ISSN 1830-5482

Rapport annuel

2010

Le Contrôleur européen
de la protection des données

Rapport annuel

2010

Europe Direct est un service destiné à vous aider à trouver des réponses aux questions que vous vous posez sur l'Union européenne.

Un numéro unique gratuit (*):

00 800 6 7 8 9 10 11

(*) Certains opérateurs de téléphonie mobile ne permettent pas l'accès aux numéros 00 800 ou peuvent facturer ces appels.

De nombreuses autres informations sur l'Union européenne sont disponibles sur l'internet via le serveur Europa (http://europa.eu).

Une fiche catalographique figure à la fin de l'ouvrage.

Luxembourg: Office des publications de l'Union européenne, 2011

ISBN 978-92-95073-21-0
doi:10.2804/21446

© Union européenne, 2011
Reproduction autorisée, moyennant mention de la source
© Photos: Parlement européen et iStockphoto

Printed in Luxembourg

IMPRIME SUR PAPIER BLANCHI SANS CHLORE ELEMENTAIRE (ECF)

Sommaire

GUIDE DE L'UTILISATEUR

Le lecteur trouvera, immédiatement après ce guide, l'avant-propos de M. Peter Hustinx, Contrôleur européen de la protection des données (CEPD) et de M. Giovanni Buttarelli, Contrôleur adjoint, précédé de l'énoncé de leur mission.

Le chapitre 1, **«Faits marquants de 2010»**, présente les grands axes des activités du CEPD en 2010 et les résultats obtenus dans les différents champs d'activité.

Le chapitre 2, «Contrôle», décrit les travaux menés pour vérifier que les institutions et les organes de l'Union européenne (UE) s'acquittent de leurs obligations en matière de protection des données. Ce chapitre présente une analyse des principales problématiques dans le domaine des contrôles préalables, de la suite donnée aux réclamations et du contrôle du respect des règles et des avis sur les mesures administratives traitées en 2010. Il présente les lignes directrices thématiques adoptées par le CEPD dans le domaine des enquêtes administratives et des procédures disciplinaires ainsi que la suite du travail relatif aux lignes directrices sur la vidéosurveillance. Ce chapitre présente également la nouvelle politique du CEPD en matière de conformité aux règles et de répression des infractions.

Le chapitre 3, **«Consultation»**, traite de l'évolution du rôle consultatif du CEPD. Il s'intéresse principalement aux avis et commentaires formulés sur les propositions législatives et documents connexes, ainsi qu'à leur incidence dans un nombre croissant de domaines. Ce chapitre aborde également l'implication du CEPD dans les litiges soumis à la Cour de justice. Il contient une analyse de certains thèmes horizontaux, comme par exemple certains nouveaux problèmes liés à la technologie et l'évolution des politiques et de la législation.

Le chapitre 4, **«Coopération»**, décrit le travail effectué dans des forums importants comme par ex. le groupe de travail «Article 29» (groupe de travail sur la protection des données), la Conférence européenne et la Conférence internationale des commissaires à la protection des données. Il aborde également le contrôle coordonné (par le CEPD et par les autorités nationales chargées de la protection des données) des systèmes d'information et de communication à grande échelle.

Le chapitre 5, **«Communication»**, présente les activités d'information et de communication du CEPD et les résultats obtenus, y compris les activités de communication extérieure avec les médias, les événements de sensibilisation, l'information du public et les outils d'information en ligne.

Le chapitre 6, **«Administration, budget et personnel»**, détaille les principales évolutions intervenues au sein de l'organisation du CEPD, notamment en ce qui concerne les aspects budgétaires, la question des ressources humaines et les accords de nature administrative.

Le chapitre 7, **«Délégué à la protection des données (DPD) du CEPD»**, présente le travail de la nouvelle équipe du DPD du CEPD. Sur la base du plan d'action du DPD et des dispositions d'application adoptées, il souligne les progrès accomplis au niveau du registre des notifications, de la conformité avec l'«exercice de printemps», et insiste sur la nécessité d'information et de sensibilisation.

Le chapitre 8, **«Principaux objectifs pour 2011»** donne un aperçu des priorités principales pour l'année 2011.

Le rapport est complété d'**annexes**. Parmi celles-ci, un aperçu du cadre juridique pertinent, les dispositions du règlement (CE) n° 45/2001, la liste des délégués à la protection des données, la liste des avis et avis consultatifs relatifs aux contrôles préalables du CEPD, les discours prononcés par le Contrôleur et son adjoint, et la composition du secrétariat du CEPD.

Un résumé de ce rapport est également disponible, avec une vue d'ensemble synthétique des développements principaux intervenus en 2010 dans le cadre des activités du CEPD.

Pour de plus amples informations sur le CEPD, nous vous invitons à consulter notre site internet (http://www.edps.europa.eu), sur lequel vous pourrez souscrire à notre newsletter.

Il est possible de commander auprès de l'EU Bookshop (http://www.bookshop.europa.eu) ou des services du CEPD des exemplaires gratuits du rapport annuel et du résumé.

MANDAT DU CEPD

Le Contrôleur européen de la protection des données (CEPD) a pour mission de veiller à ce que, lorsqu'ils traitent des données à caractère personnel, les institutions et organes de l'Union respectent les droits fondamentaux et les libertés des personnes, en particulier leur vie privée.

Le CEPD est chargé de:

- superviser et d'assurer le respect des dispositions du règlement (CE) n° 45/2001 ([1]) et des autres actes communautaires relatifs à la protection des droits fondamentaux et des libertés lorsque les institutions et organes de l'UE traitent des données à caractère personnel (contrôle);
- conseiller les institutions et les organes de l'UE pour toutes les questions concernant le traitement de données à caractère personnel, ce qui inclut la consultation dans le cadre de l'élaboration de dispositions législatives et le suivi des nouveaux développements ayant une incidence sur la protection des données à caractère personnel (consultation);
- coopérer avec les autorités nationales de supervision et avec les organes de supervision relevant de l'ancien troisième pilier de l'UE, en vue d'améliorer la cohérence en matière de protection des données à caractère personnel (coopération).

Conformément à ces lignes d'action, le CEPD a pour objectifs stratégiques:

- de promouvoir une culture de la protection des données au sein des institutions et organes de l'Union, et de contribuer ainsi à améliorer la bonne gestion des affaires publiques;
- d'intégrer le respect des principes de protection des données dans la législation et la politique de l'Union;
- d'améliorer la qualité des politiques de l'UE, chaque fois que la protection effective des données personnelles est une condition essentielle au succès de ces politiques.

([1]) Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

AVANT-PROPOS

Nous avons l'honneur de présenter au Parlement européen, au Conseil et à la Commission le rapport annuel sur les activités du Contrôleur européen de la protection des données (CEPD), conformément au règlement (CE) n° 45/2001 du Parlement européen et du Conseil, et en application de l'article 16 du traité sur le fonctionnement de l'Union européenne, qui a remplacé l'article 286 du traité CE.

Le présent rapport concerne l'année 2010, sixième année complète d'activité du CEPD en tant que nouvelle autorité de supervision indépendante, dont la mission est de veiller à ce que, lors du traitement de données à caractère personnel, les libertés et droits fondamentaux des personnes physiques, en particulier leur vie privée, soient respectés par les institutions et organes de l'UE. Ce rapport couvre également la deuxième année de notre mandat commun de cinq ans, en tant que membres actuels de cette autorité.

Cette année a été une fois de plus d'une importance cruciale pour le droit fondamental à la protection des données. Le traité de Lisbonne, qui garantit une base juridique solide pour une protection globale des données dans tous les domaines de la politique de l'UE, a un impact de plus en plus visible. Le processus de révision du cadre juridique de l'Union en matière de données prend forme et suscite une attention croissante. Deux programmes politiques essentiels - le programme de Stockholm en matière de liberté, de sécurité et de justice, ainsi que la stratégie numérique, l'une des pierres angulaires de la stratégie Europe 2020 - démontrent la pertinence de la protection des données en tant qu'élément essentiel pour arriver à une certaine légitimité et à une efficacité dans ces deux domaines.

Le CEPD est fortement engagé dans ces différents contextes et est déterminé à poursuivre dans cette voie à l'avenir. Parallèlement, nous avons fait en sorte que la fonction d'autorité de contrôle indépendante soit exercée dans tous les principaux domaines d'activité et que son organisation soit tout à fait adéquate. Cela a débouché sur des progrès importants, à la fois dans le contrôle des institutions et des organes de l'UE lorsqu'ils traitent des données personnelles, dans la consultation sur les nouvelles politiques et les mesures législatives, de même que dans la collaboration étroite avec d'autres autorités de contrôle, afin de garantir une plus grande cohérence en matière de protection des données.

Nous souhaitons donc profiter de l'occasion qui nous est donnée pour remercier ceux qui, au sein du Parlement européen, du Conseil et de la Commission, soutiennent notre travail, ainsi que les nombreux membres des diverses institutions et des divers organes qui sont responsables de la manière dont la protection des données est mise en pratique. Nous souhaitons également encourager ceux qui doivent faire face aux défis importants qui nous attendent.

Enfin, nous souhaitons tout particulièrement remercier les membres de notre personnel. Par leurs qualités exceptionnelles, ces derniers contribuent largement à l'efficacité de notre action.

Peter Hustinx
Contrôleur européen de la protection des données

Giovanni Buttarelli
Contrôleur adjoint

1 FAITS MARQUANTS DE 2010

1.1. Éléments clés

Plusieurs événements récents ont contribué à mettre **les droits fondamentaux et la protection des données** au cœur de l'agenda européen. Le traité de Lisbonne, en vigueur depuis le 1er décembre 2009, a renforcé la protection des droits fondamentaux dans l'Union européenne (UE) en conférant à la Charte des droits fondamentaux la même valeur juridique que les traités et en imposant à l'Union européenne d'adhérer à la **Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales** (CEDH). S'agissant tout particulièrement de la protection des données, l'article 16 TFUE fournit également une base juridique générale pour la protection des individus en ce qui concerne le traitement des données à caractère personnel par les institutions et organes de l'Union, ainsi que par les États membres dans l'exercice des activités qui relèvent du champ d'application du droit de l'Union.

L'importance des droits fondamentaux en général, et de la protection des données en particulier, est encore soulignée par le **programme de Stockholm**, le programme politique quinquennal actuel dans l'espace de liberté, de sécurité et de justice. Ce programme souligne la nécessité de garantir le respect des droits fondamentaux, la liberté et l'intégrité des personnes tout en garantissant leur sécurité. En conséquence, le respect des droits de l'homme, de la dignité humaine et des autres droits inscrits dans la Charte et dans la CEDH, et notamment le droit à la vie privée et à la protection des données, sont définies comme les valeurs essentielles de l'action de l'Europe dans ce domaine. Il est important de noter que le Conseil européen a invité la Commission à soumettre «rapidement» une proposition relative à l'adhésion de l'Union à la CEDH.

Ces évolutions ont également bénéficié du soutien des autres institutions. Dans le contexte du programme de Stockholm, le Parlement européen a beaucoup insisté sur le rôle des droits fondamentaux pour le développement futur de l'espace de liberté, de sécurité et de justice[2]. La Commission elle-même a récemment adopté une communication mettant en place une stratégie pour la mise en œuvre effective de la Charte dans le nouvel environnement juridique existant depuis l'entrée en vigueur du traité de Lisbonne.

Le **processus de révision du cadre de protection des données**, lancé en 2009 et poursuivi en 2010, est un élément décisif dans la création d'une Europe des droits fondamentaux. En novembre 2010, la Commission a publié une communication définissant une approche globale de la protection des données à caractère personnel dans l'Union européenne. Cette communication décrit l'approche que la Commission compte adopter pour moderniser le cadre juridique européen de la protection des données à caractère personnel dans tous les domaines d'activité de l'Union. Cette communication vise à faire face aux défis de la mondialisation et des nouvelles technologies, afin de garantir un degré élevé de protection des données à l'avenir. Le CEPD suit de près le

[2] Résolution du Parlement européen du 25 novembre 2009 sur la communication de la Commission au Parlement européen et au Conseil - un espace de liberté, de sécurité et de justice au service des citoyens - programme de Stockholm, P7_TA(2009)0090.

processus de révision et y a déjà contribué à différents stades. Ce projet restera l'une de nos priorités principales au cours de l'année 2011.

En 2010, la Commission a également consacré des efforts considérables à la mise en œuvre des différentes initiatives liées au programme de Stockholm. Plusieurs de ces propositions reposent sur un échange intensif d'informations entre les forces de police ou les forces de sécurité de différents pays, et elles ont donc un impact substantiel sur la vie privée et sur la protection des données personnelles. Dans le développement de **l'espace de liberté, de sécurité et de justice**, le législateur européen doit toujours garder un équilibre entre la sécurité et la libre circulation des citoyens et la protection de leur vie privée et de leurs données personnelles. La mise en œuvre du programme de Stockholm a été un élément crucial des activités du CEPD en 2010, et on peut s'attendre à ce qu'il en soit de même à l'avenir.

Un autre aspect important de cette année concerne les questions de protection des données liées aux **nouvelles technologies**. La technologie actuelle permet d'échanger et de traiter des données à une échelle sans précédent. Parallèlement, le traitement des données est devenu plus subtil et moins facilement détectable. Les réseaux sociaux, l'informatique dématérialisée, la collecte des péages routiers, les dispositifs de géolocalisation, la publicité comportementale et d'autres nouveaux services similaires posent tous d'énormes défis en matière de protection des données. La révision du cadre de protection des données devra relever ces défis avec succès pour assurer un degré élevé de protection des données personnelles dans un monde reposant sur la technologie. Les nouvelles technologies sont également au cœur des initiatives reprises dans la stratégie numérique pour l'Europe de la Commission. Le CEPD examinera ces initiatives et les évaluera dans tous les cas où elles posent des problèmes de protection des données des personnes.

1.2. Aperçu général de 2010

Les principales activités du CEPD en 2010 se sont appuyées sur la même stratégie globale que précédemment, mais leur importance et les domaines couverts ont continué de se développer. L'aptitude du CEPD à agir efficacement s'est également améliorée.

Le cadre juridique([3]) dans lequel le CEPD opère définit un certain nombre de tâches et de compétences qui permettent de distinguer trois fonctions principales. Ces fonctions continuent de faire office de cadre stratégique pour les activités du CEPD et sont présentées dans l'énoncé de sa mission:

- une **fonction de supervision**, qui consiste à superviser et assurer le respect des garanties juridiques existantes par les institutions et organes de l'UE([4]) chaque fois qu'ils traitent des données à caractère personnel;

- une **fonction de consultation**, qui consiste à conseiller les institutions et les organes de l'UE sur toutes les questions pertinentes, et en particulier sur les propositions législatives ayant une incidence sur la protection des données à caractère personnel;

- une **fonction de coopération**, qui consiste à collaborer avec les autorités nationales de contrôle et les organes de contrôle relevant de l'ancien troisième pilier de l'UE chargés de la coopération policière et judiciaire en matière pénale, en vue d'améliorer la cohérence en matière de protection des données à caractère personnel.

Ces fonctions sont exposées en détail dans les chapitres 2, 3 et 4 du présent rapport annuel, qui présentent les principales activités du CEPD et les progrès réalisés en 2010. Certains éléments essentiels seront résumés dans ce chapitre.

L'importance de l'information et de la communication pour ces activités justifie entièrement que nous ayons consacré un chapitre à cet aspect de la question (cf. chapitre 5). Toutes ces activités reposent sur une gestion efficace des ressources financières, humaines et autres qui font l'objet du chapitre 6.

([3]) Cf. l'aperçu du cadre juridique à l'annexe A et un extrait du règlement (CE) n° 45/2001 à l'annexe B.

