Newsletter du CEPD

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

N° 22 | 16 DECEMBRE 2009

Entrée en vigueur du Traité de Lisbonne: impact sur la protection des données

Le traité de Lisbonne, qui est entré en vigueur le 1er Décembre 2009, a des conséquences importantes pour la protection des données.

Le traité de Lisbonne abolit la structure en piliers qui, au fil des années, a soulevé de nombreuses questions relatives à la protection des données. Il crée une nouvelle base juridique pour la protection des données, en introduisant l'article 16 du traité sur le fonctionnement de l'Union européenne (TFUE). Cette nouvelle base juridique remplace l'article 286 du traité CE, qui a servi de fondement à la création du CEPD.

Le nouvel article 16 améliore les dispositions relatives à la protection des données qui, auparavant isolées dans le traité, appartiennent maintenant à la partie I, titre II du TFUE, qui contient des dispositions générales du droit de l'UE (telles que la non-discrimination ou l'accès du public aux documents). La portée de l'article est générale, puisqu'il s'applique aux niveaux national et européen, à la fois aux secteurs privé et public, et couvre également la coopération policière et judiciaire. En vertu de l'article 16 du TFUE, chacun bénéficie du droit à la protection de ses données personnelles.

Le Conseil et le Parlement européen fixeront les règles sur la protection des données. Jusqu'à ce que ces nouvelles règles soient adoptées, le cadre actuel pour l'ancien premier pilier (principalement la directive 95/46/CE), pour l'ancien troisième pilier (notamment la décision-cadre 2008/977/JAI), et pour

le traitement des données personnelles par les institutions de l'UE (principalement le règlement (CE) n° 45/2001) continuera de s'appliquer.

Le caractère désormais contraignant de la Charte des droits fondamentaux de l'Union européenne, notamment son article 8 sur la protection des données, constitue également une évolution importante. L'article 8 résume les principaux éléments du droit fondamental de la protection des données, telles que limitation de la finalité, le droit d'accès et de rectification aux données personnelles, ainsi que la supervision par un organe indépendant.

CONSULTATION

> Avis du CEPD sur l'établissement d'une agence pour les systèmes d'information à grande échelle

L'avis du CEPD, adopté le 7 décembre 2009, porte sur le paquet législatif proposé par la Commission européenne portant création d'une agence pour la gestion opérationnelle des systèmes d'information à grande échelle dans le domaine de la liberté, de la sécurité et de la justice. L'agence serait responsable de la gestion opérationnelle du système d'information Schengen (SIS II), du système d'information sur les visas (VIS), Eurodac et d'éventuels autres systèmes d'information à grande échelle.

Étant donné que ces bases de données contiennent de grandes quantités de données personnelles sensibles (données sur les passeports, visas et empreintes digitales, par exemple), le CEPD a analysé la proposition du point de vue de la protection des données, en vue d'assurer que les risques éventuels, pouvant avoir un impact important sur la vie privée des individus, soit suffisamment pris en compte dans l'acte législatif.

Le CEPD reconnaît les avantages de la mise en place d'une agence pour la gestion opérationnelle de certains systèmes d'information à grande échelle car cela clarifie les questions de responsabilité et de droit applicable. Il souligne cependant qu'une telle agence ne devrait être mise en place qu'à la condition que le champ de ses activités et ses responsabilités soient clairement définis. Ceci est essentiel pour éviter le risque de "détournement d'usage" (i.e. élargissement des fonctions de l'agence, données recueillies pour un but précis et utilisées à d'autres desseins) ou de mauvaise utilisation des données personnelles.

> ***« La création d'une agence pour la gestion de ces bases de données à grande échelle doit être fondée sur une législation qui est sans ambiguïté sur les compétences et la portée des activités de l'agence. »*** Peter Hustinx, CEPD

Le CEPD encourage le législateur à adopter une approche prudente et restrictive. Le point de départ ne devrait pas consister à mettre autant de systèmes d'information à grande échelle que possible sous la gestion d'une seule agence. Seulement après avoir acquis de l'expérience et suite à une évaluation positive de son fonctionnement, d'autres systèmes pourraient se voir placés sous la responsabilité de l'agence. Afin d'améliorer la proposition, le CEPD recommande aux législateurs européens de:

- clarifier si le champ d'activités de l'agence est limité aux politiques relatives aux contrôles aux frontières, d'asile et d'immigration, ou s'il devrait potentiellement couvrir tous les systèmes

d'information à grande échelle développés dans le domaine de la liberté, de la sécurité et de la justice;

- clarifier la notion de systèmes d'information à grande échelle dans ce cadre, et faire savoir clairement si elle est limitée aux systèmes qui stockent les données dans une base de données centralisée pour laquelle la Commission ou l'agence est responsable.

