Newsletter du CEPD
N° 38 | JUILLET 2013
LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

- FAITS MARQUANTS -

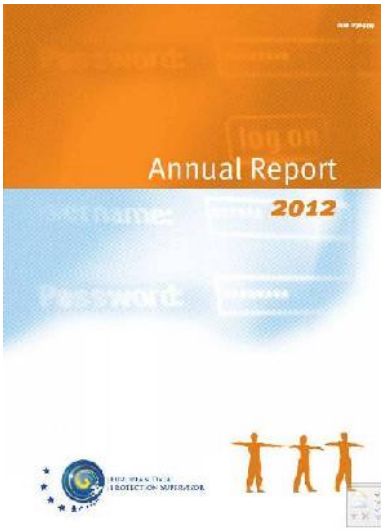
> Une protection des données forte pour une meilleure approche de l'UE en matière de crimes graves

Une prise en considération effective de la protection des données peut renforcer la **crédibilité** des enquêtes sur les **crimes graves** dans l'UE. C'est le message que le Contrôleur européen de la protection des données (CEPD) a adressé dans l'avis qu'il a publié le 3 juin 2013 sur la proposition de la Commission concernant un nouveau cadre juridique pour l'Agence de l'UE pour la coopération et la formation des services répressifs (Europol). Le CEPD soutient pleinement la nécessité d'adopter des approches novatrices et flexibles dans la prévention et la lutte contre les crimes graves, mais insiste aussi sur la nécessité de **garanties solides**. La validité d'une enquête criminelle repose sur la qualité et l'intégrité des données récoltées. Le respect des principes de protection des données peut aider à renforcer la **fiabilité** de ces preuves.

Un cadre de protection des données solide est important non seulement pour les personnes soupçonnées ou impliquées dans une enquête, mais contribue aussi à la réussite de la coopération policière et judiciaire. Comme le travail d'Europol repose sur la coopération avec et entre les services répressifs en Europe, il est important que la protection des données soit pleinement prise en considération; en pratique, cela signifie qu'Europol doit recueillir des données personnelles pour des enquêtes spécifiques uniquement. Il importe qu'Europol maintienne un niveau de protection des données élevé du fait de son rôle accru dans la lutte contre les crimes graves. Une supervision efficace d'Europol est nécessaire pour garantir qu'il opère dans le plein respect de la jurisprudence spécifique de la Cour de justice de l'UE.

☞ Avis (pdf) et communiqué de presse (pdf) du CEPD

> Un cadre de protection des données plus fort et plus efficace pour une Europe "intelligente, durable et inclusive"



Le 29 mai 2013, le CEPD a présenté son **rapport annuel** d'activité pour 2012 à la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen.

Lors de la conférence de presse animée qui a suivi, Peter Hustinx, CEPD, a évoqué le lobbying exceptionnel exercé autour de la **révision** actuelle de la **législation européenne sur la protection des données** par des organisations d'Europe et d'ailleurs. Il a **mis en garde** le législateur européen contre toute forme de pression indue de l'industrie et de pays tiers visant à abaisser le niveau actuel de protection des données, l'invitant plutôt à saisir l'occasion de garantir une **protection plus forte** et **plus efficace** des personnes dans l'ensemble de l'UE.

La législation en vigueur en matière de protection des données a été adoptée il y a 18 ans, à un moment où l'internet en était à ses balbutiements. Une mise à jour est, depuis longtemps, nécessaire, et le CEPD participe étroitement aux travaux en cours sur la réforme. Le processus de révision a suscité une attention considérable de la part l'industrie, qui affirme que les règles de protection des données sont un obstacle à l'innovation.

Les avantages pour l'industrie ne doivent et ne peuvent se faire au détriment de nos droits fondamentaux à la vie privée et à la protection des données. L'intégration des principes de protection des données dans l'innovation technique ou lors du transfert de nos informations personnelles vers des entités compétentes, à des fins de sécurité par exemple, peut ajouter une valeur significative, à la fois en termes d'efficacité et de réduction des coûts, si le respect de la vie privée est intégré dès le départ dans la conception des processus en question.