([4]) Les termes «institutions» et «organes» qui figurent dans le règlement (CE) n° 45/2001 sont utilisés tout au long du rapport. Ils désignent aussi les agences de l'UE. Pour une liste complète de celles-ci, utilisez le lien: http//europa.eu/agencies/community_agencies/index.fr.htm

Supervision

Les tâches de supervision vont du conseil et de l'aide aux délégués à la protection des données à la conduite d'enquêtes, en ce compris les inspections sur le terrain et le traitement des réclamations, en passant par le contrôle préalable des opérations de traitement des données à risque. Les avis complémentaires à l'administration de l'UE peuvent également prendre la forme de consultations concernant les mesures administratives ou la publication de lignes directrices thématiques.

Toutes les institutions et tous les organes de l'UE doivent posséder au moins un **délégué à la protection des données** (DPD). En 2010, le nombre total de DPD est passé à 47. Il est important, pour une supervision efficace, d'interagir régulièrement avec ces délégués et leurs réseaux. Un «quatuor de délégués à la protection des données», composé des quatre DPD du Conseil, du Parlement européen, de la Commission européenne et du Centre de traduction des organes de l'Union européenne a été désigné afin de coordonner le réseau des DPD. Le CEPD a étroitement collaboré avec ce quatuor.

En 2010, le **contrôle préalable** des opérations de traitement à risques a encore constitué l'essentiel des activités de supervision. Le CEPD a adopté 55 avis de contrôle préalable sur des procédures administratives standard telles que l'évaluation du personnel, le recrutement et les promotions, mais aussi sur des activités principales, comme le système d'alerte précoce et de réaction pour l'échange d'informations sur les maladies transmissibles. Ces avis sont publiés sur le site du CEPD et leur mise en œuvre fait l'objet d'un suivi systématique.

L'**application du règlement** par les institutions et organes fait également l'objet d'un suivi systématique à travers un bilan régulier des indicateurs de performance impliquant toutes les institutions et tous les organes de l'UE. À la suite de l'opération générale de contrôle lancée au printemps 2009, le CEPD a continué de contrôler la mise en œuvre des règles et principes de protection des données par les institutions et les organes concernés. La prochaine opération générale de contrôle (printemps 2011) commencera en début d'année 2011. Des contrôles ciblés ont également été effectués dans les cas où, à la suite des activités de supervision, le CEPD s'est inquiété du degré de conformité aux normes de certaines institutions ou certains organes. Certains de ces contrôles ont été réalisés par correspondance, tandis que d'autres ont pris la forme d'une visite de l'organe concerné. En 2010, le CEPD a procédé à deux visites de ce type. Le CEPD a également réalisé une inspection sur place au sein du Centre commun de recherche de la Commission à Ispra afin de vérifier la conformité par rapport à des points spécifiques.

En 2010, le nombre total des **réclamations** s'est élevé à 94; 25 de ces réclamations ont été déclarées recevables. De nombreuses réclamations irrecevables concernaient des problématiques nationales, pour lesquelles le CEPD n'est pas compétent. La plupart des questions couvertes par des réclamations recevables portaient sur des violations présumées des règles d'accès aux données, sur des cas de rectification des données, d'utilisation abusive, de collecte excessive ou de suppression des données. Dans 11 cas, le CEPD à conclu à une violation des règles de protection des données.

Des travaux ont également été effectués sous la forme d'une **consultation sur les mesures administratives** envisagées par les institutions et organes de l'UE concernant le traitement des données à caractère personnel. Diverses questions ont été évoquées, notamment en ce qui concerne les transferts internationaux de données, l'accès à l'identité d'un informateur, l'utilisation interne des courriels ou encore le contrôle électronique.

Le CEPD a également adopté des **lignes directrices** concernant les enquêtes administratives, les procédures disciplinaires et la vidéosurveillance.

En décembre 2010, le CEPD a adopté un document stratégique intitulé «Contrôler et garantir le respect du règlement (CE) n° 45/2001». Ce document définit le cadre dans lequel le CEPD contrôle, évalue et garantit le respect des règles de protection des données dans l'administration européenne. Il explique la nature des différents **pouvoirs d'exécution** conférés au CEPD et décrit les facteurs déterminants et déclencheurs de toute mesure formelle que celui-ci serait susceptible de prendre.

Consultation

En 2010, la Commission a fait des progrès importants vers un nouveau **cadre juridique modernisé de protection des données en Europe**. La consultation publique lancée en 2009 a été conclue et complétée par d'autres consultations ciblées auprès de différentes parties prenantes essentielles. En novembre 2010, la Commission a publié

sa communication définissant une approche globale en matière de protection des données à caractère personnel dans l'Union européenne, identifiant les priorités principales et les objectifs-clés pour la révision des règles actuelles.

Le CEPD a accordé une attention particulière au processus de révision tout au long de l'année 2010 et transmis ses messages par divers canaux. Le CEPD a notamment organisé une conférence de presse *ad hoc* immédiatement après la publication de la communication de la Commission afin d'exprimer publiquement son avis concernant le nouveau cadre juridique. À cette occasion, le CEPD a souligné l'importance de cette révision, dont il estime qu'il arrive à point nommé, et il a donné son point de vue concernant les principaux points du nouveau cadre.

Le CEPD a continué de mettre en œuvre sa **politique de consultation** générale et a publié un nombre record de 19 avis législatifs sur différents sujets. Cette politique assure également une approche proactive incluant un inventaire régulier des propositions législatives à soumettre à la consultation ainsi que la disponibilité de commentaires informels lors des étapes préparatoires des propositions législatives. La plupart des avis du CEPD ont été suivis au cours des discussions du Parlement et du Conseil.

En 2010, le CEPD a suivi de près plusieurs initiatives directement liées à la mise en œuvre du **programme de Stockholm**. Le CEPD s'est notamment penché sur des questions critiques de protection des données liées à la stratégie de sécurité intérieure, à la gestion de l'information dans l'espace de liberté, de sécurité et de justice, ainsi qu'à la politique antiterroriste européenne et les règlements Frontex et Eurodac. Dans l'ensemble, les développements ayant trait au programme de Stockholm ont dominé le programme de travail du CEPD et continueront de le faire au cours des prochaines années.

L'interface entre la vie privée et les développements technologiques est également un domaine dans lequel le CEPD est intervenu de façon significative. En mai 2010, la Commission a publié sa communication relative à une stratégie numérique pour l'Europe, l'objectif étant de fixer les priorités de l'Union dans les domaines de l'internet et des technologies numériques. En mars 2010, le CEPD a adopté un avis sur «la promotion de la confiance dans la société d'information par des mesures d'encouragement de la protection des données et de la vie privée», qui constitue sa contribution à cette stratégie numérique. Il est également intervenu de diverses façons dans des initiatives relatives à l'internet et à la neutralité du réseau, à la révision de la directive sur la conservation des données, à la directive sur les déchets électroniques et électriques, au règlement ENISA et à la justice en ligne.

Le CEPD a également été consulté à propos de différentes initiatives dans le domaine de la **coopération internationale en matière de sécurité et de maintien de l'ordre**, comme l'accord général UE - États-Unis relatif à l'échange de données à des fins de maintien de l'ordre et l'accord relatif à l'échange de données financières aux fins du programme de surveillance du financement du terrorisme (TFTP II). Il est également intervenu dans le contexte de l'accord commercial anti-contrefaçon (ACAC) et des accords relatifs à l'échange des dossiers passagers (PNR).

Le CEPD est également intervenu dans d'autres domaines tels que la fiscalité et les douanes (y compris la coopération administrative dans le domaine de la fiscalité et de la coopération douanière internationale), les échanges de données à grande échelle dans le contexte du Système d'information sur le marché intérieur, l'utilisation des scanners de sûreté dans les aéroports ou encore différentes affaires portant sur la relation entre l'accès public et la protection des données.

Coopération

La principale plate-forme de coopération entre les autorités de protection des données en Europe est le groupe de travail «Article 29» sur la protection des données. Le CEPD participe aux activités de ce groupe de travail, qui joue un rôle important dans l'application uniforme de la directive sur la protection des données.

Le CEPD et le groupe de travail «Article 29» coopèrent en parfaite synergie sur toute une série de sujets, en particulier en ce qui concerne la mise en œuvre de la directive relative à la protection des données et l'interprétation de certaines de ses dispositions principales. Le CEPD a contribué activement dans différents domaines, par ex. par des avis concernant les concepts de «responsable du traitement» et de la «sous-traitance», le principe de responsabilité et le droit applicable.

Le CEPD participe également aux réunions et aux activités du Groupe de travail sur la police et la

Chiffres-clés du CEPD en 2010

➔ **55 avis de contrôle préalable adoptés,** concernant notamment les données relatives à la santé, l'évaluation du personnel, le recrutement, la gestion du temps, les enquêtes concernant la sécurité, les enregistrements téléphoniques et les outils de performances

➔ **94 réclamations reçues, dont 25 recevables.** Principaux types de violations alléguées: violation de la confidentialité des données, collecte excessive de données ou usage illégal de données par le responsable du traitement.

- **10 affaires résolues** dans lesquelles le CEPD n'a constaté aucune violation des règles de protection des données
- **11 violations déclarées** des règles de protection des données

➔ **35 consultations sur les mesures administratives.** Des conseils ont été donnés sur toute une série d'aspects juridiques liés au traitement des données personnelles par les institutions et organes de l'UE

➔ **1 inspection sur place effectuée**

➔ **2 lignes directrices publiées:** l'une sur les enquêtes administratives et les procédures disciplinaires, et l'autre sur la vidéosurveillance.

➔ **19 avis législatifs rendus** concernant des initiatives relatives au domaine de la liberté, de la sécurité et de la justice, aux évolutions technologiques, à la coopération internationale et au transfert des données, ainsi qu'à la fiscalité et aux douanes.

➔ **7 séries d'observations formelles publiées,** concernant notamment la révision du règlement Frontex, l'internet libre et la neutralité du réseau, le Système d'information sur le marché intérieur, les scanners de sûreté et les accords internationaux d'échange de données

➔ **3 réunions du Groupe de coordination du contrôle d'Eurodac organisées;** celles-ci ont permis de lancer une nouvelle inspection coordonnée et d'entamer les travaux de préparation d'un audit de sécurité complet.

➔ **12 nouveaux fonctionnaires recrutés**

justice, un groupe consultatif traitant de questions qui relevaient précédemment du troisième pilier.

L'une des tâches de coopération les plus importantes du CEPD concerne Eurodac. La responsabilité de la supervision est ici partagée avec les autorités nationales de protection des données. Le groupe de coordination du contrôle d'Eurodac, composé de représentants des autorités nationales chargées de la protection des données et du CEPD, s'est réuni à trois reprises à Bruxelles, en mars, en octobre et en décembre 2010. Ce groupe a entamé les travaux préparatifs en vue de l'audit de sécurité complet qui devra être effectué par les autorités responsables de la protection des données au niveau national comme au niveau central (UE). Une nouvelle inspection coordonnée a été lancée fin 2010, et ses résultats sont attendus pour 2011.

En ce qui concerne le contrôle du Système d'information douanier (SID), le CEPD a organisé deux réunions du groupe de coordination du contrôle du SID en 2010. Ces réunions ont rassemblé les représentants des autorités nationales chargées de la protection des données ainsi que des représentants de l'Autorité de contrôle commune des douanes et du Secrétariat chargé de la protection des données. Lors de la réunion de décembre, ce groupe a adopté le règlement qui régira ses travaux futurs relatifs au SID et discuté des mesures à prendre éventuellement en 2011-2012 afin de garantir un contrôle global de la protection des données dans ce système.

Le CEPD a poursuivi sa coopération étroite avec les autorités mises en place pour exercer un contrôle commun des systèmes informatiques à grande échelle de l'Union.

La coopération au sein d'autres forums internationaux a continué d'attirer l'attention, notamment la conférence européenne et la conférence internationale des commissaires à la protection des données et de la vie privée, organisées respectivement à Prague et à Jérusalem.

En collaboration avec l'Université européenne de Florence, le CEPD a également organisé un atelier sur la «Protection des données dans les institutions internationales». Cet atelier s'est penché sur différents problèmes rencontrés par les organisations internationales qui s'efforcent d'assurer un bon niveau de protection des données dans des contextes parfois difficiles et sans base juridique claire.

1.3. Résultats obtenus en 2010

Les principaux objectifs suivants avaient été fixés en 2009. La plupart de ces objectifs ont été totalement ou partiellement atteints.

- **Soutien au réseau des délégués à la protection des données**

Le CEPD a continué de soutenir pleinement les délégués à la protection des données et encouragé l'échange de compétences et de bonnes pratiques. Dans le cadre de leur réseau, les DPD ont rédigé un document sur les «Normes professionnelles des délégués à la protection des données des institutions et organes européens travaillant en application du règlement (CE) n° 45/2001». Le CEPD a envoyé une lettre à tous les directeurs et autres personnes responsables des institutions et agences de l'UE, dans laquelle il approuve les normes ainsi définies et souligne l'importance du rôle des DPD pour garantir la conformité aux règles de protection des données énoncées dans le règlement.

- **Rôle du contrôle préalable**

Le CEPD a quasiment achevé le contrôle préalable des opérations de traitement existantes pour la plupart des institutions et des organes établis. Lors de ce contrôle, il a mis un accent particulier sur le suivi des recommandations. Cette année, 137 cas ont été résolus. Une attention particulière a été accordée au contrôle préalable des opérations de traitement communes dans les agences, de même qu'au traitement des affaires susmentionnées dans le cadre d'avis conjoints.

- **Lignes directrices horizontales**

En vue de garantir la conformité au sein des institutions et des organes de l'UE, et de simplifier les procédures de contrôle préalable, le CEPD a publié des lignes directrices sur les enquêtes administratives et les procédures disciplinaires, ainsi qu'en matière de vidéosurveillance.

- **Politique d'inspection**

En 2010, le CEPD a procédé au suivi des inspections antérieures. Il a par ailleurs procédé à une inspection au Centre commun de recherche de la Commission, à Ispra. En décembre 2010, le CEPD a publié une ligne politique exhaustive sur le contrôle de la conformité et l'application des règles valables en matière de protection des données dans les institutions et organes de l'UE.

- **Étendue des consultations**

Le CEPD a publié un nombre record de 19 avis et 7 séries d'observations formelles sur les propositions de nouvelle législation, en s'appuyant sur un inventaire systématique des matières et des priorités pertinentes. Il a également veillé à ce que ces avis et observations fassent l'objet d'un suivi adéquat. Tous les avis et observations, ainsi que l'inventaire, sont disponibles sur son site internet. Une attention particulière a été accordée au plan d'action pour la mise en œuvre du programme de Stockholm.

- **Révision du cadre juridique**

À diverses occasions et en ayant recours à différents outils, le CEPD a encouragé l'adoption d'une approche ambitieuse consistant à mettre en place un cadre juridique moderne et exhaustif de protection des données couvrant toutes les politiques de l'UE et assurant une protection efficace dans la pratique, tout en étant à même de garantir la sécurité juridique pendant de nombreuses années. Le CEPD a exposé ses points de vue dans un avis publié en janvier 2011.

- **Stratégie numérique**

Dans le cadre de l'exercice de son rôle consultatif, le CEPD s'est concentré sur les principaux défis à relever pour parvenir à une protection efficace des données à caractère personnel. À cette fin, il convient d'assurer un juste équilibre entre la nécessité de sécurité et la protection des données, en tenant compte des évolutions technologiques et en faisant face aux effets des flux internationaux de

données. Dans un avis adopté en mars 2010, le CEPD a accordé une attention particulière à la stratégie numérique de la Commission, en intégrant le principe du respect de la vie privée dès la conception (*Privacy by Design*).

- **Activités d'information**

Le CEPD a poursuivi ses efforts pour améliorer la qualité et l'efficacité des actions de communication et des outils d'information. L'introduction de l'allemand en tant que troisième langue, en complément de l'anglais et du français, pour les communiqués de presse et autres activités de communication a représenté une évolution majeure à cet égard.