☞ Avis du CEPD (EN) (pdf)

> Réaction du CEPD suite à l'adoption de la directive "Vie privée et communications électroniques"

Suite à l'accord intervenu début novembre sur la réforme du "Paquet Télécom", rien ne s'oppose maintenant à l'entrée en vigueur de la directive "vie privée et communications électroniques". Les formalités requises pour son adoption formelle seront engagées dans les semaines à venir. La directive révisée, telle que modifiée par le Parlement européen et adoptée par le Conseil, devra alors être mise en œuvre par les États membres dans les 18 mois.

Les nouvelles dispositions de la directive apportent des améliorations importantes en matière de protection de la vie privée et des données personnelles de tous les Européens intervenant dans l'environnement en ligne. Les améliorations ont trait aux atteintes à la sécurité, aux logiciels espions, aux cookies, au spam, et à la mise en œuvre des règles. Le CEPD a étroitement coopéré avec le Parlement européen, le Conseil et la Commission sur le travail législatif qui a permis d'aboutir au texte final.

Le CEPD salue les nombreuses améliorations en matière de protection de la vie privée dans la version révisée de la directive. Il souligne qu'il est maintenant essentiel d'élargir la portée des dispositions relatives aux atteintes à la sécurité à tous les secteurs et de mieux définir les procédures de notification. Il relève en particulier l'accent mis sur une application plus efficace des règles sur les logiciels espions et les cookies. Cela revêt un intérêt d'autant plus important lorsque le droit à la vie privée doit être protégé par rapport à la publicité dite ciblée.

Les modifications apportées comprennent:

- l'introduction, pour la première fois dans l'Union européenne, d'un cadre pour la **notification obligatoire des failles de sécurité**. Tout fournisseur de communications électroniques ou fournisseur d'accès à Internet (FAI) impliqué dans une violation de données personnelles devra informer les individus concernés si la violation est susceptible de leur nuire. Cela concernera par exemple une situation où la perte de données peut occasionner un vol d'identité ou une fraude, ou être à l'origine d'une humiliation ou de dommages à la réputation;

- une protection renforcée contre l'interception des communications au moyen, notamment, de **logiciels espions** et de ***cookies*** stockés sur l'ordinateur des utilisateurs ou sur un autre appareil. Avec la nouvelle directive, les utilisateurs devraient se voir offrir une meilleure information et de plus grandes facilités pour contrôler l'installation de cookies dans leur équipement terminal;

- la possibilité pour toute personne affectée par le **"spamming"** (envoi non sollicité de courriels), y compris les FAI, d'engager une procédure judiciaire contre les "spammeurs";
- un renforcement des pouvoirs d'exécution des autorités nationales de protection des données. Celles-ci seront par exemple en mesure d'ordonner la cessation immédiate des infractions et auront des capacités renforcées en matière de coopération transfrontalière.

☞ Premier (pdf) et deuxième (pdf) avis du CEPD sur la révision de la directive "Vie privée et communications électroniques"

> Avis du CEPD sur la lutte contre la fraude dans le domaine de la taxe sur la valeur ajoutée

Le 30 octobre 2009, le CEPD a adopté un avis sur la proposition de la Commission visant à modifier un règlement du Conseil sur la lutte contre la fraude à la TVA. Avec cette proposition, la Commission entend accroître l'efficacité de la coopération transfrontalière dans ce domaine et améliorer la collecte et le partage d'informations. Les amendements prévoient également une base juridique pour l'établissement d'une structure d'opération commune pour la coopération multilatérale, appelée Eurofisc.