Peter Hustinx, CEPD

☞ Rapport annuel 2012 (pdf), résumé (pdf) et communiqué de presse du CEPD (pdf)

CONSULTATION

> Respect de la vie privée et confiance doivent être les fondements de toute stratégie de cybersécurité crédible en Europe

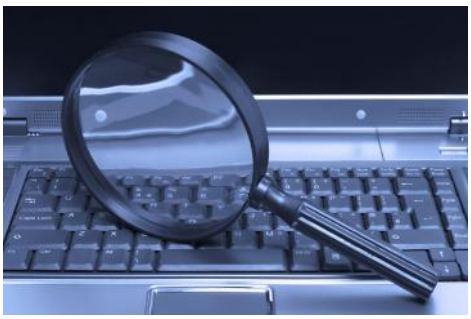
La cybersécurité ne peut servir de prétexte à la surveillance et à l'analyse **illimitées** des données à caractère personnel, a déclaré le CEPD le 17 juin 2013 à la suite de la publication de son **avis** sur la **stratégie de l'UE en matière de cybersécurité**. Bien qu'elle reconnaisse à juste titre l'importance des principes de protection des données pour une politique de cybersécurité solide, la stratégie n'est **pas claire** sur la façon dont ces principes seront appliqués en pratique en vue de renforcer la sécurité des personnes, de l'industrie, des gouvernements et d'autres organisations.

Peter Hustinx, CEPD, a déclaré: «La sécurité passe par la protection de la vie privée; je suis donc ravi que la stratégie de l'UE reconnaisse qu'il n'y a pas d'opposition entre respect de la vie privée et cybersécurité, et que les principes de protection des données à caractère personnel servent plutôt de principes directeurs en la matière. Toutefois, les ambitions de la stratégie ne se reflètent pas dans sa mise en œuvre pratique. Nous reconnaissons que les questions de cybersécurité doivent être abordées au niveau international au travers de normes internationales et de la coopération, mais si l'UE veut coopérer sur la cybersécurité avec d'autres pays, dont les États-Unis, cette coopération doit forcément reposer sur une confiance mutuelle et le respect des droits fondamentaux, prémisses qui paraissent actuellement compromises».

☞ Avis (pdf) et communiqué de presse (pdf) du CEPD

> Focus sur la surveillance du marché

Le règlement proposé par la Commission concernant la surveillance du marché des produits (qui modifie également divers instruments législatifs) vise à garantir que les produits ne portent pas atteinte à la santé, à la sécurité ou à tout autre aspect lié à la protection de l'intérêt public et qu'ils sont conformes aux exigences établies dans la législation d'harmonisation de l'Union applicable aux produits.



La proposition est un bon exemple de proposition législative ayant des implications significatives en matière de protection des données qui ne sont pas

immédiatement évidentes. Dans notre avis du 30 mai 2013, nous avons souligné qu'une proposition devrait toujours déterminer si les règles de l'UE en matière de protection des données sont applicables, en particulier lorsque le partage d'informations est autorisé, via des plateformes informatiques spécialisées ou non. En règle générale, chaque fois qu'une proposition législative implique le traitement de données à caractère personnel, même s'il ne s'agit pas de son objectif principal, les règles nationales mettant en œuvre la directive 95/46/CE sur la protection des données et/ou le règlement (CE) n° 45/2001 sont d'application. Certaines conditions s'appliquent dès lors chaque fois que des données à caractère personnel doivent être recueillies, analysées ou traitées. Par exemple, seules les données à caractère personnel strictement nécessaires à la finalité indiquée doivent être recueillies et des durées spécifiques de conservation des données collectées doivent être fixées. Nous avons en outre souligné que lorsque les données à caractère personnel d'un opérateur économique (par exemple, le fabricant, son mandataire, l'importateur et/ou le distributeur d'un produit disponible sur le marché de l'UE) doivent être rendues publiques, le type de données personnelles devant être publiées et les raisons de le faire doivent être formulés explicitement dans une déclaration de confidentialité à adresser au préalable aux personnes concernées.