- **Organisation interne**

Le secrétariat du CEPD a été réorganisé en vue d'une définition plus précise des responsabilités de chacun et d'une exécution plus efficace et plus efficiente des différentes fonctions et tâches. Dans la nouvelle structure organisationnelle, le directeur assume la responsabilité de la mise en œuvre des politiques et de la coordination horizontale des activités mises en place dans cinq secteurs distincts. Le nouvel organigramme est disponible sur le site web.

- **Gestion des ressources**

Au cours de l'année 2010, le nombre de membres du personnel du CEPD a connu une augmentation considérable (un tiers). Cette hausse de l'effectif a nécessité non seulement de procéder à une réorganisation interne, mais aussi de consentir de nouveaux efforts en matière de planification, de procédures internes et d'exécution budgétaire. Une attention particulière a été accordée à un nécessaire espace de bureaux supplémentaire et au développement d'un système de gestion des dossiers.

2 SUPERVISION ET MISE EN APPLICATION

2.1. Introduction

La mission du CEPD, en sa qualité de contrôleur indépendant, consiste à surveiller le traitement des données à caractère personnel effectué par les institutions et organes de l'UE (à l'exclusion de la Cour de justice dans l'exercice de ses fonctions juridictionnelles). Le règlement (CE) n° 45/2001 (ci-après «le règlement») définit et confère un certain nombre de fonctions et de compétences qui permettent au CEPD de s'acquitter de sa tâche.

Le traité de Lisbonne constitue un changement de cadre juridique pour la protection des données dans l'administration européenne, avec l'introduction de l'article 16 du traité sur le fonctionnement de l'Union européenne, qui remplace l'article 286 du traité CE. Du fait de la suppression de la structure en piliers, la mission de contrôle du CEPD couvre désormais en principe tous les organes et toutes les institutions de l'UE, y compris dans des domaines qui se situent complètement en dehors de l'ancien «droit communautaire»([5]), sauf disposition contraire explicite dans d'autres actes législatifs de l'Union. Les conséquences précises de ces changements pour les activités de contrôle du CEPD font encore l'objet d'un examen et pourraient nécessiter une clarification supplémentaire.

Le contrôle préalable des opérations de traitement est resté un élément important de la supervision en 2010 (voir section 2.3), avec une attention particulière accordée au suivi des recommandations émises dans le cadre de ses avis. Le CEPD s'est également consacré à d'autres formes de supervision, comme le traitement des réclamations, les inspections, les avis sur les mesures administratives et la rédaction de lignes directrices thématiques. Le contrôle d'Eurodac est une activité spécifique du CEPD qui nécessite une coopération étroite avec les autorités nationales chargées de la protection des données (voir section 4.2).

Le CEPD a également adopté une politique en matière de conformité et de mise en œuvre, signalant par là un changement de rythme dans l'application du règlement.

2.2. Délégués à la protection des données

Un élément intéressant du paysage de la protection des données dans les institutions de l'Union européenne est l'obligation de désigner un délégué à la protection des données (DPD) (article 24, paragraphe 1, du règlement). Certaines institutions ont associé à ce DPD un assistant ou un adjoint. La Commission a également nommé un DPD pour l'Office européen de lutte antifraude (l'OLAF, une direction générale de la Commission). Plusieurs institutions ont également nommé des coordinateurs de la protection des données chargés de coordonner tous les aspects de la protection des données au sein d'une direction ou d'unité particulière.

([5]) Voir l'article 3, paragraphe 1, du règlement (CE) n° 45/2001, qui est désormais moins pertinent qu'avant le 1er décembre 2009.

En 2010, deux nouveaux DPD ont été nommés dans de nouvelles agences ou des entreprises conjointes, ce qui porte leur nombre total à 47.

Depuis plusieurs années, les DPD se rencontrent régulièrement afin d'échanger leurs expériences et d'examiner les questions horizontales. Ce réseau informel a fait la preuve de son efficacité en termes de collaboration, ce qui a continué d'être le cas en 2010.

Un «quatuor de délégués à la protection des données», composé de quatre DPD (Conseil, Parlement européen, Commission européenne et Centre de traduction des organes de l'Union européenne) a été désigné afin de coordonner le réseau des DPD. Le CEPD a étroitement collaboré avec ce quatuor.

Le CEPD a assisté aux réunions des DPD organisées en mars 2010 à la Banque européenne d'investissement à Luxembourg, et en octobre 2010 à l'Agence européenne des médicaments à Londres. Il en a profité pour informer les DPD sur ses activités, pour donner un aperçu des derniers développements en matière de protection des données dans l'UE et pour discuter des questions d'intérêt commun.

Plus particulièrement, le CEPD a saisi l'occasion de ce forum pour expliquer et discuter de la procédure de contrôle préalable, pour rendre compte de l'évolution des notifications en vue d'un contrôle préalable, pour informer les DPD des discussions en cours avec les comités interinstitutionnels, pour expliquer la nouvelle structure et pour présenter les lignes directrices thématiques du CEPD. Le CEPD a également informé les DPD de l'adoption de la politique de conformité et d'application. Ce forum permet également de partager des initiatives en vue de la Journée européenne de la protection des données (le 28 janvier).

Dans le cadre de leur réseau, les DPD ont rédigé un document sur les «Normes professionnelles des délégués à la protection des données des institutions et organes européens travaillant en application du règlement (CE) n° 45/2001», finalisé lors de la réunion du réseau des DPS du 14 octobre 2010. Le CEPD a envoyé une lettre à tous les directeurs et aux autres personnes responsables des institutions et agences de l'UE, dans laquelle il souscrit aux normes ainsi définies et souligne l'importance du rôle des DPD pour garantir la conformité aux règles de protection des données énoncées dans le règlement. Le CEPD entend s'inspirer de ce document, lorsque cela s'avère indiqué, dans sa mission de contrôle vis-à-vis des institutions et des organes de l'Union.

Les délégués à la protection des données lors de leur réunion à Bruxelles (mars 2010).

2.3. Contrôles préalables

2.3.1. Base juridique

L'article 27, paragraphe 1, du règlement (CE) n° 45/2001 prévoit que tous «les traitements susceptibles de présenter des risques particuliers au regard des droits et des libertés des personnes concernées du fait de leur nature, de leur objet ou de leur finalité» doivent être soumis au contrôle préalable du CEPD.

L'article 27, paragraphe 2, du règlement dresse une liste non exhaustive des opérations de traitement susceptibles de présenter des risques. Les critères élaborés au cours des années précédentes(6) ont continué d'être appliqués pour l'interprétation de cette disposition, tant pour décider qu'un cas notifié par un DPD ne devait pas faire l'objet d'un contrôle préalable que pour émettre un avis dans le cadre d'une consultation sur la nécessité de procéder à un tel contrôle (voir le point 2.3.4).

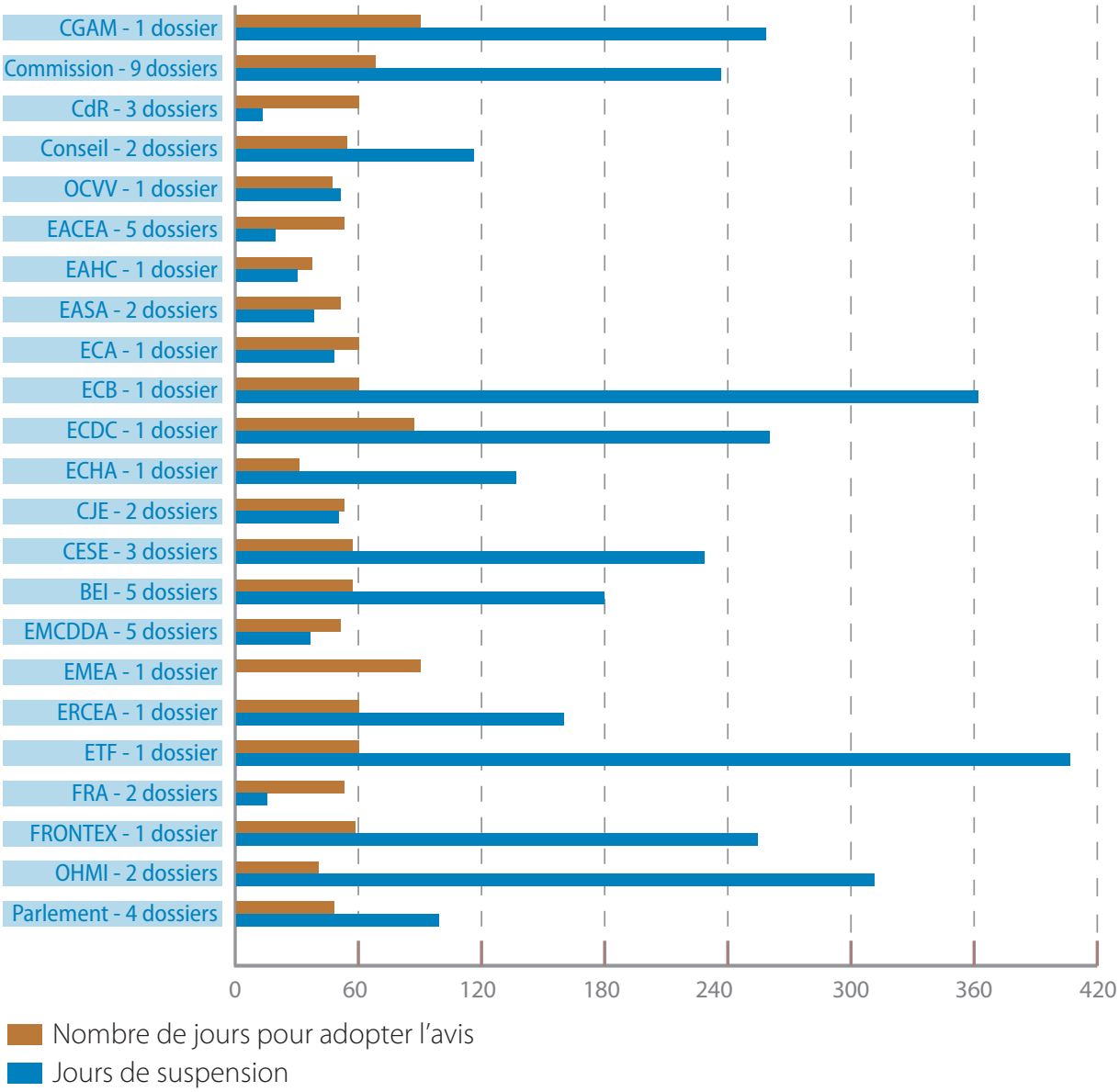
2.3.2. Procédure

Notification

Les contrôles préalables doivent être effectués par le CEPD après réception de la notification du DPD. Si celui-ci hésite quant à la nécessité de soumettre une

(6) Cf. rapport annuel 2005, point 2.3.1.

Délais moyens par institution/agence



opération de traitement à un contrôle préalable, il peut consulter le CEPD (voir le point 2.3.4).

Les contrôles préalables concernent les opérations qui ne sont pas encore en cours, mais aussi les traitements qui ont commencé avant le 17 janvier 2004 (date de nomination du CEPD et de son adjoint) ou avant l'entrée en vigueur du règlement (contrôles préalables *ex post*). Dans ces situations, un contrôle dans le cadre de l'article 27 ne peut être «préalable» au sens strict du terme, mais doit être traité *a posteriori*.

Délai, suspension et prolongation

Le CEPD doit rendre son avis dans les deux mois qui suivent la réception d'une notification(7). Lorsqu'il demande des informations complémentaires, le délai de deux mois est généralement suspendu jusqu'à ce que les informations en question lui aient été communiquées. Cette période de suspension comprend le délai accordé au DPD pour formuler ses observations et fournir, le cas échéant, des informations complémentaires sur le projet final. Lorsque la complexité du dossier l'exige, le CEPD peut également prolonger la période initiale de deux mois. Si, au terme de ce délai de deux mois, éventuellement prolongé, aucune décision n'a été rendue, l'avis du CEPD est réputé favorable. Jusqu'à présent, ce cas de figure dans lequel l'avis aurait été rendu de manière tacite ne s'est jamais produit.

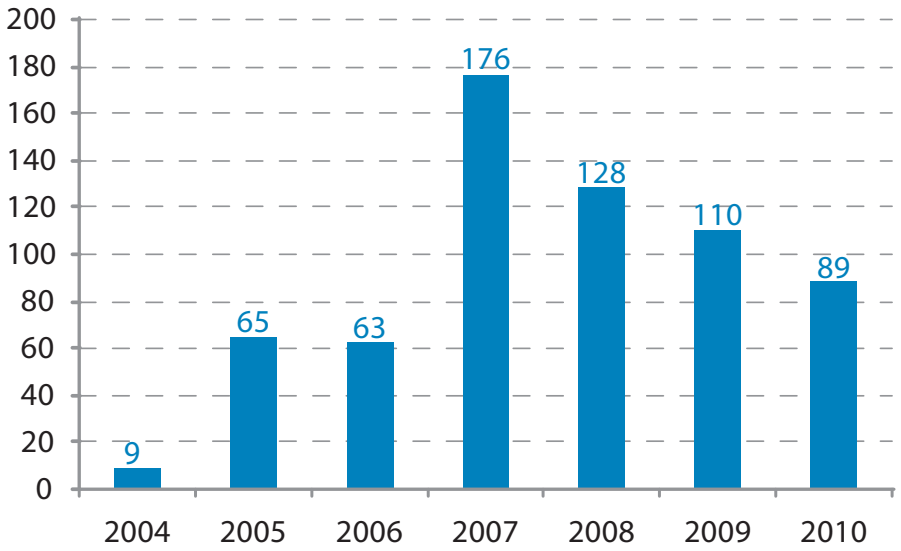
(7) Pour les cas examinés a posteriori reçus avant le 1er septembre 2010, le mois d'août a été exclu des calculs, tant pour les institutions/organes que pour le CEPD.

Registre

En 2010, le CEPD a reçu 89 notifications pour contrôle préalable, soit une légère baisse par rapport à 2009, étant donné que le CEPD arrive au bout de l'arriéré des dossiers de contrôle préalable *ex post*.

L'article 27, paragraphe 5, du règlement prévoit que le CEPD doit tenir un registre de tous les traitements qui lui sont notifiés en vue d'un contrôle préalable. Ce registre doit contenir les informations visées à l'article 25 et être accessible au public pour consultation. Par souci de transparence, toutes les

Notifications au CEPD

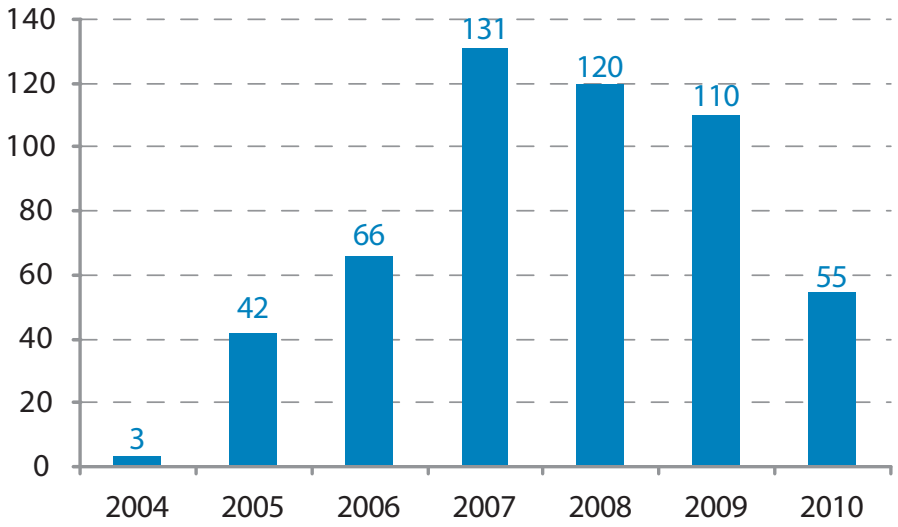


informations sont consignées dans le registre disponible sur le site internet du CEPD (à l'exception des mesures de sûreté, qui ne sont pas mentionnées dans le registre).