Le CEPD conclut que toutes les exigences provenant des règles communautaires sur la protection des données ne sont pas satisfaites. Cela est principalement dû au fait que les dispositions sont trop générales et laissent trop de place à la l'interprétation. Un premier point concerne l'utilisation de la notion "toute information". Cette notion très étendue ouvre la porte à la collecte, au stockage et à l'échange de toutes sortes d'informations personnelles. Le CEPD demande donc au Conseil de préciser et de limiter cette notion.

Le CEPD souligne également la responsabilité en matière de conformité avec les règles de protection des données. Le CEPD considère qu'il n'est pas toujours clair si ce sont les États membres, la Commission ou l'Eurofisc qui sont responsables du respect des règles. Le CEPD invite le Conseil à clarifier cela dans le texte final.

Une incertitude existe en outre en ce qui concerne les finalités pour lesquelles les autorités compétentes dans les États membres échangent des données sur des éventuelles fraudes à la TVA. Le CEPD souligne que ces finalités devraient être clarifiées. Il considère par ailleurs que le Conseil devrait s'assurer que les données soient seulement utilisées si elles sont nécessaires à l'objectif poursuivi. Le CEPD indique également qu'une période maximale de conservation des données devrait être fixée.

La question de la protection des données est traitée par une disposition de la proposition. Le CEPD n'est pas satisfait du texte proposé car il ne répond pas à l'exigence selon laquelle les données ne doivent être utilisées qu'aux fins pour lesquelles elles ont été collectées. Cette disposition prévoit en outre des restrictions aux droits de la personne concernée d'une manière qui n'est pas compatible avec les règles de protection des données.

☞ Avis du CEPD (EN) (pdf)

> Droit d'accès d'un candidat d'EPSO aux questions des tests de présélection (Affaire Pachtitis c/ la Commission)

Le CEPD est intervenu devant le Tribunal de Fonction publique, le 1er décembre 2009, dans l'affaire Pachtitis c/ la Commission. Un agent du CEPD a plaidé à l'appui d'un des appels du requérant concernant la décision d'EPSO de rejeter sa demande visant à accéder à une partie des documents des tests, à savoir les questions auxquelles il avait répondues. Le CEPD a fait valoir que le requérant ne pourrait évaluer sa performance et vérifier la décision d'EPSO qu'à la condition de recevoir les questions auxquelles il avait répondues pendant les tests de présélection. C'est pourquoi le requérant a le droit d'avoir accès à ces données.

Dans sa plaidoirie, le CEPD a expliqué l'objectif de l'intervention, à savoir les raisons pour lesquelles les questions des tests devaient être considérées en tant que données à caractère personnel et pourquoi la demande d'accès du requérant devait être examinée à la lumière du règlement sur la protection des données dans les institutions et organes communautaires (règlement (CE) n° 45/2001) et non du règlement relatif à l'accès aux documents (règlement (CE) n° 1049/2001).

En outre, le CEPD a fait contre-valoir:

- la position de la Commission selon laquelle le Tribunal de la Fonction publique n'est pas compétent pour juger des questions concernant le règlement relatif à la protection des données;
- la position de la Commission selon laquelle le règlement sur la protection des données ne peut pas s'appliquer parce l'article 6 de l'annexe III du Statut des fonctionnaires des Communautés européennes - selon lequel les travaux du jury sont secrets - s'applique comme *lex specialis*;
- la nécessité administrative de la Commission de pouvoir utiliser les questions dans d'autres concours.

Le CEPD a conclu que, étant donné que la Commission n'avait fourni aucune raison légitime pour justifier une restriction au droit d'accès en vertu de l'article 20 du règlement sur la protection des données, elle avait enfreint le droit fondamental d''accès aux données personnelles du requérant.

☞ Le texte de la plaidoirie est disponible sur le site web du CEPD.

SUPERVISION

> Contrôles préalables de traitements de données personnelles

Une opération de traitement de données personnelles par l'administration européenne qui est susceptible de présenter des risques particuliers pour les personnes concernées doit faire l'objet d'un contrôle préalable par le CEPD. Cette procédure permet de déterminer si le traitement est conforme au règlement (CE) No 45/2001 qui établit les obligations des institutions et organes communautaires en matière de protection des données.