☞ Avis du CEPD (pdf)

> Réglementation des prix des médicaments à usage humain

Le 30 mai 2013, nous avons adopté un avis sur la proposition modifiée de la Commission concernant une directive relative à la *transparence des mesures régissant la fixation des prix des médicaments à usage humain et leur inclusion dans le champ d'application des systèmes publics d'assurance-maladie.* La proposition vise à garantir que les règles nationales relatives à la fixation des prix et au remboursement des médicaments ne sont pas contraires au principe de libre circulation des biens dans l'UE. Nous avons attiré l'attention sur le fait que les données à caractère personnel traitées dans le cadre des procédures des autorités sanitaires nationales en matière de fixation des prix et de remboursement peuvent renvoyer à des données relatives à la santé des patients. Par conséquent, il convient de relever le niveau de protection des données. Nous avons recommandé que toute donnée relative à la santé des patients comprise dans les informations soumises par une entreprise pharmaceutique en vue d'être autorisée à commercialiser un médicament soit rendue pleinement anonyme – en d'autres termes, que l'identité de la personne ne puisse être établie – avant que cette donnée ne soit transférée aux autorités sanitaires nationales pour tout traitement ultérieur. Nous avons en outre mis en cause la nécessité et la proportionnalité de la publication obligatoire des noms et des déclarations d'intérêts des experts, des membres des organes de décision et des membres des entités chargées des procédures de recours.

☞ Avis du CEPD (pdf)

> Renforcer la coopération dans le domaine de la répression au sein de l'UE: le modèle européen d'échange d'informations

Le 29 avril 2013, nous avons adopté un avis sur la communication de la Commission intitulée «Renforcer la coopération dans le domaine de la répression au sein de l'UE: le modèle européen d'échange d'informations (EIXM)». Nous nous sommes félicités que la communication ait conclu que des bases de données en matière de répression au niveau de l'UE ni de nouveaux instruments d'échange d'informations de l'UE ne sont nécessaires. Cependant, nous avons attiré l'attention sur le fait que les instruments et initiatives existants dans le domaine de la justice et des affaires intérieures devront être soumis à un processus d'évaluation complet, dont les résultats pourront mener à une politique européenne globale, intégrée et bien structurée en matière d'échange et de gestion des informations.

☞ Avis du CEPD (pdf)

> La protection des données fait partie intégrante de la coopération en matière de stupéfiants

Le 23 avril 2013, nous avons adopté un avis sur la proposition de la Commission relative à la conclusion d'un accord entre l'Union européenne et la Fédération de Russie concernant les précurseurs de drogues. L'accord vise à renforcer la coopération afin d'empêcher que des substances légales ne soient utilisées pour fabriquer de manière illicite des stupéfiants et des substances psychotropes («précurseurs de drogues»). Il autorisera, par exemple, le transfert de données à caractère personnel sur les transactions suspectes de précurseurs de drogues.

Nous avons salué les dispositions relatives à la protection des données à caractère personnel dans le texte de l'accord ainsi que l'inclusion des principes obligatoires de protection des données dans l'annexe. Cependant, nous nous préoccupons de l'applicabilité effective de ces principes. C'est pourquoi nous avons recommandé que les autorités de protection des données européennes et russes réexaminent conjointement la mise en œuvre de l'accord. Nous avons également recommandé que le texte permette explicitement la suspension ou la résiliation éventuelle de l'accord si les principes de protection des données ne sont pas respectés.

En outre, nous avons conseillé que les garanties en matière de protection des données soient mieux définies, comme par exemple la finalité des transferts de données à caractère personnel, les durées de conservation des données, les catégories de données à échanger et la protection des données relatives à des transactions suspectes. Dans un souci d'exhaustivité des principes obligatoires de protection des données, nous avons recommandé l'ajout de dispositions relatives aux données

sensibles, à la sécurité des données et à la limitation des transferts de données à caractère personnel ultérieurs.

☞ Avis du CEPD (pdf)

SUPERVISION

> EIGE: vers la protection des données

Le 22 mai 2013, Giovanni Buttarelli, Contrôleur adjoint, a visité l'Institut européen pour l'égalité entre les hommes et les femmes (EIGE) à Vilnius, en Lituanie, en vue d'améliorer le respect des règles en matière de protection des données au sein de l'agence.