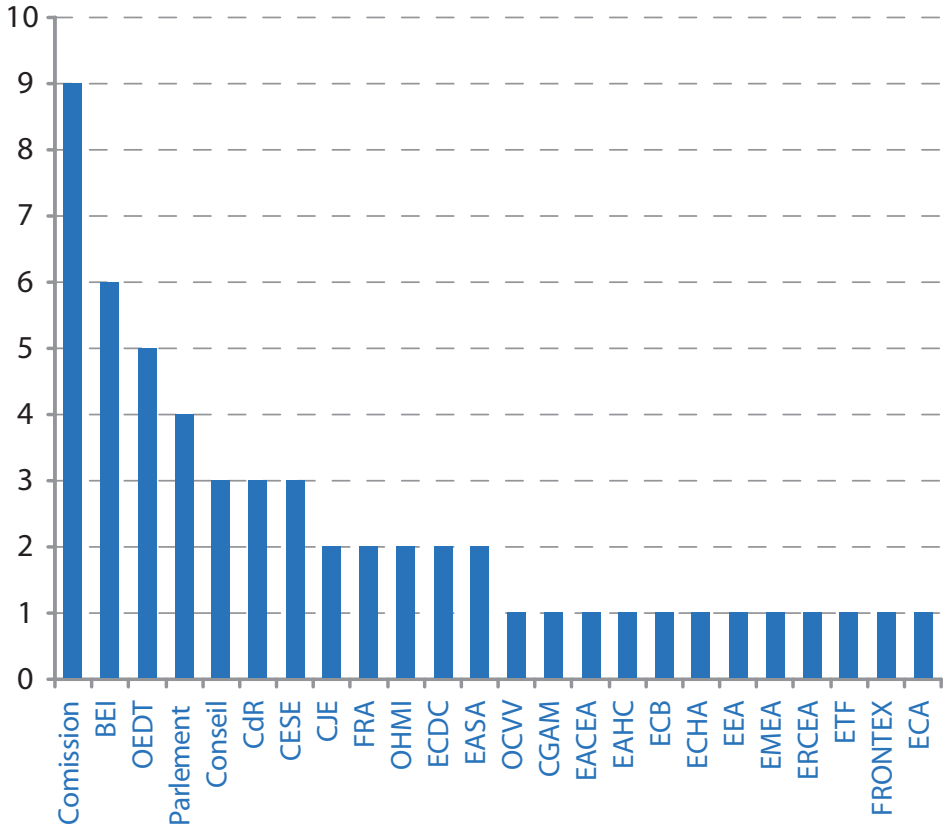
Avis

Conformément à l'article 27, paragraphe 4, du règlement, la position finale du CEPD revêt la forme d'un avis qui doit être notifié au responsable du traitement et au délégué à la protection des données de l'institution ou de l'organe concerné. En 2010, le CEPD a rendu **55 avis sur des notifications en vue d'un contrôle préalable** (voir ci-dessus,

Avis du CEPD faisant suite à un contrôle préalable, par an



Avis du CEPD faisant suite à un contrôle préalable, par institution en 2010



le graphique «nombre d'avis du CEPD en vue d'un contrôle préalable par an»), et **8 avis concernant des contrôles non préalables** (voir point 2.3.5). Même si ces chiffres représentent une baisse par rapport aux années précédentes, on notera qu'à la suite des lignes directrices sur la vidéosurveillance et le recrutement, le CEPD a traité un nombre important de cas via des opinions communes, ce qui est une façon plus efficace de traiter ces problèmes.

Une **grande partie de ces avis concernent les grandes institutions**: neuf avis de contrôle préalable (et trois contrôles non préalables) concernent des opérations au niveau de la Commission européenne, quatre au Parlement européen et trois au Conseil (voir le graphique «Avis du CEPD par institution»). Les agences ont également continué de notifier leurs activités principales et des procédures administratives standard conformément aux procédures établies par le CEPD (voir point 2.3.2).

Les avis contiennent une description de la procédure, un résumé des faits et une analyse juridique examinant si le traitement respecte les dispositions applicables du règlement. Si nécessaire, des recommandations sont formulées à l'intention du responsable du traitement en vue de garantir le respect du règlement. Dans ses conclusions, le CEPD déclare généralement que le traitement ne paraît pas entraîner de violation d'une disposition quelconque du règlement, pour autant qu'il soit tenu compte des recommandations émises.

Une fois que le CEPD a rendu son avis, celui-ci est rendu public. Tous les avis, ainsi qu'un résumé du dossier concerné, sont disponibles sur le site internet du CEPD.

Un manuel garantit que l'ensemble du personnel s'appuie sur des bases identiques et que les avis du CEPD sont adoptés à l'issue d'une analyse complète de toutes les informations pertinentes. Ce manuel comprend un modèle d'avis basé sur l'expérience pratique accumulée jusqu'à présent et mis à jour en permanence. Un système de gestion des tâches a été mis en place pour s'assurer que toutes les recommandations relatives à un dossier donné sont mises en œuvre et, le cas échéant, que toutes les décisions sont respectées (voir le point 2.3.6).

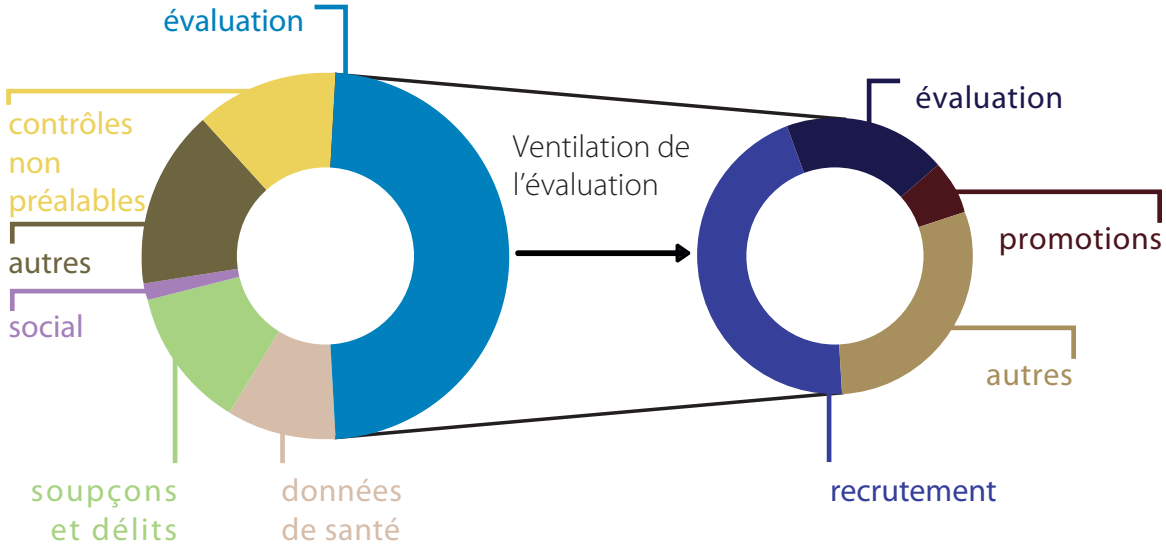
Procédure applicable aux contrôles préalables *ex post* dans les agences

En octobre 2008, le CEPD a lancé une nouvelle procédure applicable aux contrôles préalables *ex post* dans les agences. Étant donné que les procédures standard sont identiques dans la plupart des agences de l'UE et sont fondées sur des décisions de la Commission, l'idée est de rassembler les notifications portant sur un thème similaire et soit de rendre un avis collectif (pour plusieurs agences), soit de réaliser un «mini-contrôle préalable» traitant des seuls besoins spécifiques d'une agence. Pour aider les agences à remplir leurs notifications, le CEPD présentera un résumé des principaux points et conclusions sur le thème concerné en s'inspirant des avis rendus sur la notification en vue d'un contrôle préalable (voir la section 2.7 «Lignes directrices thématiques»).

Le premier thème était le **recrutement**, qui a fait l'objet d'un avis horizontal du CEPD en mai 2009, couvrant les notifications de 12 agences. Un deuxième ensemble de lignes directrices a été envoyé aux agences à la fin septembre 2009 concernant **le traitement des données relatives à la santé**. Au moment de la rédaction du présent rapport, le CEPD a envoyé son projet d'avis horizontal aux 19 agences concernées en vue de recevoir leurs commentaires. Il espère pouvoir adopter cet avis au début de l'année 2011. En avril 2010, le CEPD avait émis des lignes directrices concernant le traitement des données à caractère personnel dans les **enquêtes administratives et les procédures disciplinaires** des institutions et organes européens. Le CEPD reçoit actuellement des notifications de la part des agences dans ce domaine et compte adopter un avis commun au cours du premier semestre 2011.

2.3.3. Principales questions liées aux contrôles préalables

Avis 2010 par catégorie



2.3.3.1. Système d'alerte précoce et de réaction - Commission européenne

Le Système d'alerte précoce et de réaction (SAPR) est un outil de communication utilisé par la Commission, le Centre européen de prévention et de contrôle des maladies (CEPCM) et les États membres de l'UE pour échanger des informations relatives à la prévention des maladies transmissibles (telles que la tuberculose, la rougeole, SARS, H1N1 et d'autres) afin de faciliter les actions transfrontalières. Une caractéristique du SAPR est la «**recherche des contacts**» (*contact tracing*), une procédure utilisée pour identifier et contacter les personnes susceptibles d'avoir été en contact avec une personne infectée. Une fois ces contacts identifiés, il est possible de les diagnostiquer et de leur assurer les soins nécessaires. La recherche des contacts sert également des intérêts de santé publique en limitant ou en empêchant la propagation de la maladie.

Dans son avis (dossier 2009-0137), le CEPD se concentre sur la nécessité de **déterminer clairement les rôles, tâches et responsabilités** des parties impliquées dans l'exploitation et l'utilisation du système, et notamment les rôles de la Commission et de l'ECDC. Les responsables du traitement et les sous-traitants doivent être désignés clairement d'une façon qui corresponde à leurs rôles effectifs et au statut juridique des organisations impliquées.

Il convient de spécifier clairement les responsabilités des parties impliquées et la façon dont les personnes concernées peuvent exercer leurs droits. À court terme, il a été conseillé au SAPR d'adopter un ensemble de lignes directrices en matière de protection des données. La Commission a également été encouragée à réviser le cadre juridique afin de garantir une base juridique plus sûre et une répartition claire des responsabilités.

Le CEPD a également souligné la nécessité de mettre en œuvre le principe du **respect de la vie privée dès la conception** («Privacy by Design») et d'intégrer la protection des données à la formation des utilisateurs. Il convient de prévoir un mécanisme clair permettant aux personnes concernées de faire valoir leur **droit d'accès** aux données. Enfin, pour garantir la cohérence et la transparence, l'opérateur du SAPR devrait fournir des **informations**

Le SAPR est un outil de communication pour l'échange d'informations relatives aux maladies transmissibles.

complètes et facilement compréhensibles aux personnes concernées sur son site internet. Ces informations devraient être complétées par des notices fournies par les points de contact des États membres conformément aux législations nationales en matière de protection des données.

2.3.3.2. Système européen de surveillance («TESSy») - Centre européen pour la prévention et le contrôle des maladies

Le 3 septembre 2010, le CEPD a rendus un avis de contrôle préalable (dossier 2009-0474) concernant les aspects liés à la protection des données de TESSy. TESSy est un outil de communication du Centre européen de prévention et de contrôle des maladies. Il a été conçu pour assurer un échange rapide et efficace des données de surveillance épidémiologique entre les États membres de l'UE.

Cet avis explique que les **données statistiques** restent considérées comme des «données à caractère personnel», et donc soumises au règlement, aussi longtemps que les personnes concernées peuvent être identifiées, même de façon indirecte. Le fait que certaines «techniques d'anonymisation» aient été utilisées ne signifie pas nécessairement que ces données soient «suffisamment anonymes» au sens du considérant 8 du règlement, et qu'elles ne soient donc plus considérées comme des données à caractère personnel.

Le CEPD a réaffirmé bon nombre des recommandations émises dans l'avis rendu au SAPR (voir ci-dessus) et ajouté qu'une politique de sécurité spécifique devrait être adoptée le plus rapidement possible afin d'aider à garantir la sécurité de TESSy.

2.3.3.3. Régime commun d'assurance maladie

Le comité de gestion du régime commun d'assurance maladie (CGAM) est chargé du fonctionnement du régime commun d'assurance maladie. Le CGAM se compose de représentants du personnel désignés par les comités du personnel de chaque institution et de représentants des administrations. Il gère les modifications des règles, les réclamations introduites par ses membres et émet des avis, des recommandations et des avis concernant le fonctionnement de ce régime.

Le CEPD et le CGAM se sont réunis en novembre 2008 pour évoquer les questions liées à la protection des données dans le contexte des dossiers gérés par le CGAM. Comme les réclamations des membres contiennent souvent des données sensibles, il a été décidé que le comité enverrait une notification au CEPD.

Cette notification a abouti à un avis (dossier 2009-0070), rendu le 18 janvier 2010, dans lequel le CEPD fait des recommandations concernant notamment la **transmission de données à caractère personnel** au CGAM, la **période de conservation** sur CIRCA (une application web pour les groupes de travail utilisant des données partagées) et l'adoption **d'une politique de sécurité adéquate** dans un délai de six mois suivant l'adoption de cet avis.

2.3.3.4. Inspections de sécurité - Commission européenne (Centre commun de recherche, Ispra)

Le 6 septembre 2010 (dossier 2009-0682), le CEPD a rendu un avis de contrôle préalable concernant les inspections de sécurité au Centre commun de recherche de la Commission européenne d'Ispra. Cet avis concernait les opérations de traitement des données effectuées dans le but de préserver et d'améliorer les normes de sécurité en vigueur.

Le CEPD a reconnu que la «*Procedura in caso d'infortunio*» (procédure en cas de catastrophe) nécessite le traitement de données relatives à la santé par différentes parties dans le but de prévenir et de réduire au minimum les conséquences d'incidents de sécurité de ce genre sur le site Ispra.

Le CEPD a émis des recommandations visant à **garantir le respect du principe de «limitation de la finalité» en cas de transfert de données** ainsi que la **conformité aux principes de qualité des données** applicables au stockage et au traitement de données à caractère personnel traitées dans ce contexte. Il a également été suggéré de réviser la déclaration de confidentialité en ce sens.

2.3.3.5. Inventaire de la perception de soi de BELBIN - École européenne d'administration

La finalité du traitement est de permettre aux participants aux formations de l'École européenne d'administration (EEA) de recevoir des commentaires et des réactions sous la forme d'un rapport décrivant leur rôle préféré au sein d'une équipe. Ces données ne doivent intervenir dans aucune forme d'évaluation de la personne concernée. Dans son avis du 15 mars 2010 (dossier 2009-0377), le CEPD s'est concentré sur deux aspects:

- **La relation entre responsable du traitement, sous-traitants et sous-contractant**. Même si l'EEA n'a pas accès aux données traitées par le sous-contractant, ce dernier doit agir conformément aux instructions qui ont été données par l'EEA au contractant. L'EEA est le responsable de ce traitement des données car c'est elle qui définit les objectifs et les moyens utilisés (utilisation de l'outil en ligne). Les trois contractants chargés d'assurer les formations et le sous-contractant responsable de l'outil en ligne sont tous considérés comme des sous-traitants de données personnelles agissant pour le compte de l'EEA. Le sous-contractant n'est pas autorité à effectuer tout traitement autre que celui défini par l'EEA et précisé dans le contrat conclu entre le sous-contractant et le contractant conformément au contrat conclu entre l'EEA et le contractant.

