 au Centre satellitaire de l'UE (CSUE) et à l'Agence du GNSS européen

(GSA), qui n'offraient ni l'un ni l'autre un niveau de conformité satisfaisant en matière de protection des données, selon *l'enquête du CEPD en 2013*.

Lorsque nous avons mené notre enquête, la communication s'est révélée problématique: aucune des deux agences n'a répondu à notre enquête en fournissant des preuves suffisantes de conformité satisfaisante dans les délais que nous avons fixés. En raison de ces difficultés, nous avons décidé d'effectuer des visites au niveau opérationnel. Les responsables du dossier au CEPD ont donc organisé des formations et des sessions de questions-réponses, afin d'apporter une aide pratique à chaque agence et



d'enseigner au personnel et à la direction comment intégrer de manière optimale les principes de protection des données dans leur environnement de travail. La visite incluait des discussions sur des questions variées, de la gestion des ressources humaines à la sécurité informatique ou aux tâches de divers acteurs de l'organisation associées à la protection des données. Les deux agences se sont fortement impliquées et se sont engagées à améliorer le respect des principes de protection des données. Nous prévoyons une autre visite de ce type à l'Institut d'études de sécurité de l'Union européenne (IESUE) en octobre 2014, et nous espérons obtenir une réaction tout aussi positive.



Bonne santé des normes relatives à la protection des données

En vertu du règlement n° 45/2001, les *institutions et organes de l'UE* sont tous responsables devant leur autorité de contrôle, le CEPD. En d'autres termes, ils sont chargés d'assurer et de démontrer leur respect des règles de protection des données, et une inspection du CEPD leur offre l'occasion d'exercer cette responsabilité.

Durant les mois de mars et d'avril 2014, nous avons mené des inspections thématiques ciblées dans le service médical de la Commission et dans le service médical et l'unité sociale du Conseil. Ces inspections étaient importantes, à la fois en raison de la taille des institutions (et donc de la quantité de données qu'elles traitent), et de la nature particulièrement sensible et privée des données impliquées. Nos inspections se sont concentrées sur l'obligation du secret pro-

fessionnel pour le personnel non médical, tels les secrétaires et les travailleurs sociaux; le traitement des informations personnelles concernant les employés de la Commission et du Conseil; et les mesures de sécurité matérielle et organisationnelle utilisées pour protéger les données relatives à la santé traitées par les deux institutions.

Selon les conclusions de nos rapports d'inspection du 23 juillet 2014, sous réserve de quelques mesures d'amélioration, les deux institutions se conforment aux règles applicables en matière de protection des données personnelles. Nous nous félicitons des résultats positifs de ces inspections récentes, qui offrent un bon exemple d'application du principe de responsabilité dans un domaine sensible, au sein de deux grandes institutions.

Traitement des allégations de faute professionnelle

Afin de garantir des normes optimales d'intégrité de la recherche, l'Agence exécutive du Conseil européen de la recherche (ERCEA) a élaboré une procédure permettant de traiter toute information reçue à propos d'une *faute professionnelle* présumée. Ce terme couvre une vaste gamme de cas possibles, tels que la fraude et la violation des réglementations.

Dans le contexte des propositions soumises au Conseil européen de la recherche (ERC) ou des projets financés par une subvention de l'ERC, la notion de faute professionnelle, interprétée au sens large, s'applique à chaque fois que le comportement d'une personne compromet la valeur de la science et, en particulier, la réputation des membres de la communauté scientifique, et des organes qui financent ou accueillent ces scientifiques. À titre d'exemple, si un auteur commet un plagiat ou ne respecte pas les normes éthiques lorsqu'il soumet une proposition à l'ERC, il est jugé coupable de faute professionnelle.