>> Vérification des pointages flexitime

Le traitement envisagé dans le cadre de ce contrôle préalable concerne la vérification des pointages Flexitime par rapport aux données sur l'accès physique au Secrétariat Général du Conseil (SGC).

Le SGC utilise une application Flexitime qui gère le temps de travail et les présences. Elle permet le calcul des droits à congés et contrôle les prises de congés ainsi que le calcul automatique des heures supplémentaires. Cette application a déjà fait objet d'un contrôle préalable par le CEPD.

Le SGC dispose également d'un système de contrôle d'accès géré par le Bureau de Sécurité, qui stocke ces données dans une base de données. Ces données ne sont accessibles aux services de l'administration que dans le cadre d'une enquête administrative formelle.

La comparaison des données vise à identifier les personnes qui enfreignent les règles du Flexitime, mais aussi à évaluer leur comportement (infractions aux règles du Flexitime). Le système est également susceptible de conduire à l'adoption de mesures disciplinaires.

Dans son avis publié le 12 novembre 2009, le CEPD a estimé que la nécessité et la proportionnalité de la vérification des pointages Flexitime par rapport aux données sur le contrôle d'accès physique étaient contestables. Selon le CEPD, il n'existe pas de preuve suffisante démontrant que la mise en œuvre d'un système de vérification des pointages Flexitime par rapport aux données sur l'accès physique est nécessaire à l'exécution de la mission pour la gestion de personnel et le fonctionnement de SGC.

Dans sa conclusion, le CEPD a donc estimé que le traitement envisagé enfreindrait le règlement (CE) n° 45/2001 à différent niveaux (, nécessité et proportionnalité, changement de finalité, qualité des données) dans le cas où la vérification des pointages Flexitime par rapport aux données sur le contrôle d'accès physique était effectué hors du cadre d'une enquête administrative.

☞ Avis du CEPD (pdf)

>> Intelligence émotionnelle (EEA) - évaluation à 360 degrés - Commission

Le but de ce traitement est de permettre aux participants aux formations de l'Ecole européenne d'Administration (EEA) d'obtenir des commentaires et récations, sous forme de rapport, afin de les aider à améliorer leurs compétences dans les domaines de l'autogestion, de la gestion des relations et de la communication. L'exercice est conduit grâce à l'utilisation d'un outil en ligne : "Emotional IntelligenceView 360". Le rapport est généré automatiquement suite aux réponses fournies par les participants et leurs collègues, et n'indique pas la manière dont les collègues ont complété les réponses.

Il convient de noter que, bien que l'EEA n'ait pas accès aux données traitées par le contractant (les données utilisées par la société qui effectue les tests dans le cadre de la "Emotional Intelligence View 360"), ce dernier doit agir selon les instructions données par l'EEA. L'EEA est donc la responsable du traitement des données. Le contractant n'est pas autorisé à effectuer d'autres activités de traitements des données allant au-delà de ce qui est déterminé par l'EEA et spécifié dans le contrat.

Dans son avis publié le 30 octobre 2009, le CEPD a notamment recommandé à l'EEA:

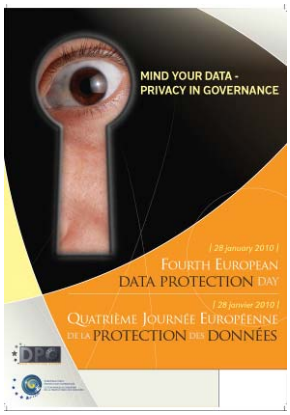
- d'explorer les possibilités de rendre anonyme l'utilisation de cet outil. À cet égard, des variables telles que les mises au point informatiques, les procédures et le coût devront être prises en compte;
- d'inclure une clause dans le contrat passé avec le sous-traitant spécifiant que la loi applicable concernant l'obligation de confidentialité et la sécurité du traitement effectué par le sous-traitant est la loi de l'État membre dans lequel le sous-traitant est établi, dans ce cas, le

Royaume-Uni.