- **Le caractère anonyme des données**. Le rapport remis aux participants ne peut pas être considéré comme «anonyme» parce que le sous-contractant est en mesure de lier les réponses aux personnes concernées; en effet, les participants utilisent généralement une adresse de courrier électronique indiquant leur nom et leur prénom.

Le CEPD a émis des recommandations concernant ces deux aspects. Il recommande en particulier que le contrat comporte une clause spécifiant tous les éléments obligatoires, notamment la **confidentialité et la sécurité du traitement** entre le contractant et le sous-contractant.

2.3.3.6. Contrôle électronique - Cour des comptes

La **Cour des comptes** a élaboré une procédure d'**accès aux supports informatiques privés et aux courriers électroniques** afin de pouvoir faire face à diverses situations (par ex. décès, départ ou absence d'un membre du personnel) dans lesquelles les données situées dans ces supports sont nécessaires au fonctionnement de l'institution. La procédure proposée impose à la personne qui introduit la demande d'information de compléter un formulaire standard. Cette demande doit contenir une proposition détaillée de la/des raison(s) justifiant l'accès, le nom du ou des fichiers, le compte de courrier électronique et/ou la nature de l'information. Ce formulaire doit être envoyé au responsable de la sécurité informatique ou, en son absence, au responsable de la sécurité physique.

La Cour des comptes a élaboré une procédure d'accès aux disques durs et courriers électroniques privés.

À l'origine, la demande était envoyée au CEPD pour consultation, parce que cette procédure **implique potentiellement un accès à des données confidentielles** et que le CEPD avait effectivement considéré que cette opération de traitement présentait des risques spécifiques nécessitant une notification en vue d'un contrôle préalable.

Dans son avis du 10 janvier 2010 (**dossier 2009-0629**), le CEPD a **recommandé** à la CC d'adopter une **base juridique spécifique** pour l'utilisation et le stockage des courriels privés et de définir des **lignes directrices claires** pour l'utilisation des ressources en réseau et des courriels.

2.3.3.7. Retenues sur salaire en cas de grève - Banque centrale européenne

En vertu de l'article 1.4 du statut du personnel de la Banque centrale européenne (BCE), les membres du personnel jouissent du droit de grève. L'article 1.4.5 prévoit que «sauf décision contraire du Conseil des gouverneurs, la durée totale de la grève est déduite des paiements salariaux au membre du personnel prenant part à la grève». En outre, «aucune mesure disciplinaire ne peut être prise à l'encontre d'un membre du personnel participant à une grève sauf si ce membre du personnel a été désigné pour assurer les services minimaux décrits ci-dessus et manque à cette obligation pour participer à la grève» (article 1.4.7).

Dans la mesure où la participation à une grève entraîne automatiquement une déduction du salaire et des autres indemnités, le traitement des données personnelles liées à cette déduction fait l'objet d'un contrôle préalable par le CEPD. En effet, il s'agit d'un traitement qui exclut des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat.

Le 28 septembre 2010, le CEPD a émis un avis de contrôle préalable (dossier 2009-0514) concernant cette opération de traitement. Cet avis comporte des recommandations concernant la **période de conservation** de toute documentation stockée dans le système électronique de gestion des archives et des documents de la BCE et concernant les **informations** à fournir aux personnes concernées.

2.3.3.8. Enquête sur des cas de fraude - Banque européenne d'investissement

La Division Enquêtes sur les fraudes (IG/IN) de la Banque européenne d'investissement (BEI) enquête sur les allégations de pratiques interdites conformément aux procédures anti-fraude de la BEI. Pour mener ses enquêtes, l'IG/IN a accès à toutes les informations, toutes les données et tous les documents pertinents concernant le personnel, y compris les données électroniques de la BEI. Aucune interception de communications ou de conversations n'est par contre autorisée. Le chef de la division IG/IN détermine si une plainte ou allégation est fondée et renvoie le dossier aux autorités compétentes au sein de la BEI ou en dehors de celle-ci afin que soient prises les mesures adéquates. Si, à l'issue d'une enquête raisonnable, l'IG/IN

La division Enquêtes sur les fraudes de la BEI (IG/IN) enquête sur les allégations de pratiques interdites.

détermine qu'une plainte ou allégation n'est pas fondée, elle documente ses résultats dans une note au dossier et clôt ce dossier.

Le CEPD a rendu un avis de contrôle préalable (dossier 2009-0459) concernant les opérations de traitement de données liées à ces enquêtes pour fraude et recommandé que la BEI examine la **base légale** de ces enquêtes, qu'elle adopte un **protocole formel pour la réalisation des enquêtes scientifiques informatiques**, qu'elle harmonise les périodes de conservation et qu'elle communique des informations aux personnes concernées.

2.3.3.9. Analyse empirique des corrélations entre les variables du système de travail et le processus décisionnel - Office de l'harmonisation dans le marché intérieur

Ce contrôle préalable (dossier 2010-0468) couvrait les aspects de protection des données d'un exercice entrepris par l'Office de l'harmonisation dans le marché intérieur (OHMI) et intitulé «Analyse empirique des corrélations entre les variables du système de travail et le processus décisionnel». L'objectif de cette analyse était de contribuer à identifier des profils de fonction comparables et de développer de bonnes pratiques de gestion des ressources humaines pour ces profils. Outre les avantages pratiques qu'il apporte à l'OHMI, le projet poursuit aussi d'autres finalités scientifiques, dans la mesure où l'analyste projette de publier les résultats de ses recherches dans une thèse de doctorat (après les avoir soigneusement expurgés afin de protéger la vie privée des participants à cette opération). Le CEPD a émis un certain nombre de recommandations concernant notamment la conservation des données, les transferts à des tiers et l'information des personnes concernées.

Le CEPD a recommandé de supprimer toutes les données à caractère personnel des serveurs de l'OHMI à la fin de la période de conservation (2011). Le CEPD a également recommandé à l'analyste de respecter le droit national applicable concernant les micro-données conservées en vue de recherches futures éventuelles ou transférées à des parties tierces afin de respecter les obligations en matière de nécessité, de finalité et de confidentialité.

2.3.3.10. Base de données centrale des exclusions - Commission européenne

Afin de protéger les intérêts financiers des institutions et sur la base du règlement financier, la Commission européenne traite les données figurant dans une base de données centrale des exclusions. Ces données peuvent servir uniquement à exclure de toute procédure de passation de marché ou de demande de subvention au titre des fonds de l'UE ou des Fonds européen de développement les entités susceptibles de porter atteinte aux intérêts financiers européens.

Le CEPD a effectué son analyse (dossier 2009-0681) en étroite collaboration avec l'institution dès les premières phases.

Selon les conclusions du CEPD, rien n'indique qu'il y ait eu violation des dispositions du règlement relatif à la protection des données. Il a par contre fait un certain nombre de recommandations concernant l'information préalable des candidats, des soumissionnaires et des candidats aux subventions à fournir lors de l'appel à propositions et de l'appel d'offres.

2.3.3.11. Opérations de retour conjointes - FRONTEX

Le 26 avril 2010, le CEPD a adopté un avis (dossier 2009-0281) sur le traitement de données à caractère personnel par FRONTEX concernant la «Collecte de noms et de certaines données pertinentes des rapatriés pour des opérations de retour conjointes (ORC)». Ce traitement doit servir à la préparation et à la réalisation d'ORC avec l'aide de FRONTEX. Il s'agit de fournir aux compagnies aériennes une liste de passagers, de connaître, entre autres, le nombre de rapatriés, leur identité et les risques liés aux rapatriés, mais aussi d'assurer une assistance médicale adéquate au cours de l'ORC afin de garantir la sécurité de celle-ci et la bonne santé des personnes rapatriées.

FRONTEX a informé le CEPD que les données personnelles n'avaient pas été traitées pour des activités opérationnelles jusqu'à présent, mais que cela deviendrait nécessaire dans un avenir proche pour 1) mieux accomplir et continuer de développer la mission de l'Agence dans le contexte des ORC, 2) aider un État membre organisateur ou un pays associé à Schengen à dresser des listes de passagers et à les mettre à jour, 3) avoir en permanence une vue d'ensemble des États membres participants ou des pays associés à Schengen ayant (ou n'ayant pas) fourni les données requises au pays organisateur et 4) renforcer l'efficacité et l'efficience de l'assistance FRONTEX dans l'organisation de l'ORC.

Le CEPD a accordé une attention particulière à la base juridique du traitement. Le CEPD a admis qu'un traitement de données à caractère personnel pouvait être nécessaire à l'accomplissement de la mission de l'Agence dans le contexte de l'ORC. L'Agence doit être considérée comme le responsable de ce traitement. Cependant, en raison de la sensibilité des données et des activités concernées par rapport à une population vulnérable, le CEPD a considéré que l'article 9 du règlement FRONTEX (Coopération en matière de retour) et l'article 5(a) du règlement sur la protection des données ne pouvaient servir que de base juridique provisoire à l'activité de traitement, qui devrait faire l'objet d'une révision attentive et qui nécessiterait une base juridique spécifique.

Le CEPD a également demandé à ce que **FRONTEX mette en œuvre les procédures nécessaires pour garantir les droits des personnes concernées** et imposer **l'obligation d'informer** avant l'activité de traitement.

2.3.4. Consultations concernant la nécessité d'un contrôle préalable

La simple présence éventuelle de **données sensibles** ne signifie pas automatiquement qu'un contrôle préalable est nécessaire. Toutefois, le traitement de données sensibles couvrant par exemple des données relatives à la santé ou à des infractions civiles ou pénales nécessite d'accorder une attention particulière à l'adoption de mesures de sécurité appropriées, conformément à l'article 22 du règlement.

En cas de doute, les institutions et les organes de l'UE peuvent consulter le CEPD quant à la nécessité d'un contrôle préalable. En 2010, le CEPD a reçu six consultations de ce type de la part de DPD.

Parmi les dossiers examinés par le CEPD, on peut citer les procédures de sélection du personnel aux postes élevés, les listes de présence des membres d'associations participant à des événements auprès d'une institution, les activités de traitement d'un comité du personnel et une politique de formation du personnel.

2.3.5. Notifications non soumises au contrôle préalable ou retirées

À l'issue d'une analyse minutieuse, il a été conclu que huit dossiers ne devaient pas faire l'objet d'un contrôle préalable en 2010. Dans ces situations (appelées aussi «contrôles non préalables»), le CEPD peut malgré tout faire des recommandations. Par ailleurs, trois notifications ont été retirées et une notification a été remplacée.

Dans un dossier concernant la formation (dossier 2010-0638), les informations supplémentaires reçues de l'Autorité européenne de sécurité des aliments (EFSA) dans le contexte de la notification ont clarifié que les données recueillies étaient principalement de nature statistique et étaient uniquement destinées à l'assurance-qualité de la politique de formation de l'EFSA. Même si ces données peuvent inclure des évaluations de formateurs, le rapport produit n'est pas destiné à l'évaluation des formateurs à titre individuel. Sur la base de ces informations, le CEPD a conclu que cette notification n'était pas soumise à un contrôle préalable.

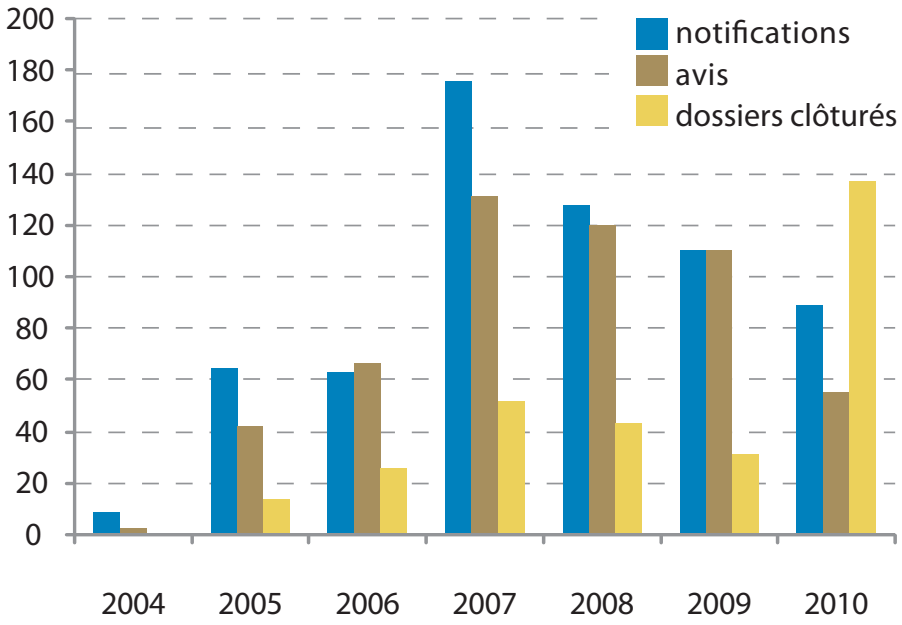
2.3.6. Suivi des avis relatifs aux contrôles préalables

*Un avis du CEPD relatif à un contrôle préalable conclut généralement que l'opération de traitement n'enfreint pas le règlement pour autant que certaines **recommandations** soient mises en œuvre. Des recommandations sont également formulées lorsque le CEPD examine un dossier afin de décider de la nécessité d'un contrôle préalable et lorsque certains aspects essentiels semblent nécessiter des rectifications. Si le responsable du traitement ne respecte pas ces recommandations, le CEPD peut exercer les pouvoirs qui lui sont conférés en vertu de l'article 47 du règlement (CE) n° 45/2001.*

Les institutions et organes ont suivi volontairement les recommandations du CEPD et, à ce jour, il n'a pas été nécessaire de prendre des décisions d'exécution. Dans la lettre formelle transmise avec son avis, le CEPD demande que l'institution ou l'organe concerné l'informe, dans un délai de trois mois, des mesures adoptées pour mettre en œuvre les recommandations.

Le CEPD considère ce suivi comme un **élément fondamental du respect intégral** du règlement. Conformément à son document de politique récent intitulé «Contrôler et garantir le respect du règlement (CE) n° 45/2001», le CEPD attend des institutions et des organes qu'ils se montrent **responsables** des recommandations éventuellement

Situation comparative



formulées. Cela signifie qu'ils sont chargés de les mettre en œuvre, et qu'ils doivent pouvoir en apporter la preuve au CEPD. Toute institution ou tout organe qui ne donne pas suite à ces recommandations s'expose donc à une mesure formelle d'exécution.

2.3.7. Conclusions

Les 55 avis formulés par le CEPD ont jeté une lumière précieuse sur les opérations de traitement des administrations européennes, et ont permis au CEPD de renforcer son expertise et de fournir des orientations génériques dans certains domaines, par exemple en matière de procédures administratives communes. Cela apparaît clairement dans les traitements liés aux enquêtes administratives et aux procédures disciplinaires (voir la section 2.7 «Lignes directrices thématiques»). Le CEPD continuera de fournir ces orientations aux institutions et agences, et il continuera de faciliter le processus de notification des agences.

Comme la plupart des institutions sont arrivées à la fin de la notification de leurs opérations de traitement existantes dans les procédures administratives standard, le CEPD a reçu de nombreuses notifications en 2010 concernant les activités principales propres à certaines institutions ou agences.

Le CEPD a atteint une étape importante dans le suivi de ses avis relatifs au contrôle préalable, dans la mesure où 137 dossiers ont été clos en 2010. Le CEPD continuera de contrôler de près le travail de suivi afin de faire en sorte que les institutions et agences intègrent les recommandations formulées par le CEPD en temps utile et de façon satisfaisante.

2.4. Réclamations

2.4.1. Les fonctions du CEPD

L'une des fonctions principales du CEPD est établie par l'article 46 du règlement (CE) n° 45/2001: le CEPD «entend et examine les réclamations» et «effectue des enquêtes, soit de sa propre initiative, soit sur la base d'une réclamation».