L'Agence reçoit des allégations de faute professionnelle sous



diverses formes, y compris de manière anonyme. Nous avons traité ces questions dans notre *avis* du 9 juillet 2014. Nous avons souligné combien il est important de prendre des mesures adéquates pour garantir un haut niveau d'exactitude lors du traitement des données à caractère personnel. Nous nous sommes également félicités du fait que la personne ayant prétendument enfreint les bonnes pratiques scientifiques ait l'opportunité de faire connaître ses observations sur les allégations à son encontre. Nous avons aussi noté que l'ERCEA accordait une attention spéciale à toutes les personnes (informateurs

par exemple) dont les données pourraient être collectées dans le cadre de la procédure. Nous avons souligné que leur identité devait rester confidentielle, aussi longtemps que ceci n'enfreignait pas les règles nationales relatives aux procédures judiciaires. Nous avons rappelé à l'ERCEA que les personnes concernées devaient être informées des principales raisons de toute restriction de leur droit d'accès à leurs données et de leur droit de consulter le CEPD dans de tels cas, conformément aux *lignes directrices* du CEPD sur les droits des individus concernant le traitement des données à caractère personnel.

[Avis du CEPD](#)

Conduire une enquête efficace

Le CEPD a formulé un *avis* sur le projet de l'Office européen de lutte antifraude (OLAF) concernant le lancement d'une analyse des services fournis par les ressources humaines. Dans le cadre de son plan stratégique en matière de ressources humaines (RH), l'institution entend élaborer une stratégie des RH qui réponde davantage aux besoins des employés.

Chaque supérieur hiérarchique fera passer un entretien individuel à chaque titulaire de poste. Les réponses seront retranscrites dans un questionnaire normalisé incluant diverses rubriques, telles que le poste occupé dans l'unité,

les études, les compétences professionnelles, la formation préalable, la comparaison avec le profil idéal et les besoins en matière de formation. Les questionnaires complétés seront remis à l'unité «Ressources humaines» de l'OLAF pour être analysés, et les supérieurs hiérarchiques seront priés de ne conserver aucune copie des questionnaires complétés et de ne pas utiliser les données à des fins d'évaluation des performances.

Notre avis s'est concentré sur la nécessité de garantir l'exactitude des données collectées. À cet effet, nous préconisons de demander aux membres du personnel de signer le

questionnaire rempli par leur directeur durant l'entretien. Par ailleurs, les membres du personnel doivent clairement comprendre pourquoi des données sont collectées à leur sujet. En conséquence, nous avons également recommandé de préciser à tous les participants que, même si les données réunies dans le contexte de «l'analyse des besoins» ne sont pas utilisées à des fins d'évaluation des performances, elles contribueront à l'élaboration de plans de formation individuels, qui font l'objet d'un suivi dans le cadre de l'évaluation du personnel par le supérieur hiérarchique.

[Avis du CEPD](#)



CONSULTATION

Assurer la protection des données

Le 11 juillet 2014, le CEPD a publié un *avis* sur deux propositions de la Commission. La première concernait la résilience du système bancaire européen et la seconde la déclaration et la transparence des opérations de financement sur titres ou, plus simplement, les activités de prêt et d'emprunt associées au *système bancaire parallèle*.

Comme pour les précédentes propositions concernant la réglementation des services financiers, nous avons préconisé de mettre en œuvre des garanties adéquates contre un mauvais traitement des informations personnelles. À titre d'exemple, nous avons recommandé que, en cas d'infraction aux règles, la publi-

cation d'avertissements et de sanctions concernant l'individu identifié ne soit pas automatique. Au lieu de quoi, chaque individu devra être soumis à une évaluation spécifique, en tenant compte de la proportionnalité et de la nécessité de publier ses données personnelles.

[Avis du CEPD](#)



L'espace: la dernière frontière

Le 11 juillet 2014, le CEPD a publié des commentaires sur une proposition de directive, présentée par la Commission, relative à la diffusion de données satellitaires d'observation de la terre à des fins commerciales.

La directive proposée vise à définir les règles de diffusion des données satellitaires à haute résolution (DSHR). Les DSHR sont produites par les opérateurs de satellites, puis transmises par les fournisseurs de données au secteur des «services à valeur ajoutée», qui comprennent notamment les prestataires de services de géo-information. Ces derniers sont des opérateurs commerciaux qui combinent les

données satellitaires à d'autres informations utiles aux clients. Le produit final est ensuite transmis aux entreprises qui le demandent.