L'EIGE, devenu opérationnel au cours de l'été 2010, n'a pas encore atteint la norme de référence établie par ses pairs. À ce jour, l'agence n'a soumis aucune notification conformément à l'article 27 du règlement. En vertu dudit article, tout traitement de données à caractère personnel dans une institution ou un organe de l'Union européenne présentant des risques particuliers au regard des droits et libertés des individus est soumis au contrôle préalable du CEPD.

Des réunions à des fins de sensibilisation et d'orientation ont eu lieu dans le cadre de la visite avec la direction, le personnel et le délégué à la protection des données. En conclusion, la direction de l'EIGE a, avec le CEPD, convenu d'une feuille de route exposant des activités et objectifs précis en matière de protection des données, laquelle devrait contribuer à pallier les faiblesses actuelles de l'Institut.

> Clarification de la portée de l'utilisation compatible des données à caractère personnel à la BEI

La Banque européenne d'investissement (BEI) nous a consultés sur la légalité de l'analyse des données issues d'un système de sécurité d'accès ou d'un système de gestion du temps pour une autre finalité, c'est-à-dire pour des enquêtes en vue d'instruire des procédures disciplinaires.

Dans notre analyse du 17 avril 2013, nous avons attiré l'attention sur le fait que le concept de la limitation de la finalité représente une première étape essentielle dans l'application de la législation relative à la protection des données. La limitation de la

finalité signifie que les données à caractère personnel ne peuvent être collectées qu'à des fins déterminées, explicites et légitimes. Elle concourt à la transparence, à la sécurité juridique et à la prévisibilité, et vise à protéger les individus en fixant des limites concernant la façon dont leurs données sont utilisées. Néanmoins, elle procure également une certaine souplesse à la BEI.

À la suite d'une analyse des règles régissant les procédures disciplinaires et les enquêtes sur les fraudes à la BEI, nous avons conclu que ces règles pouvaient permettre l'utilisation des données concernées dans des enquêtes disciplinaires et être compatibles avec les finalités concernées. Cette possibilité est toutefois limitée auxdites finalités, et la proportionnalité ainsi que la nécessité du traitement des données doivent être respectées. En outre, la réutilisation de ces données pour une autre finalité ne devrait être permise que dans le cadre d'une procédure disciplinaire ouverte pour un cas spécifique et ne devrait pas constituer une occasion de procéder à des recherches aléatoires d'informations compromettantes – tentative de découvrir certains faits en recueillant de nombreuses informations sur des affaires souvent non liées ou mineures ou de manière secrète.

C'est le deuxième des deux dossiers que nous avons récemment analysés qui est en rapport avec la définition de l'utilisation compatible et qui révèle une tendance possible à l'utilisation ultérieure des données initialement recueillies pour une autre finalité. Voir également l'affaire du 9 avril 2013 concernant l'EFSA, non soumise à un contrôle préalable.

☞ Avis du CEPD (pdf)

> Transferts de données relatives au personnel vers les représentations permanentes

Le délégué à la protection des données (DPD) d'une agence de l'Union européenne a consulté le CEPD au sujet du transfert d'informations individuelles du personnel vers la représentation permanente des États membres [les représentants permanents sont principalement chargés de préparer collectivement le travail du Conseil de l'Union européenne dans le cadre du Comité des représentants permanents (Coreper)].

Dans sa réponse du 9 avril 2013, le CEPD a indiqué que ces demandes doivent toujours préciser une finalité et reposer sur une base juridique claire, comme par exemple l'article 15, deuxième alinéa, du protocole n° 7 du traité sur le fonctionnement de l'Union européenne (TFEU) sur les privilèges et immunités de l'Union européenne, qui prévoit que les noms, qualités et adresses des fonctionnaires et autres agents compris dans certaines catégories sont «communiqués périodiquement aux gouvernements des États membres».

Il semble que cette question soit très répandue. C'est pourquoi, le 8 mai 2013, le CEPD a lancé une enquête en vue de recueillir davantage d'informations de la part des DPD concernant ces transferts dans d'autres institutions, organes et agences de l'Union européenne.