En principe, une personne ne peut présenter une réclamation que pour une violation présumée de ses droits en matière de protection des données à caractère personnel. Seul le personnel de l'UE peut se plaindre d'une violation présumée des règles en matière de protection des données, que le plaignant soit directement touché par le

Toute personne peut se plaindre auprès du CEPD concernant le traitement de données à caractère personnel par l'administration de l'UE.

traitement ou pas. Le statut des fonctionnaires de l'Union européenne permet également de soumettre une réclamation au CEPD (article 90 ter).

Le règlement prévoit que le CEPD peut uniquement traiter des réclamations soumises par des personnes physiques. Les réclamations soumises par des entreprises ou des personnes morales ne sont pas recevables.

Les plaignants doivent également s'identifier et les requêtes anonymes ne sont donc pas considérées comme des «réclamations». Toutefois, les informations anonymes peuvent être prises en considération dans le cadre d'une autre procédure (enquête d'initiative ou demande de notification d'une opération de traitement de données, etc.).

***Une réclamation devant le CEPD ne peut porter que sur le traitement de données à caractère personnel**. Le CEPD n'est pas compétent pour traiter les cas de mauvaise administration, pour modifier le contenu des documents que le plaignant souhaite contester ou pour octroyer des dommages et intérêts.*

*Le traitement de données à caractère personnel faisant l'objet d'une réclamation doit être effectué par l'**un des organes ou institutions de l'UE**. En outre, le CEPD n'est pas une instance de recours pour les décisions prises par les autorités nationales chargées de la protection des données.*

Un membre du personnel de la Commission européenne a contesté le contenu du rapport d'évaluation préparé par sa hiérarchie. Il a demandé au CEPD d'ordonner à la Commission de rectifier ce rapport, puisque celui-ci contient ses données personnelles. Le CEPD n'a pas suivi le raisonnement du plaignant. En fait, même si les données d'évaluation sont des données personnelles, il y a par définition des évaluations subjectives qui ne peuvent être rectifiées automatiquement sur la base des règles existant en matière de protection des données. Une procédure spécifique de contestation des rapports d'évaluation devrait être suivie pour contester l'inclusion de ces données.

2.4.2. Procédure de traitement des réclamations

Le CEPD examine les réclamations en vertu du cadre juridique en vigueur, des principes généraux du droit européen et des bonnes pratiques administratives communes aux institutions et organes de l'UE. En décembre 2009, le CEPD a adopté un manuel interne dont le but est de mettre des orientations en matière de traitement des réclamations à la disposition de son personnel. Le CEPD a également mis en place un outil statistique conçu pour examiner les activités liées aux réclamations, et en particulier pour suivre l'évolution de certains dossiers.

À tous les stades du traitement de la réclamation, le CEPD respecte les principes de proportionnalité et d'équité. Guidé par les principes de transparence et de non-discrimination, il prend les mesures appropriées en tenant compte:

- de la nature et de la gravité de la violation alléguée des règles régissant la protection des données;
- de l'importance du préjudice qu'une ou plusieurs personnes peuvent avoir subi du fait de la violation;
- de l'importance potentielle de l'affaire, en tenant compte des autres intérêts publics et/ou privés en cause;
- de la probabilité d'établir l'existence de la violation;
- de la date exacte des événements en cause, de tout comportement ne produisant plus d'effets, de l'élimination de ces effets ou d'une garantie satisfaisante quant à l'élimination de ces effets.

Le CEPD examine attentivement chaque réclamation qu'il reçoit. L'examen préliminaire est spécifiquement destiné à vérifier si la réclamation remplit les conditions d'ouverture d'une enquête et s'il existe des éléments suffisants pour justifier l'ouverture d'une enquête.

Une réclamation pour laquelle le CEPD **n'a pas de compétence juridique** sera déclarée irrecevable et le plaignant en sera informé. Dans de tels cas, le CEPD peut conseiller au plaignant de s'adresser à une autre autorité compétente (par ex. tribunal, Médiateur, autorités nationales de protection des données, etc.).

Une réclamation portant sur des faits **manifestement insignifiants** ou des questions dont l'examen nécessiterait des **efforts disproportionnés** ne fera pas l'objet d'une enquête complémentaire. Le CEPD ne peut examiner que les réclamations qui concernent une violation **réelle ou potentielle**, et pas simplement hypothétique, des règles régissant le traitement des données à caractère personnel. Il s'agit notamment d'analyser quelles sont les autres options disponibles pour traiter la question, que ce soit pour le plaignant ou le CEPD. Celui-ci peut par exemple ouvrir une enquête sur un problème général de sa propre initiative en plus d'ouvrir une enquête sur un dossier individuel soumis par le plaignant. Dans ce cas, le plaignant est informé de tous les moyens d'action disponibles.

Une personne a demandé au CEPD si elle pouvait accéder aux données à caractère personnel des autres candidats dans une procédure de recrutement, ou si cet accès pouvait lui être refusé pour des raisons de protection des données. Le CEPD n'a pas pris position, puisque cette question était encore hypothétique. En effet, l'organe de l'Union concerné n'avait pas encore refusé l'accès aux informations requises et n'avait donc pas encore invoqué la protection des données pour motiver son refus.

La réclamation est en principe **irrecevable** si le plaignant **n'a pas d'abord contacté l'institution concernée** pour qu'elle remédie à la situation. Si le plaignant n'a pas contacté l'institution, il doit fournir au CEPD des raisons suffisantes pour expliquer cette inaction.

Si la question est déjà examinée par des organes administratifs, par exemple si une enquête interne par l'institution concernée est en cours, la réclamation est en principe irrecevable. Toutefois, le CEPD peut décider, sur la base des éléments particuliers du dossier, d'attendre l'issue de ces procédures administratives avant de commencer son enquête. À l'inverse, si la même question (ou les mêmes circonstances factuelles) fait déjà l'objet d'un examen par un tribunal, la réclamation est déclarée irrecevable.

Pour assurer le traitement cohérent des réclamations concernant la protection des données et éviter toute redondance inutile, le **Médiateur européen** et le CEPD ont signé un mémorandum d'accord en novembre 2006 qui stipule entre autres qu'une réclamation qui a déjà été examinée ne peut être ouverte une seconde fois par l'autre institution, sauf si des éléments nouveaux importants sont apportés.

En ce qui concerne les **délais**, si les faits sont communiqués au CEPD après plus de deux ans, la réclamation est en principe irrecevable. La période de deux ans commence le jour où le plaignant a pris connaissance des faits.

Si la réclamation est recevable, le CEPD lance une **enquête**. Cette enquête comprend une demande d'information à l'institution concernée, une révision des documents concernés, une rencontre avec le responsable du traitement, une inspection sur place, etc. Le CEPD a le pouvoir d'obtenir l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires pour l'enquête de la part de l'institution ou de l'organe concerné. Il peut également avoir accès à tous les locaux dans lesquels un responsable du traitement, une institution ou un organe exerce ses activités.

À la fin de l'enquête, il envoie sa **décision** au plaignant ainsi qu'au responsable du traitement des données. Dans cette décision, il exprime son avis concernant toute violation des règles régissant la protection des données par l'institution concernée. Le CEPD **dispose de vastes pouvoirs**, allant du simple conseil aux personnes concernées à l'interdiction du traitement ou la saisine de la Cour de justice européenne, en passant par un avertissement ou une admonestation au responsable du traitement.

Toute partie intéressée peut demander au CEPD de **revoir** sa décision dans un délai d'un mois à compter de la date d'adoption de cette décision. Les parties concernées peuvent également introduire un recours direct auprès de la Cour de justice.

À deux reprises en 2009, les plaignants ont contesté les décisions du CEPD auprès du Tribunal (affaires T-164/09 et T193/09). Dans la première affaire, le Tribunal a estimé qu'il n'y avait plus lieu de statuer sur l'action du CEPD parce que le recours était devenu sans objet. Dans la deuxième affaire, la demande d'aide judiciaire introduite par le plaignant a été rejetée par le Tribunal. Celui-ci n'a pas examiné l'affaire au fond.

2.4.3. Confidentialité garantie aux plaignants

*Le CEPD reconnaît que certains plaignants prennent des risques pour leur carrière en dévoilant des violations des règles de protection des données et que la **confidentialité** doit donc être assurée aux plaignants et informateurs qui le demandent. D'autre part, le CEPD s'est engagé à travailler **de manière transparente** et à publier au moins le fond de ses décisions. Les procédures internes du CEPD reflètent ce difficile équilibre.*

Généralement, les réclamations sont traitées de manière confidentielle. Le **traitement confidentiel** signifie que les informations personnelles ne sont pas divulguées à des personnes extérieures au CEPD. Toutefois, pour le déroulement correct de l'enquête, il pourrait s'avérer nécessaire d'informer les services de l'institution concernée et les tierces parties impliquées du contenu et de l'identité du plaignant. Le CEPD envoie également une copie de sa correspondance avec l'institution au délégué à la protection des données (DPD) de ladite institution.

Si le plaignant exige l'**anonymat** envers l'institution, le DPD ou les tierces personnes concernées, il est invité à en expliquer les raisons. Le CEPD analyse ensuite ses arguments et examine les conséquences pour la viabilité de son enquête future. S'il décide de ne pas accepter l'anonymat du plaignant, il explique pourquoi et demande au plaignant s'il accepte que le CEPD examine la réclamation sans garantir l'anonymat ou s'il préfère retirer sa réclamation, auquel cas l'institution concernée ne sera pas informée de son existence. Dans ce cas, le CEPD peut entreprendre d'autres actions en la matière, sans révéler à l'institution concernée l'existence de la réclamation. Il s'agit alors d'une enquête d'initiative ou d'une demande de notification d'une opération de traitement des données.

À l'issue d'une enquête, tous les **documents relatifs à la réclamation**, y compris la décision finale, restent en principe confidentiels. Ils ne sont pas entièrement publiés ni transmis à des tiers. Toutefois, un résumé anonyme de la réclamation peut être publié par le CEPD sur son site internet et dans son rapport annuel sous une forme qui ne permet d'identifier ni le plaignant, ni les tiers. Le CEPD peut également décider de publier la décision finale *in extenso* s'il s'agit de dossiers importants. Il doit alors prendre en considération la demande de confidentialité du plaignant et ne permet donc pas d'identifier le plaignant ou les autres personnes concernées.

2.4.4. Réclamations traitées en 2010

2.4.4.1. Nombre de réclamations

La complexité des réclamations reçues par le CEPD en 2010 a augmenté, tandis que leur nombre a diminué. ***En 2010, le CEPD a reçu 94 réclamations*** *(soit une baisse de 15 % par rapport à 2009).* ***Sur ce total, 69 ont été jugées irrecevables****, la majorité portant sur un traitement au niveau national, et pas au niveau d'une institution ou d'un organe de l'UE.*

Les 25 réclamations restantes ont nécessité une enquête approfondie (une baisse de 41 % par rapport à 2009). En outre, 18 réclamations recevables soumises les années précédentes (16 en 2009 et deux en 2008) en étaient toujours au stade de l'enquête ou de l'examen.

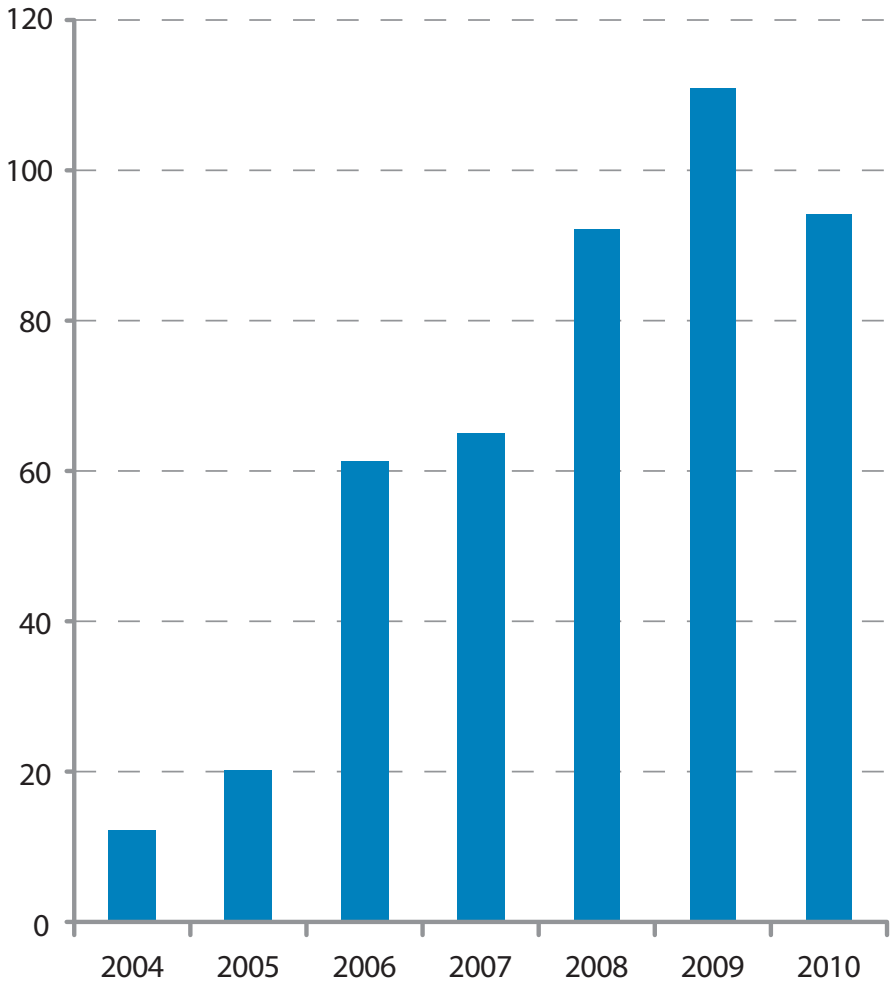
2.4.4.2. Nature des plaignants

Sur les 94 réclamations déposées, 17 (18 %) ont été soumises par des membres du personnel des institutions ou organes de l'UE, y compris des anciens membres et des candidats. En ce qui concerne les 77 autres réclamations, le plaignant ne semblait pas avoir de lien professionnel avec l'administration de l'UE.

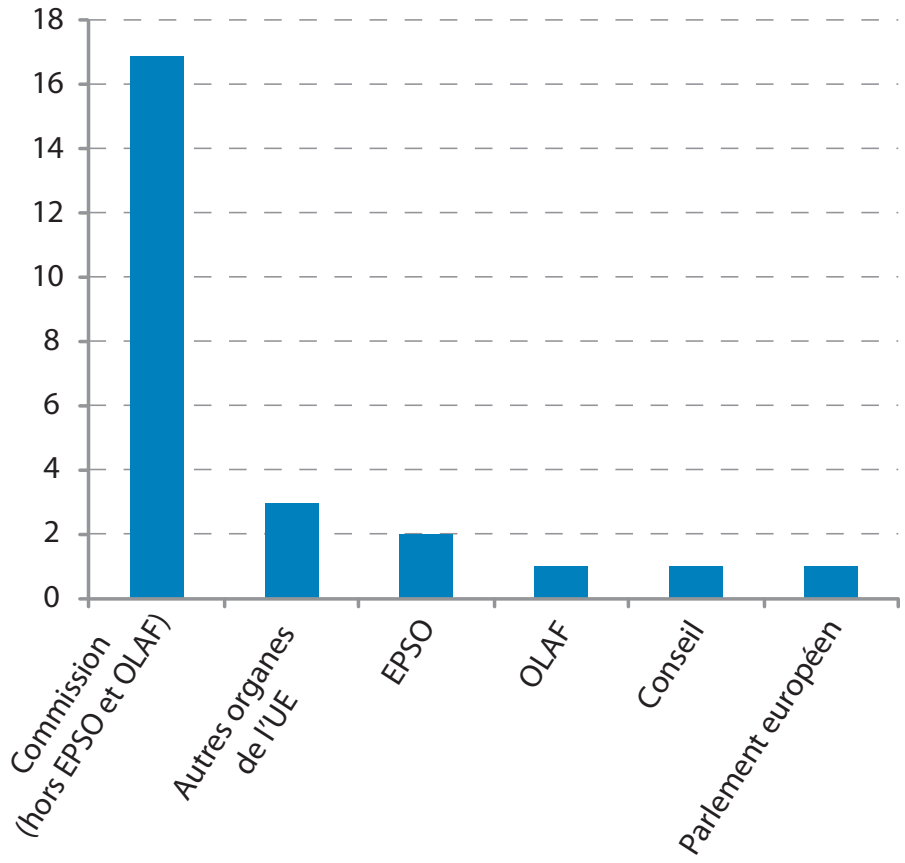
2.4.4.3. Institutions concernées par les réclamations

Sur l'ensemble des plaintes recevables reçues en 2010, la majorité (80 %) étaient dirigées contre la **Commission européenne, notamment l'OLAF et l'EPSO**. Cette situation est prévisible dans la mesure où la Commission traite plus de données à caractère personnel que les autres institutions et organes de l'UE. Le nombre relativement élevé de réclamations concernant l'OLAF et l'EPSO peut s'expliquer par la nature des activités exercées par ces organes.