Nous avons souligné dans nos *commentaires* que, malgré l'absence théorique de préoccupations relatives à la protection des données à l'heure actuelle, la combinaison de DSHR avec des données provenant du secteur des services à valeur ajoutée pouvait conduire, dans bien des cas, au traitement de données relatives à des personnes physiques directement ou indirectement identifiables. Nous avons donc souligné que ces données devaient être traitées confor-

mément aux dispositions établies dans la directive 95/46/CE et aux dispositions législatives nationales prises pour la mettre en œuvre.

De plus, nous avons remarqué que la technologie des DSHR ne permettait pas encore d'identifier directement des personnes, mais que les avancées technologiques pourraient rendre une telle identification possible à l'avenir. Nous avons donc recommandé que la Commission envisage cette éventualité en incluant un article sur la protection des données dans la proposition.

Commentaires du CEPD



Étendre ses activités devient plus simple

La proposition de la Commission relative aux sociétés unipersonnelles à responsabilité limitée est destinée à donner à tout créateur d'entreprise potentiel, en particulier aux PME, la possibilité d'établir plus facilement des sociétés dans d'autres États membres de l'UE. Elle entend à cet effet «harmoniser les conditions de création et d'activité des sociétés unipersonnelles à responsabilité limitée». Afin de garantir la transparence, la proposition nécessite l'enregistrement et/ou la publication de certaines informations concernant la société unipersonnelle,

qui peuvent inclure des données à caractère personnel.

Dans notre *avis* du 23 juillet 2014, nous nous sommes félicités des garanties incluses par la Commission dans la proposition, telle la limitation de la collecte de données relatives à l'exclusion aux cas où celle-ci est encore en vigueur. Ceci signifie qu'aucune donnée historique ne sera traitée. Nous avons également approuvé le fait que la Commission envisage la possibilité d'échanges d'informations par l'intermédiaire du système d'information sur le marché intérieur (IMI).

Il est toutefois possible d'améliorer certains points. Nous avons notamment recommandé que la proposition:

- précise plus clairement quelles données à caractère personnel peuvent être échangées par l'intermédiaire de l'IMI, et notamment si des informations supplémentaires peuvent être collectées concernant les exclusions,
- précise plus clairement quels documents doivent être rendus publics et indique que toute publication d'informations sera uniquement soumise aux mesures de protection des données prévues par la législation nationale,
- précise que les données à caractère personnel rendues publiques en vertu de la proposition ne peuvent être utilisées qu'à des fins de transparence et de responsabilité,
- veille à ce que des mesures d'ordre technique et organisationnel soient prises pour limiter dans le temps l'accessibilité de toute information relative aux personnes physiques figurant dans les registres.

Avis du CEPD

Plateforme dédiée au partage de données en Europe

Dans le cadre de sa proposition visant à renforcer la coopération entre les autorités nationales chargées de faire appliquer la législation, la Commission et les autres organisations pertinentes, en vue de prévenir et de décourager le travail non déclaré, la Commission a proposé de créer une «plateforme européenne». Cette plateforme, composée des autorités nationales chargées de faire appliquer la législation et de la Commission, sera utilisée pour: «étudier les moyens d'améliorer le partage des données dans le respect des règles de protection des données de l'Union, y compris les possibilités d'utiliser le système d'information du marché intérieur (IMI) et l'échange électronique d'informations sur la sécurité sociale (EESSI)».

Dans le cadre de cette proposition, le partage d'informations portera uniquement sur les informations relatives aux mesures et politiques mises en place par les États membres de l'UE pour lutter contre le travail non déclaré. À ce stade, le partage d'informations ne s'applique pas aux données à caractère personnel

des travailleurs non déclarés, ni à celles des personnes physiques ou organisations employant des travailleurs sans les déclarer.