☞ Avis du CEPD (pdf)

> Déclarations d'intérêts: équilibre entre vie privée et transparence

Le 8 mars 2013, l'entreprise commune européenne pour ITER et le développement de l'énergie de fusion (F4E) nous a informés des traitements de données auxquels elle procédait sur les déclarations d'intérêts des membres de son comité exécutif. Ces déclarations garantissent l'indépendance de ces membres et permettent d'éviter tout conflit d'intérêts susceptible d'interférer avec leurs activités. Elles contiennent des informations sur les emplois actuel et antérieurs des membres, sur les investissements qu'ils ont réalisés ou les subventions qu'ils ont perçues ainsi que leurs conjoint(e), compagne/compagnon ou membres de leur ménage. Les déclarations d'intérêts peuvent être rendues publiques sur demande.

Dans notre avis du 30 mai 2013, nous avons déclaré que cette publication peut être justifiée pour permettre un contrôle par les pairs et le public tributaire des tâches des membres du comité exécutif.

Toutefois, comme dans d'autres cas similaires (par exemple, celui de l'ECDC dont il est fait état dans notre newsletter de décembre 2012), nous avons recommandé à l'agence d'adopter une approche proactive concernant les questions de transparence. Les institutions et organes devraient évaluer le caractère potentiellement public des données à caractère personnel lorsqu'ils les recueillent et informer correctement les individus concernés de l'éventuelle divulgation de ces données et de leur droit d'opposition (dans une déclaration de confidentialité, par exemple).

Nous avons également souligné que la divulgation des déclarations d'intérêts constitue en fait un transfert de données. Comme énoncé dans le document du CEPD intitulé «Accès du public aux documents contenant des données à caractère personnel après l'arrêt rendu dans l'affaire *Bavarian Lager*», une institution doit tenir compte des intérêts et des points de vue légitimes du/des individu(s) concernés afin de mettre en balance les intérêts de toutes les personnes concernées et de prendre une décision en connaissance de cause. Selon nous, le consentement n'est pas nécessaire, faute de quoi la mise en balance des intérêts serait vidée de sa substance. Les individus ont toutefois le droit de s'opposer à la publication des données pour des raisons impérieuses et légitimes.

☞ Avis du CEPD (pdf)

> Clarification de la portée de l'utilisation compatible des données à caractère personnel à l'EFSA

Dans notre réponse du 9 avril 2013 à une notification de l'Autorité européenne de sécurité des aliments (EFSA) en vue d'un contrôle préalable au sujet de l'utilisation des informations que comportent les badges d'accès concernant la présence du personnel dans les bureaux, nous avons conclu que l'opération n'était pas soumise à un contrôle préalable. Cependant, comme pour la consultation de la BEI décrite plus haut, ce dossier nous a permis de clarifier la question de l'utilisation compatible des données issues d'un système de contrôle d'accès.

Nous avons souligné l'importance du principe de limitation de la finalité, selon lequel, dans chaque situation où l'utilisation ultérieure de données à caractère personnel est envisagée, il convient de faire une distinction entre les utilisations supplémentaires qui sont «compatibles» et les autres utilisations, qui devraient demeurer «incompatibles». Par exemple, il serait incompatible de relier une base de données de contrôle d'accès à une base de données de gestion du temps.

En l'occurrence, l'utilisation pourrait être jugée compatible pour aider les titulaires d'un emploi. Cependant, nous avons exprimé des doutes quant à la nécessité de mettre en œuvre un tel système, car d'autres moyens ne nécessitant pas l'utilisation d'informations du système de contrôle d'accès sont disponibles.

☞ Avis du CEPD (pdf)

ÉVÉNEMENTS

> Atelier du CEPD sur les communications électroniques, à Bruxelles

Le 12 juin 2013, nous avons organisé un atelier sur l'utilisation des communications électroniques sur le lieu de travail, à l'occasion duquel 75 participants, dont des délégués à la protection des données (DPD), des coordinateurs de la protection des données (CPD) et des agents des domaines informatique et des ressources humaines, représentaient la plupart des institutions et organes de l'Union européenne. Les participants ont apporté une précieuse contribution en partageant l'expérience qu'ils ont acquise dans leur travail quotidien en ce qui concerne l'utilisation des téléphones, de l'internet et du courrier électronique. D'autres réunions ainsi que des échanges électroniques avec les réseaux de DPD/CPD et le personnel des services informatiques, des ressources humaines et d'autres domaines de l'administration de l'UE contribueront à recueillir d'autres informations pertinentes en la matière.