Nombre des réclamations reçues (évolution 2004-2010)



Institutions et organes de l'Union concernés



2.4.4.4. Langue des réclamations

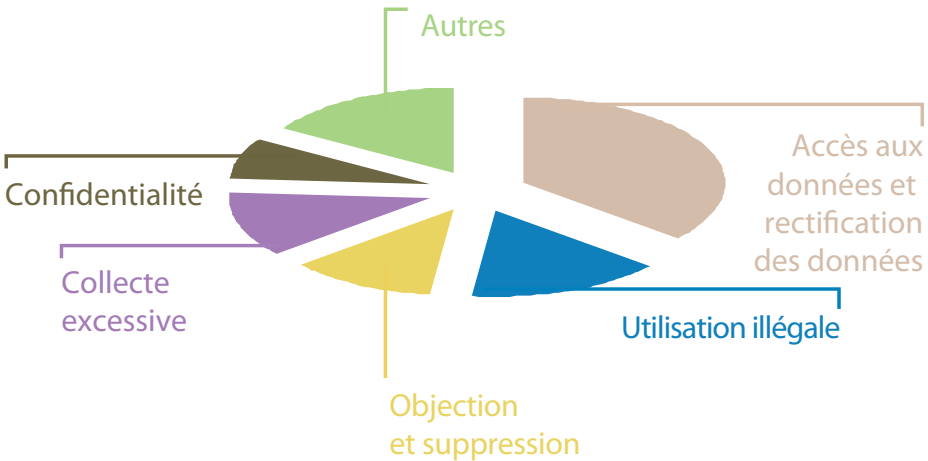
La majorité des réclamations étaient rédigées en anglais (44 %), l'allemand (33 %) et le français (15 %) étant moins souvent utilisés. Les réclamations dans d'autres langues sont relativement rares (8 %).

2.4.4.5. Types de violations invoqués

Les violations des règles en matière de protection des données alléguées par les plaignants en 2010 concernaient principalement:

- une atteinte aux droits des personnes concernées, comme les droits d'accès ou de rectification des données (36 %) ou le droit d'objection et de suppression (12 %);

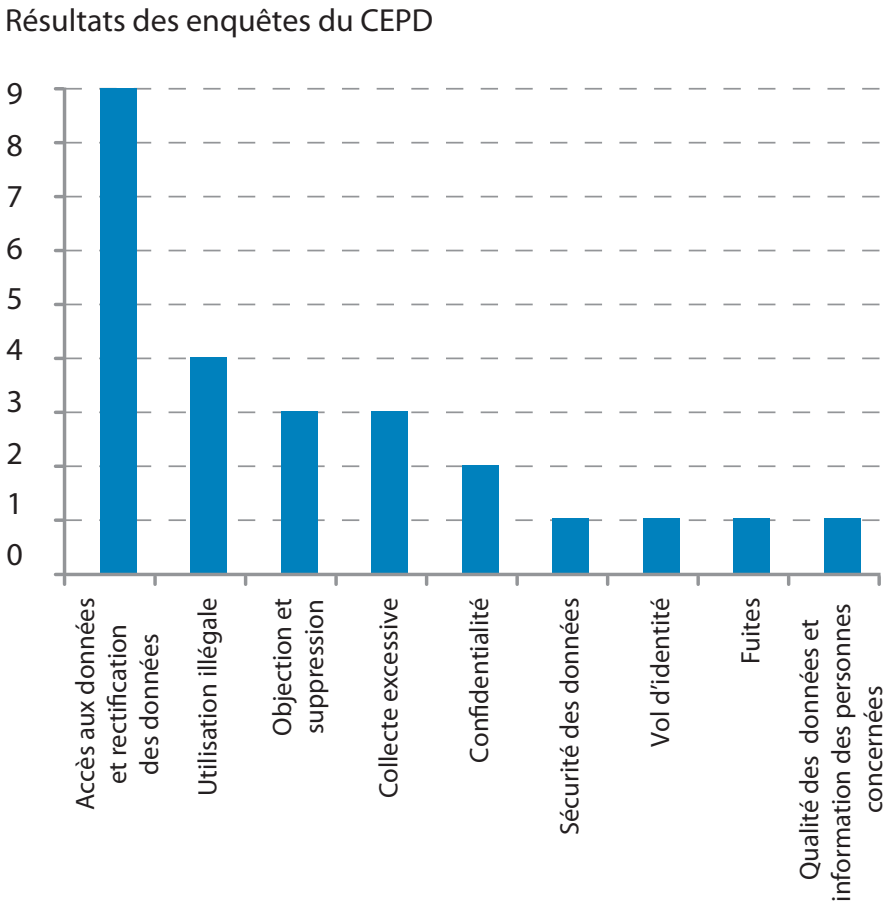
Types de violations invoqués



- l'utilisation illégale (16 %), la collecte excessive de données personnelles (12 %), la violation de la confidentialité (8 %).

D'autres violations moins souvent invoquées concernent la sécurité des données (4 %), le vol d'identité (4 %), les fuites (4 %), la qualité des données et l'information des personnes concernées (4 %).

2.4.4.6. Résultats des enquêtes du CEPD



Dans 11 dossiers résolus en 2010, le CEPD n'a constaté aucune violation des règles en matière de protection des données.

À l'inverse, dans 10 dossiers, le CEPD a constaté un non-respect des règles de protection des données et a soumis des recommandations au responsable du traitement des données.

Le CEPD a reçu une réclamation concernant l'accès aux fichiers médicaux détenus par le service médical d'une institution. Le CEPD a confirmé qu'en vertu des règles relatives à la protection des données, l'accès aux données personnelles n'impose pas au responsable du traitement d'envoyer le dossier médical original. Dans la pratique, cet accès suppose la possibilité de consulter ce dossier (en personne ou, dans certains cas, via un médecin) et/ou d'en faire des copies. En ce qui concerne le droit à la rectification des données inexactes ou incomplète, le CEPD a souligné que, dans le cas de données médicales, l'obligation de rectifier les données concerne uniquement les données factuelles et non les évaluations en matière de santé. Le responsable du traitement n'est donc pas tenu, en vertu des règles sur la protection des données, de modifier la conclusion d'un rapport médical donné. Dans ce contexte, le droit de rectifier les données pourrait entraîner la possibilité d'inclure un autre rapport produit par un autre professionnel de santé et présentant une évaluation différente. Dans ce cas précis, le CEPD a donc conclu qu'il n'y avait aucune violation des règles en matière de protection des données.

Le CEPD a reçu une réclamation portant sur la publication de données personnelles hautement sensibles au Journal officiel de l'Union européenne et dans le procès-verbal d'une séance au Parlement européen. Au terme de son enquête sur ce dossier, le CEPD a conclu que l'avis du député aurait pu être exprimé et que le message politique de la déclaration écrite aurait pu être transmis efficacement sans que soit révélée l'identité des personnes concernées. Le CEPD a demandé la suppression des noms des personnes citées par le député dans la déclaration écrite et dans tout autre format. Il a également demandé la mise en place d'une procédure formelle et efficace pour faire en sorte que les versions définitives des documents publiés au Journal officiel et sur le site internet du Parlement tiennent compte des modifications introduites par les services chargés de la préparation des documents.

Le CEPD a reçu une réclamation concernant la communication des numéros d'employé des membres du personnel d'une agence à tous les utilisateurs via les adresses électroniques internes de l'agence. L'objectif de ce traitement était d'inviter tous les membres du personnel à un rendez-vous avec le service de sécurité de l'agence pour se faire prendre en photo. Le CEPD a considéré qu'à cette fin, il aurait été amplement suffisant d'envoyer une liste contenant uniquement le nom et le prénom des personnes concernées. Le numéro d'employé figurant sur cette liste était inutile et excessif par rapport à cette finalité, et donc contraire à l'article 4 du règlement. Le CEPD a demandé à l'agence de donner une consigne formelle aux membres du personnel traitant des données personnelles de se montrer sélectifs et particulièrement attentifs quand ils envoient des courriers par l'internet ou externes contenant des données personnelles, et de n'y inclure que les données nécessaires à la finalité du message.

Un membre du personnel s'est plaint d'une vidéosurveillance cachée dans son institution. Il a notamment contesté la légalité de l'utilisation d'une caméra vidéo l'enregistrant à son insu lorsqu'il pénétrait dans le bureau de son supérieur en son absence. Le CEPD a conclu que l'institution n'avait pas démontré l'existence d'une base juridique autorisant explicitement des opérations aussi intrusives et prévoyant des conditions et des mesures de protection spécifiques. Sans une base juridique transparente de ce type et sans approche structurée, le caractère proportionnel de cette vidéosurveillance cachée était douteux. Le CEPD a donc invité l'institution à réexaminer son souhait de recourir à la vidéosurveillance à l'avenir et, le cas échéant, à soumettre ses projets au CEPD en vue d'un contrôle préalable.

2.4.5. Autres travaux dans le domaine des réclamations

Le CEPD compte faciliter le processus de dépôt des réclamations et accélérer le traitement des réclamations par les services du CEPD en créant un **formulaire en ligne de dépôt de plainte** sur le site internet du CEPD (voir section 5.6.1). Une version provisoire de ce formulaire est disponible sur le site internet du CEPD depuis début 2010. La version définitive sera plus interactive. Le CEPD s'attend à ce que la généralisation de l'utilisation de cette application aide les plaignants à évaluer la recevabilité de leur réclamation, et donc à ne soumettre au CEPD que des cas pertinents. En outre, le CEPD espère obtenir des informations plus complètes et pertinentes afin de traiter les réclamations plus efficacement et de réduire le nombre des réclamations manifestement irrecevables,

Le CEPD compte également réviser le manuel de procédure interne pour le traitement des plaintes adopté en 2009. Les procédures modifiées intégreraient la nouvelle structure organisationnelle du CEPD et clarifieraient le flux interne de traitement des réclamations.

2.5. Contrôle du respect du règlement

*Le CEPD est chargé d'assurer le suivi et de **veiller à l'application du règlement (CE) n° 45/2001**. Le contrôle a notamment pris la forme d'un **rapport** intitulé «printemps 2009». En plus de cet exercice général de contrôle, des contrôles ciblés ont également été effectués dans les cas où, à la suite des activités de supervision, le CEPD s'est inquiété du degré de conformité aux normes de certaines institutions ou certains organes. Certains de ces contrôles ont été réalisés par correspondance, tandis que d'autres ont pris la forme d'une **visite** d'une journée de l'organe concerné aux fins de remédier aux défauts de conformité. Enfin, des **inspections** ont été opérées dans certaines institutions et certains organes pour vérifier leur respect du règlement concernant des questions spécifiques.*

2.5.1. Exercices ciblés de contrôle et de compte rendu

Le CEPD a lancé des exercices ciblés de contrôle par correspondance dans des cas où il s'inquiétait d'un problème de conformité au règlement dans une institution ou une agence. Ce fut le cas par exemple à la BCE, en matière d'enquêtes administratives internes, ou dans les opérations de traitement de la DG RELEX.

Enquêtes administratives internes - Banque centrale européenne

En janvier 2010, le CEPD a ouvert une enquête sur la protection des données à caractère personnel dans le cadre des enquêtes administratives internes au sein de la Banque centrale européenne (BCE). Cette décision a été prise sur la base de l'article 46, point b), du règlement, à la suite de l'avis formulé le 22 décembre 2005 par le CEPD concernant ces enquêtes à la BCE. Cette enquête s'est concentrée sur l'accès éventuel aux fichiers électroniques et sur l'interception de conversations téléphoniques. Plusieurs questions ont été envoyées à la BCE concernant l'application de la circulaire administrative 01/2006 de la BCE relative aux enquêtes administratives internes et de ses principes. Ces questions portaient, entre autres, sur la façon dont cette procédure est documentée, sur l'existence ou non d'un protocole informatique scientifique et de statistiques annuelles concernant l'interception de conversations téléphoniques et l'accès aux fichiers électroniques et aux données du trafic. Cette enquête n'est pas encore terminée.

Inventaire de la DG RELEX

À la suite d'un certain nombre de réclamations, le CEPD s'est préoccupé du fait que l'inventaire des opérations de traitement sous le contrôle de la DG RELEX ne reflétait pas correctement les opérations de traitement impliquant des données à caractère personnel au sein des délégations de l'Union européenne. Le CEPD a également souhaité vérifier que DG RELEX avait bien notifié toutes les opérations de traitement des délégations de l'Union au DPD de la Commission conformément à l'article 25. La DG RELEX a communiqué des mises à jour et a fourni des garanties adéquates sur ces deux points, et le dossier a été clos.

Visite de l'Agence européenne chargée de la sécurité des réseaux et de l'information

Le 17 septembre 2010, le CEPD a visité l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) afin de vérifier le degré peu élevé de conformité avec le règlement (CE) n° 45/2001 et d'en discuter. Cette visite a été provoquée par des données recueillies au cours des activités de supervision du CEPD, sous la forme d'une réclamation, d'une consultation et de l'absence de suivi après un avis de contrôle préalable.

Cette visite a également permis au DPD d'informer le CEPD des progrès d'ENISA, parmi lesquels un registre électronique, un mécanisme de suivi et un nouvel inventaire. Le DPD a mis en évidence des problèmes d'indépendance dans l'exercice de ses activités de DPD, et le Contrôleur adjoint a évoqué le document relatif aux normes professionnelles à l'intention des DPD (adopté par la suite en octobre 2010), qui devrait aider le DPD à renforcer et à clarifier son rôle en interne.

Lors de la réunion de clôture, et sur la base des exigences du CEPD, une feuille de route de supervision (incluant des échéances spécifiques) a été mise au point par les deux parties, qui ont souligné l'importance des trois outils majeurs de conformité au règlement: l'inventaire, le registre et les notifications au CEPD en vertu de l'article 27. Le CEPD sui-

vra de près les progrès accomplis par la suite par l'ENISA afin de garantir le respect du règlement.

Visite de l'Agence européenne pour l'environnement

Le 10 décembre 2010, le CEPD a visité l'Agence européenne pour l'environnement (AEE) afin de vérifier et de discuter du degré de conformité au règlement de l'Agence.

Cette visite a consisté en une réunion entre le CEPD et le directeur de l'AEE, avec d'autres réunions impliquant le DPD et le responsable des opérations de traitement. Ces réunions ont donné au CEPD l'occasion d'exprimer ses préoccupations concernant le degré actuel de conformité de l'AEE, et elles ont permis à l'Agence de l'informer de ses progrès vers la pleine conformité. Dans ce contexte, le CEPD s'est réjoui de constater les efforts importants consentis récemment par l'Agence et l'engagement qu'elle a pris de combler ses lacunes.