☞ Avis du CEPD (EN) (pdf)

EVENEMENTS

> Evénements à venir



>> 4ème Journée européenne de la protection des données, 28 janvier 2010

Les Etats membres du Conseil de l'Europe, ainsi que les institutions et organes européens célèbreront le la quatrième édition de la Journée européenne de la protection des données le 28 janvier 2010. Cette date marque l'anniversaire de la Convention 108 sur la protection des données du Conseil de l'Europe, premier instrument international juridiquement contraignant dans le domaine de la protection des données.

L'événement donnera l'occasion au CEPD et aux délégués à la protection des données de sensibiliser le personnel des institutions à leurs droits et obligations en matière de protection des données - ces droits et obligations sont énoncées dans le règlement (CE) n° 45/2001, dont l'application est supervisée par le CEPD.

A cette fin, le CEPD tiendra un **stand d'information**, sur trois jours consécutifs, au Conseil (le 26 janvier), à la Commission européenne (le 27 janvier) et au Parlement européen (le 28 janvier).

Pour marquer l'événement, Peter Hustinx, CEPD, interviendra en **conférence de midi** sur le thème: "Vie privée et protection des données: quels impacts sur vous?" le 28 janvier. La présentation, qui est principalement destinée au personnel de la Commission européenne, se tiendra à la DG ADMIN (Guimard) à 12h30.

Le CEPD participera également à la conférence concluant la **campagne "Think privacy"** lancée par European Schoolnet et Microsoft en vue de la journée de la protection des données. Cette deuxième édition de la campagne se caractérise par un concours à l'échelle européenne à destination des 15 à 19 ans qui sont invités à proposer une présentation multimédia. Le thème de cette année est "La vie privée est un droit fondamental - prêtez-y attention". Les gagnants seront sélectionnés par un jury et invités à assister à une cérémonie de remise des prix, le 28 janvier 2010, au cours de laquelle des décideurs de premier plan interviendront.

☞ **Informations complémentaires:**

- Site web du CEPD
- Site web du Conseil de l'Europe
- Initiative "Think privacy"

>> 3ème conférence internationale "Informatique, vie privée et protection des données" (Bruxelles, 29-30 janvier 2010)

La conférence "Informatique, protection de la vie privée et des données - CPDP 2010" vise à mettre en rapport les responsables politiques, les universitaires, les praticiens et les activistes, à échanger des idées et à examiner les questions émergentes des technologies de l'information, de la vie privée, de la protection des données et du droit.

La CPDP est organisée par *la Vrije Universiteit* de Bruxelles, l'Université de Namur, l'Université de Tilburg, l'Institut National de Recherche en Informatique et en Automatique et le *Fraunhofer Institut für System und Innovationsforschung.*

Des sessions générales seront animées par des parties prenantes dans la matière (telles que la Commission européenne et les autorités de protection des données), tandis que des sessions spécialisées seront consacrées à des thèmes spécifiques sur les technologies de l'information, la vie privée, la protection des données et le droit.

Le thème de la conférence de cette année sera "Un élément de choix", thème qui fait référence aux nombreuses options ouvertes pour la politique en matière de protection des données.

Des membres du secrétariat du CEPD participeront aux sessions. Peter Hustinx, Contrôleur, fournira les conclusions à la conférence.

☞ Plus d'informations sur: www.cpdpconferences.org

> Compte-rendu des événements passés

>> Conférence internationale des Commissaires à la protection des données et de la vie privée (Madrid, 4-6 Novembre 2009)

Dans la lignée de la conférence de 2008, la conférence s'est intéressée aux nouveaux défis en matière de développements technologiques et de circulation des données personnelles dans un environnement globalisé. La conférence a permis de constater le besoin croissant, exprimé par tous les acteurs, y compris la société civile et l'industrie, d'un cadre harmonisé pour la protection des données au-delà des frontières. C'est dans cet esprit que la conférence a adopté une résolution saluant le projet de normes internationales pour la protection des données et de la vie privée. Ces normes sont le résultat d'un an de travail préparatoire coordonné par l'autorité espagnole. Elles représentent un premier pas vers un instrument législatif international.

La conférence a permis des échanges de vues sur les nouveaux défis en matière de sécurité et de dialogue transatlantique entre l'Europe et les Etats-Unis. Les tendances récentes dans le secteur privé ont aussi été discutées, telles que la publicité sur Internet, le concept de "privacy by design" et la responsabilité des responsables de traitement.