Cet atelier était le premier d'une série d'initiatives qui nous aideront à élaborer des orientations sur ce thème et d'autres exemples de communication électronique (y compris l'utilisation des appareils mobiles, l'informatique en nuage et les sites internet de l'UE). Nous espérons mener ce projet à bien d'ici la fin de l'année et prévoyons d'organiser des ateliers similaires plus tard dans l'année.

Le niveau de participation élevé à cet atelier confirme l'importance du sujet et le rôle clé joué par la coopération interinstitutionnelle dans l'étude de ces questions.

> Réunion du groupe de coordination du contrôle du système d'information des douanes, à Bruxelles

La sixième réunion du groupe de coordination du contrôle du système d'information des douanes (SID) a eu lieu le 11 juin 2013. Les mandats du président et du vice-président ayant expiré le 7 juin 2013, un vote à bulletin secret a été organisé dans ce cadre. M. Giovanni Buttarelli, président du

groupe, et M. Gregor Konig, vice-président du groupe, ont tous deux été réélus.

Le groupe a également examiné le projet de rapport sur l'inspection coordonnée de la liste des autorités ayant accès au SID et au FIDE, ainsi que le projet de rapport sur les droits des personnes concernées du CID. La prochaine réunion du groupe devrait avoir lieu en automne.

> Réunion du groupe de coordination du contrôle du système d'information Schengen II, à Bruxelles

La première réunion de coordination du contrôle du système d'information Schengen II (SIS II) s'est tenue le 11 juin 2013 après-midi. L'ordre du jour portait sur des questions administratives, telles que l'élection du président et du vice-président. M[me] Clara Guerra, représentant l'autorité portugaise chargée de la protection des données, et M. David Cauchi, représentant l'autorité maltaise chargée de la protection des données, ont été respectivement élus; le règlement intérieur du groupe a été adopté et le statut d'observateur a été reconnu à la Bulgarie, à Chypre, à l'Irlande, à la Roumanie et au Royaume-Uni. Des questions plus significatives, comme le piratage informatique du N-SIS danois, l'état d'avancement du processus de migration du SIS II et une campagne d'information concernant le SIS II, ont été examinées. Les mesures ultérieures à adopter par la Commission et l'agence EU-LISA, concernant la politique de sécurité du SIS II en particulier, ainsi que les futures activités du groupe de coordination du contrôle pour 2013-2014, ont également été abordées. La prochaine réunion du groupe devrait avoir lieu en automne.

DISCOURS ET PUBLICATIONS

- "Un signal clair pour une plus grande protection des données en Europe", éditorial (pdf) de Peter Hustinx dans "Zeitschrift für Datenschutz", n° 2013/7, p. 301-302 (21 juin 2013).
- "Le programme de Stockholm: état des lieux sur la coopération policière et judiciaire en matière civile et pénale", discours (pdf) prononcé par Peter Hustinx lors de la réunion de la commission interparlementaire, Parlement européen, Bruxelles (20 juin 2013).
- "Data Protection and Competition: interfaces and interaction" (Protection des données et concurrence: interfaces et interaction), discours (pdf) prononcé par Peter Hustinx lors d'un séminaire organisé par Covington & Burling LLP, à Bruxelles (13 juin 2013).
- "L'impact horizontal croissant de la protection des données", éditorial (pdf) de Peter Hustinx dans la revue "Eucrim" – European Criminal Law Associations' Forum (forum européen des associations de droit pénal), n° 2013/1, p. 1 – Focus: Information et protection des données (13 mai 2013).

DÉLÉGUÉS À LA PROTECTION DES DONNÉES

☞ Voir 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 abonnez / désabonnez à cette newsletter sur notre site web.**

Suivez-nous sur Twitter: @EU_EDPS

COORDONNÉES
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