Le CEPD a publié ses *commentaires* concernant cette proposition le 23 juillet 2014. Nous nous sommes félicités du fait qu'elle ne fournisse, de fait, pas de base juridique sous-tendant l'échange de données à caractère personnel, mais fournisse plutôt une base juridique à l'élaboration de mécanismes visant à améliorer l'échange de données à caractère personnel. Une fois que la Commission proposera des plans précis quant aux échanges de données à caractère personnel par l'intermédiaire de cette plateforme, nous lui adresserons des orientations et conseils supplémentaires à ce sujet.

Commentaires du CEPD



Un portail dédié à la justice dans l'ensemble de l'UE

Le 5 septembre 2014, le CEPD a publié un avis sur la protection des données à caractère personnel sur le portail européen e-Justice. Ce portail, conçu et géré par la Commission en coopération étroite avec les États membres de l'UE, a été lancé en 2010. Il vise à faciliter la coopération judiciaire et l'accès à la justice et aux procédures judiciaires électroniques transfrontières. Toutefois, afin d'atteindre ces objectifs, tous les registres nationaux doivent être combinés, et ce processus comporte des risques pour la protection des données.



Afin d'atténuer ces risques, nous avons encouragé la Commission à accroître ses efforts pour adopter le nouveau règlement sur l'e-Justice. Nous avons également fourni à la Commission des recommandations préliminaires concernant l'élaboration du futur règlement, ainsi qu'une liste non exhaustive de points à prendre en compte lors de la mise en place du portail, notamment:

- le champ d'application du portail (quelles bases de données nationales spécifiques seront interconnectées par l'intermédiaire du portail, et quels services interactifs seront fournis),

• les fondements juridiques du traitement de données dans le portail,

• les responsabilités spécifiques de la Commission et des diverses autres parties concernées en tant que *responsables du traitement* ou *sous-traitants*, y compris en ce qui concerne la sécurité et la protection des données dès la conception,

• la limitation de la finalité et les restrictions applicables, le cas échéant, à la combinaison de données.

Avis du CEPD



Des politiques intelligentes pour des réseaux intelligents

Le 9 mars 2012, la Commission a publié une [recommandation](#) relative à la préparation de l'introduction des systèmes intelligents de mesure. Cette recommandation était destinée à fournir des orientations aux États membres de l'UE et à garantir un niveau élevé de sécurité et de protection pour les données personnelles des consommateurs.

Dans notre [avis](#) du 8 juin 2012, nous nous sommes félicités des

efforts accomplis par la Commission pour offrir des orientations aux États membres de l'UE, tout en estimant que ces orientations pourraient être plus précises, complètes et concrètes. Nous étions particulièrement enthousiasmés par le projet de la Commission de développer un modèle pour l'analyse de l'impact sur la protection des données. Ce modèle pourrait être utilisé par les États membres de l'UE pour

évaluer l'impact potentiel du traitement des données personnelles des consommateurs utilisant des compteurs et des réseaux intelligents.

En conséquence, la Commission a chargé le [groupe de travail sur les réseaux intelligents](#), de concert avec des représentants du secteur énergétique, de produire un projet de modèle. Ce projet a été soumis deux fois à l'avis du groupe de travail «Article 29», et le CEPD a joué un rôle clé dans le travail d'évaluation effectué.

Le modèle va désormais entrer dans une phase d'essai, avant d'être intégré à une nouvelle recommandation de la Commission, qui définira le contexte et les modalités de son examen et de sa révision. Le modèle sera accompagné d'un document sur les meilleures techniques disponibles (MTD), auquel le CEPD contribue activement à travers les travaux du forum des parties prenantes sur les MTD en matière de compteurs intelligents, qui a débuté ce mois-ci. Nous continuerons à offrir un soutien à la Commission pour toutes les questions liées aux compteurs et réseaux intelligents, afin de trouver des solutions viables pour atténuer tous les risques en matière de protection des données.



Préserver la mobilité des institutions de l'UE

Les appareils mobiles sont de plus en plus présents dans le travail quotidien des institutions de l'UE. Ils sont fournis aux dirigeants et au personnel pour répondre à des besoins professionnels spécifiques, tandis que d'autres membres du personnel de l'UE sont autorisés à utiliser leurs propres appareils mobiles afin d'être aidés dans leurs tâches. Les institutions de l'UE ont non seulement trouvé une manière de s'adapter au besoin toujours croissant de mobilité au sein des institutions, mais elles ont aussi observé une satisfaction accrue chez leurs effectifs et des économies de coûts.