☞ Plus d'informations sur: www.privacyconference2009.org

>> Séminaire sur les conséquences de failles de sécurité (Bruxelles, 23 octobre 2009)

Le séminaire, organisé par le CEPD en coopération avec l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) était principalement destiné aux responsables du traitement

de données personnelles et aux professionnels en matière de sécurité des données. Il a réuni plus de 80 participants.

Introduites par les discours d'ouverture du Contrôleur Peter Hustinx, de la Commissaire Viviane Reding, et du Directeur exécutif de l'ENISA Udo Helmbrecht, les discussions ont permis d'explorer les défis liés aux principales étapes du cycle de vie des failles de sécurité: la prévention, la gestion et la notification.

Les discussions ont fait ressortir la nécessité pour les responsables du traitement et les autres parties prenantes d'adopter une gestion adéquate des risques en vue de limiter les risques de telles failles. Il a été souligné que cela ne nécessiterait pas seulement des solutions technologiques mais aussi une amélioration des mesures d'organisation, notamment en accroissant la responsabilité des instances dirigeantes des entités concernées. Elles devraient également promouvoir le développement de garanties appropriées et favoriser une répartition plus transparente des responsabilités.

Bien que l'obligation de notifier les failles de sécurité sera introduite dans la directive "vie privée et communications électroniques", les participants ont reconnu que la dépendance croissante de la société envers les technologies de l'information et de la communication signifie que le phénomène des failles de sécurité allait déjà au-delà du secteur des communications électroniques. En ce sens, la Commission a souligné que, en consultation étroite avec le CEPD et les autres parties prenantes, elle allait envisager d'aller plus loin que la directive vie privée afin d'élargir le débat aux exigences d'application générale en matière de notification des failles de sécurité et d'examiner les solutions législatives possibles.

☞ Plus d'informations sur le site du CEPD

DISCOURS ET PUBLICATIONS

- "*Intelligent transport systems and data protection - ensuring the right balance between the protection of privacy and the efficient use of ICT in logistics*", discours (EN) (pdf) de Peter Hustinx à la conférence CLECAT - 9th Freight Forwarders (Bruxelles, 3 décembre 2009)

- "*Ensuring trust in e-Health through strong health data protection*", discours (EN) (pdf) de Peter Hustinx au Sommet de politique européenne "Planning Europe's Healthcare Revolution" organisé par *Friends of Europe* (Bruxelles, 2 décembre 2009)

- "*Data protection integrated in an EU Information Management Strategy*", discours (EN) (pdf) de Peter Hustinx au séminaire sur le programme de Stockholm organisé par la Fondation Robert Schuman au Parlement européen (Bruxelles, 12 novembre 2009)

- "*Do you have a private life at your workplace? Privacy in the workplace in EC institutions and bodies*", discours (EN) (pdf) de Giovanni Buttarelli à la 31ème Conférence internationale des Commissaires à la protection des données et à la vie privée (Madrid, 6 novembre 2009)

NOUVEAUX DELEGUES A LA PROTECTION DES DONNEES

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 en interne des obligations de protection des données établies par le règlement (CE) n° 45/2001.

Nominations récentes:

- **Frederik MALFRÈRE**, Banque centrale européenne, en remplacement de Martin BENISCH
- **Guido STÄRKLE**, Agence ferroviaire européenne
- **Anne SALAÜN**, entreprise commune Artemis
- **Silvia POLIDORI**, Clean Sky Joint Technology Initiative
- **Estefania RIBEIRO**, Initiative conjointe en matière de Médicaments Innovants

☞ 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.**

COORDONNEES

www.edps.europa.eu
Tel: +32 (0)2 34234234234
Fax: +32 (0)2 34234234234
e-mail: see our contacts page

ADRESSE POSTALE

EDPS – CEDP
Rue Wiertz 60 – MO 63
B-1047 Bruxelles
BELGIQUE

BUREAUX

Rue Montoyer 63
Bruxelles
BELGIQUE

CEPD – Le gardien européen de la protection des données personnelles