Ces avantages doivent toutefois s'accompagner d'une stratégie efficace de protection des données. Le CEPD lancera prochainement un processus de consultation avec les [institutions et organes de l'UE](#), afin

d'élaborer des lignes directrices concernant la protection des données personnelles sur les appareils mobiles utilisés par les institutions de l'UE. Ces lignes directrices, qui s'adresseront principalement aux délégués à la protection des données, ainsi qu'au personnel des technologies de l'information (TI) et de la sécurité informatique, fourniront des conseils pratiques concernant le traitement des données à caractère personnel dans le cadre des appareils mobiles. Elles incluront aussi une «boîte à outils» qui offrira des conseils sur le processus de gestion des risques, expliquant comment évaluer les risques induits par l'utilisation des appareils mobiles pour traiter les données à caractère personnel, puis comment mettre en place des mesures pour atténuer ou éliminer ces risques.



ÉVÉNEMENTS

Atelier IPEN: technologie et respect de la vie privée

En réponse à l'écart croissant entre les attentes des utilisateurs concernant la protection des données et la réalité des technologies actuelles, l'initiative IPEN a accueilli des experts de la protection des données et des ingénieurs informatiques de toute l'Europe le 26 septembre 2014 à Berlin. Le thème de notre débat était le suivant: «Comment développer la structure de l'Internet, les services et les applications en ligne de manière à respecter la vie privée et les données personnelles des internautes?».

Cet atelier était le premier organisé par le réseau d'ingénierie de la vie privée sur Internet (IPEN), initiative lancée par le CEPD in 2014 (voir la [newsletter n° 42](#)). En collaboration avec des autorités nationales de protection des données, des ingénieurs, des universitaires et la société civile, cette initiative vise à développer des pratiques techniques

respectueuses de la vie privée, et à encourager les ingénieurs à intégrer des mécanismes de protection de la vie privée dans les normes, les services et les applications en ligne.

Cet atelier incluait des présentations d'intervenants renommés, tels Peter Hustinx du CEPD, le Dr Alexander Dix, commissaire du Land de Berlin pour la protection des données et la liberté de l'information, et Peter Schaar, président de l'Académie européenne pour la liberté de l'information et la protection des données (EAID). Leurs interventions se concentraient sur la définition de priorités pour l'initiative IPEN et l'élaboration de stratégies pour mettre en œuvre ces priorités.

La création d'un «manuel pour la protection des données», dédié au développement de systèmes, faisait partie des projets proposés. Conçu

pour les développeurs informatiques, ce manuel expliquera, point par point, comment inclure le respect de la vie privée dans les outils en ligne et les processus de développement. Les participants ont également recommandé la création d'un «manuel dédié à la conception de processus d'entreprise», qui fournira des conseils aux entreprises en utilisant des solutions TI.

De plus, les participants ont convenu de la nécessité de trouver des solutions pour combler le manque de communication entre les avocats et les ingénieurs. Ils ont convenu que l'amélioration de la compréhension et de la coopération entre les deux communautés était essentielle pour garantir l'inclusion de la protection des données à caractère personnel dans la technologie que nous utilisons quotidiennement.

Après le succès de son premier atelier, l'initiative IPEN privilégie désormais le développement et la réalisation des projets auxquels elle a donné la priorité. L'IPEN continuera à étudier comment développer des technologies respectueuses de la vie privée et faire de la protection de la vie privée une préoccupation centrale pour tous

les développeurs informatiques.

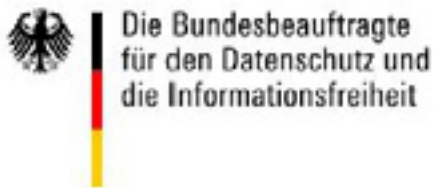
Des informations complémentaires sur l'initiative IPEN, y compris les modalités d'inscription sur notre liste d'adresses, sont disponibles sur notre site web.

[Site web de l'IPEN](#)

[Communiqué de presse](#)



«Trois années de réforme de la protection des données dans l'UE: bilan et perspectives» (Bruxelles)



Les récents arrêts de la Cour de justice de l'Union européenne sur la conservation des données et les moteurs de recherche (Google Spain) illustrent la pertinence croissante des droits fondamentaux à la vie privée et à la protec-

tion des données dans le contexte des nouveaux services d'information et des transferts de données.

Face aux mutations technologiques rapides et à la réalité croissante de la surveillance omni-

présente des données personnelles par les entités privées et publiques, l'UE s'efforce d'instaurer des règles qui protégeront efficacement les données à caractère personnel dans un monde interconnecté.

Le 5 novembre 2014, Andrea Voßhoff, commissaire fédéral allemand à la protection des données et la liberté de l'information, et Peter Hustinx, du CEPD, accueilleront de hauts représentants des sphères institutionnelles et poli-

tiques afin d'examiner les questions irrésolues et les mesures à prendre pour faire aboutir la réforme de la législation européenne en matière de protection des données.

[Informations complémentaires](#)

Lancement du concours de l'UE sur la protection des données

Du 6 novembre au 9 décembre 2014, l'Office européen de sélection du personnel (EPSO) enregistrera les inscriptions à un concours de l'UE sur la protection des données. Les candidats qui réussiront les examens pourront postuler des postes d'administrateur (AD 6) liés à la protection des données dans les institutions et les organes de l'UE.

[Informations complémentaires](#)

Votre avis sur la newsletter du CEPD

Nous souhaitons savoir ce que vous pensez de notre newsletter, afin qu'elle soit encore plus agréable à lire pour vous. Nous avons préparé neuf questions pour connaître votre opinion. Répondre à ces questions ne vous prendra que 8 à 10 minutes. L'enquête est complètement anonyme, à moins que vous

ne souhaitiez participer à une tombola qui vous permettra peut-être de gagner l'un des vingt stylets offerts. Si vous nous communiquez une adresse électronique, nous vous ferons savoir si vous êtes l'un des vingt heureux gagnants, avant de supprimer votre adresse de nos fichiers.

Vos commentaires sont importants, et nous aideront à améliorer notre newsletter et votre expérience en tant que lecteur. C'est pourquoi nous vous invitons à participer à notre enquête.

[Enquête sur la newsletter du CEPD](#)



DÉLÉGUÉS À LA PROTECTION DES DONNÉES

Nominations récentes

- M. Massimo Attoresi, délégué à la protection des données



DISCOURS ET PUBLICATIONS

- «Garantir une protection des données plus efficace à l'ère de la collecte de données massives», contribution (PDF) de Peter Hustinx au débat en ligne de European Voice sur le consentement et la collecte de données massives (14 juillet 2014)
- «Le leadership européen en matière de respect de la vie privée et de protection des données», article (PDF) de Peter Hustinx prochainement publié dans «La propuesta de Reglamento Europeo de Protección de Datos: principales desafíos actuales», Castellon 2014 (8 septembre 2014)
- «European Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation» (Législation européenne sur la protection des données: la révision de la directive 95/46/CE et la proposition de règlement général sur la protection des données), article (PDF) de Peter Hustinx fondé sur un cours donné à l'Académie de droit européen de l'Institut universitaire européen en juillet 2013; cet article sera publié dans le «Recueil des cours de l'Académie de droit européen de l'Institut universitaire européen, 1-12 juillet 2013» (15 septembre 2014)
- «Un ordre mondial pour la protection des données: un rêve qui devient réalité?», discours (PDF) prononcé par Peter Hustinx lors de la 36^e Conférence internationale des commissaires à la protection des données et à la vie privée, séance plénière II «Privacy with no Territorial Bounds», Balaclava Fort, Maurice (15-16 octobre 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

© Photos : iStockphoto/Edps et Union européenne

CEPD – Le Contrôleur européen de la protection des données