Les deux parties se sont mises d'accord sur une feuille de route de conformité (avec des échéances spécifiques) qui sera suivie de près par le CEPD.

2.5.2. Exercice général de contrôle et de compte rendu: l'exercice «printemps 2009»

À la suite de l'exercice général de contrôle lancé au printemps 2009, le CEPD a continué de contrôler la mise en œuvre des règles et principes de protection des données par les institutions et organes concernés.

Les **institutions de l'UE** ont continué de faire des **progrès importants** en matière de réponse aux exigences de protection des données. Les **agences** présentent généralement un **degré de conformité moindre**.

Dans les cas où le CEPD a jugé les progrès en matière de conformité insuffisants, des objectifs adéquats ont été fixés. Malheureusement, ces objectifs n'ont pas toujours été atteints. Dans ces cas, le CEPD a demandé des mises à jour supplémentaires. Là où ces mises à jour n'ont pas été fournies ou lorsque les progrès accomplis étaient trop lents, le CEPD a lancé des exercices de contrôle plus ciblés (voir ci-dessus).

Mises à jour relatives à l'exercice «printemps 2009»

- **Notification des opérations de traitement aux DPD par les responsables du traitement**: globalement, le niveau des notifications a augmenté. Le CEPD continue de demander des mises à jour concernant les progrès accomplis, mais il va aussi se pencher sur le problème des institutions et des organes qui respectent mal le règlement, conformément à son document stratégique sur le contrôle et la garantie du respect des règles.

- **Notification des opérations de traitement au CEPD à des fins de contrôle préalable**: la plupart des institutions ont fait des progrès importants dans ce domaine, même si, une fois de plus, les degrés de conformité restent inférieurs pour les agences. Le CEPD va s'efforcer de résoudre ce problème au cours de l'année à venir.

2.5.3. Prochaines étapes

Le CEPD encouragera et suivra de près les évolutions futures, en particulier dans les institutions et les agences qui devaient améliorer leur respect du règlement dans le domaine du contrôle préalable par le CEPD et des notifications au DPD. Il continuera également de souligner l'utilité d'un **inventaire** et d'une **procédure interne de suivi de ses recommandations** pour assurer le respect du règlement.

Le prochain exercice général de contrôle (**printemps 2011**) commencera au début de l'année 2011. Du fait des données déjà recueillies lors des exercices précédents, des initiatives ciblées supplémentaires en matière de respect des règles vont probablement continuer également.

2.5.4. Inspections

Les inspections constituent un outil indispensable pour que le CEPD puisse surveiller et assurer l'application des dispositions du règlement, et elles se basent sur ses articles 41, paragraphe 2, 46, point c), et 47, paragraphe 2.

Les pouvoirs étendus qui sont conférés au CEPD lui permettant d'accéder à toutes les informations et données à caractère personnel nécessaires à ses enquêtes et d'obtenir l'accès à tous les locaux dans lesquels le responsable du traitement ou une institution ou un organe exerce ses activités ont pour objet de lui permettre de disposer de moyens efficaces pour s'acquitter de ses fonctions.
Les inspections peuvent résulter d'une réclamation ou être effectuées de la propre initiative du CEPD.

L'article 30 du règlement prévoit que les institutions et organes de l'UE sont tenus de coopérer avec le CEPD dans l'accomplissement de ses fonctions et doivent lui communiquer les informations demandées et lui accorder l'accès requis.

Au cours des inspections, le CEPD vérifie les faits sur place, son objectif étant également d'assurer le respect du règlement. Les inspections sont suivies d'un retour d'informations adéquat à l'institution ou à l'organe qui fait l'objet de l'inspection.

En 2010, le CEPD a procédé au suivi des inspections antérieures. En décembre 2010, il a par ailleurs opéré une inspection au Centre commun de recherche de la Commission, à Ispra.

Les inspections sont un outil fondamental pour contrôler et garantir l'application du règlement relatif à la protection des données.

Suivi de l'inspection à l'Office européen de sélection du personnel

En mars 2009, le CEPD a effectué une inspection à l'Office européen de sélection du personnel (EPSO). Cette inspection visait à établir les faits concernant plusieurs opérations de traitement de données à caractère personnel soumises à des contrôles préalables dans le domaine de la sélection des fonctionnaires, agents temporaires et agents contractuels, ainsi que toute opération connexe de traitement des données à caractère personnel. Le CEPD a formulé un certain nombre de conclusions, concernant notamment la transparence des procédures de l'EPSO et la conservation des données. Ces conclusions ont été prises en considération par l'EPSO.

L'inspection visait également à garantir la conformité de certaines bases de données et de **certains outils informatiques de l'EPSO** utilisés dans les procédures de sélection. Le CEPD attend encore un retour supplémentaire concernant les progrès accomplis dans le plan de mise en œuvre de ses recommandations. Le CEPD a donc réservé ses conclusions finales concernant l'inspection en attendant de recevoir ces informations.

Suivi de l'inspection à la Cour des comptes européenne

Après l'inspection opérée en mars 2009 par le CEPD à la Cour des comptes européenne en relation avec le **personnel de contrôle** (contrôle de l'internet et rapport d'audit), la collaboration avec la Cour a été fructueuse et le CEPD a constaté des progrès de la conformité dans les domaines examinés.

Dans le **dossier relatif au contrôle de l'internet** (dossier 2008-0284), le CEPD a formulé des recommandations spécifiques dans son rapport relatif au suivi de l'avis adopté. D'autres discussions sont encore en cours en vue de garantir une conformité intégrale dans le cadre général de l'analyse de cette question dans le contexte institutionnel.

En ce qui concerne la consultation relative à une procédure d'accès aux supports informatiques et aux courriels privés des membres du personnel, le CEPD a conclu qu'une notification formelle en vue d'un contrôle préalable devait lui être soumise concernant ce traitement, qui présente un risque spécifique au titre de l'article 27, paragraphe 1, du règlement. En janvier 2010, le CEPD a rendu son avis (dossier 2009-0620) autorisant les opérations de traitement moyennant le respect de certaines recommandations, qui ont par la suite été mises en œuvre par la Cour des comptes européenne. Le CEPD a donc clos ce dossier.

Suivi de l'inspection de s-TESTA

Le réseau s-TESTA (services télématiques transeuropéens sécurisés entre administrations) fournit une infrastructure générale pour répondre aux besoins en matière de gestion des affaires et d'échanges d'informations entre les administrations européennes et nationales. Actuellement, plus de 30 applications se basent sur ce réseau sécurisé fourni par la Commission européenne.

En janvier 2010, le CEPD a adopté un rapport contenant 22 recommandations relatives à l'inspection opérée précédemment au Centre de service et d'opération (CSO) de s-TESTA. En décembre 2010, la Commission a envoyé au CEPD un rapport de mise en œuvre concernant ces recommandations, indiquant que 12 d'entre elles avaient déjà été mises en œuvre. Les 10 autres, qui nécessitaient des investissements plus importants, ont été reprises dans le plan d'amélioration continue du système et seront finalisées en 2011. Le CEPD vérifiera ces éléments restants au cours d'une action de suivi prévue pour le milieu de l'année 2011.

Inspection au Centre commun de recherche

En décembre 2010, le CEPD a procédé à une inspection sur place au Centre commun de recherche de la Commission, à Ispra. Le manque de coopération généralisé du CCR, associé à la nécessité de contrôler et de vérifier la mise en œuvre de ses recommandations *in situ*, a suscité la décision de procéder à cette inspection.

L'inspection a porté sur deux domaines principaux: la sélection et le recrutement du personnel du CCR, et les procédures mises en place par le service de sécurité (contrôle de sécurité préalable à l'emploi, enquêtes de sécurité, contrôle d'accès et enregistrement des appels d'urgence). Dans tous ces dossiers, des informations de contexte ont été fournies par des analyses de contrôles préalables.

Au cours de l'inspection, la collaboration entre le CEPD et les unités concernées du CCR a été fructueuse et a permis aux inspecteurs de conclure, entre autres, que le manque de coopération antérieur était dû principalement à des problèmes de communication. Sur la base de ces résultats, le CEPD va publier un rapport d'inspection contenant de nouvelles recommandations afin d'assurer un meilleur respect du règlement.

2.6 Consultations relatives aux mesures administratives

2.6.1. Consultations selon l'article 28, paragraphe 1, et l'article 46, point d)

*L'article 28, paragraphe 1, du règlement (CE) n° 45/2001 confère au CEPD le droit d'être informé des mesures administratives relatives au traitement des données à caractère personnel. Le CEPD peut rendre un avis soit à la **demande** de l'institution ou de l'organe concerné, soit de sa **propre initiative**.*

Une «mesure administrative» doit s'entendre comme une décision de l'administration d'application générale qui se rapporte au traitement de données à caractère personnel effectué par l'institution ou l'organe concerné (par ex. modalités d'application du règlement, règles internes ou orientations d'application générale, décisions adoptées par l'administration dans le cadre du traitement de données à caractère personnel).

Par ailleurs, l'article 46, point d), du règlement prévoit un champ d'application matériel très large pour les consultations, en ce sens qu'il les étend à «toutes les questions concernant le traitement de données à caractère personnel». C'est la base sur laquelle le CEPD s'appuie pour conseiller les institutions et organes sur des dossiers particuliers supposant des traitements ou sur des questions théoriques relatives à l'interprétation du règlement.

Dans le cadre des consultations menées sur des mesures administratives envisagées par une institution ou un organe, plusieurs questions ont été examinées. Les sous-chapitres suivants rendent compte de certains de ces dossiers.

2.6.2. Demande d'accès à l'identité d'un informateur - Médiateur européen

Le Médiateur européen a consulté le CEPD à propos d'une question évoquée dans le cadre d'une plainte introduite à l'encontre de l'OLAF. Cette consultation portait sur un certain nombre de questions, demandant notamment:

- si l'identité des personnes qui fournissent des informations à l'OLAF, tels que les informateurs ou les dénonciateurs, ne doit être divulguée à personne, exception faite des autorités judiciaires;
- si la protection des informateurs et des dénonciateurs doit également être garantie après la clôture d'une enquête ne donnant lieu à aucun suivi et, dans l'affirmative, de quelle manière et dans quelle mesure.

Le CEPD a fait des commentaires au niveau des règles et des politiques plutôt que vis-à-vis des plaintes spécifiques à l'encontre de l'OLAF. Le CEPD a considéré que l'identité d'un dénonciateur ou d'un informateur ne doit en général pas être divulguée, sauf dans les cas où cette confidentialité irait à l'encontre des règles nationales régissant les procédures judiciaires, ou lorsque le dénonciateur fait une fausse déclaration par malveillance. Dans de tels cas, ces données à caractère personnel ne doivent être divulguées qu'aux autorités judiciaires.

En ce qui concerne la deuxième question, le CEPD a considéré qu'il y a de bonnes raisons de penser que la protection des dénonciateurs et des informateurs doit être la même après la clôture d'une enquête, qu'il y ait ou non un suivi. La vulnérabilité du rôle du dénonciateur ou de l'informateur, et par conséquent les risques pour leur vie privée et leur intégrité, ne changent pas selon que l'enquête est ouverte ou refermée sans suivi.

Cette approche n'exclurait bien sûr pas que, dans la pratique, il y ait des situations où la protection des dénonciateurs ou des informateurs doit s'effacer devant les revendications légitimes d'autrui. Le temps écoulé peut être un facteur pertinent, mais il est évidemment difficile de se livrer à des spéculations de manière abstraite à ce propos.

2.6.3. Transferts internationaux de données à caractère personnel - Agence européenne de la sécurité aérienne

L'Agence européenne de sécurité aérienne (AESA) déploie certaines activités (en particulier des services dans le domaine de la certification) qui donnent lieu au paiement d'honoraires et de redevances par les demandeurs. Une partie de ces activités de certification peut être assurée entièrement ou partiellement en dehors du territoire des États membres. Dans certains cas, l'Agence a été invitée par les demandeurs à leur fournir les noms et la date de

déplacement des experts afin de leur permettre de procéder au paiement de la facture.

Le DPD de l'AESA a demandé l'avis du CEPD concernant l'application de l'article 9 du règlement au dossier concerné.

Selon l'article 9, paragraphe 1, de ce règlement, le transfert de données à caractère personnel à des destinataires autres que les institutions et organes communautaires, et qui ne sont pas soumis à la législation nationale adoptée en application de la directive 95/46/CE, ne peut avoir lieu que **pour autant qu'un niveau de protection adéquat soit assuré** dans le pays du destinataire.

Le CEPD a souligné que, si le pays tiers en question - en dehors de l'EEE - n'assure pas un niveau adéquat de protection, il y a lieu de tenir compte des autres conditions visées à l'article 9 L'article 9, paragraphe 6, prévoit que «par dérogation aux paragraphes 1 et 2, l'institution ou l'organe communautaire peut transférer des données à caractère personnel si: [...] d) le transfert [est] nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important [...]».

Comme la mise en œuvre des services décrits ci-dessus est l'une des activités essentielles de l'AESA, les transferts réalisés pour paiement de ces services pourraient être considérés, en principe, comme **nécessaires au fonctionnement de cet organe**, de manière à pouvoir bénéficier d'une dérogation au titre de l'article 9, paragraphe 6, point d).

Le CEPD a également souligné que, dans le cas présent, il semblait que les transferts ne seraient pas «répétés, massifs ou structurels», mais qu'ils seraient effectués de manière ponctuelle vers différents destinataires établis dans différents pays. Quant aux risques courus par les personnes concernées, aucun risque spécifique n'a été mentionné. Les catégories de données à transférer (nom et date de déplacement des experts concernés) ne semblent pas davantage poser de problèmes particuliers.

Le CEPD a toutefois souligné que, dans les cas où une exception est appliquée, aucune garantie n'est en principe assurée Il a donc recommandé l'inclusion d'une clause, dans le contexte du transfert, précisant que le destinataire est légalement autorisé à demander ces données et qu'il limitera leur utilisation aux seules fins justifiant le transfert.

2.6.4. Politique sur l'usage interne du courrier électronique - Commission européenne

La Commission européenne a consulté le CEPD à propos de sa politique sur l'usage interne du courrier électronique. Le CEPD a analysé certains points particuliers de cette politique du point de vue des principes de la protection des données à caractère personnel et du respect de la vie privée ainsi que du point de vue des mesures de sécurité.

Dans ce contexte, la Commission a informé le CEPD qu'elle ne procède pas à un contrôle à grande échelle au niveau individuel. Un courrier envoyé au CEPD précise que «*la seule forme de contrôle routinier par le service du courrier électronique de la Commission (DG DIGIT) se fait au niveau des DG et des services, et non au niveau de boîtes individuelles ni au niveau des données de trafic propres à un personnel. DG DIGIT contrôle l'utilisation afin de réduire les menaces opérationnelles, mais aucun compte rendu de routine n'est produit contrôlant l'activité d'une boîte individuelle ou divulguant des données individuelles de trafic susceptibles d'être utilisées pour analyser des abus individuels*».

Cela signifie que le contrôle d'une boîte de courrier électronique en particulier est **uniquement possible dans le cadre d'une enquête en cours**. Le CEPD a salué cette approche, qu'il considère comme la meilleure pratique.

2.6.5. Accès des administrateurs IT- Banque européenne d'investissement

Le 26 mars 2010, le CEPD a répondu à une consultation de la Banque européenne d'investissement (BEI) en lui adressant des recommandations quant à la gestion de l'accès des administrateurs IT aux données à caractère personnel enregistrées dans les systèmes et les applications informatiques. Le CEPD a souligné la nécessité d'appliquer le **principe de la séparation des tâches**. Le degré de séparation doit être défini en fonction du niveau de risque identifié pour le processus concerné.

La gestion des droits d'accès des administrateurs IT doit reposer sur une approche équilibrée comportant à la fois des mesures techniques et organisationnelles. Le CEPD a également recommandé que ces mesures soient correctement documentées dans une politique de sécurité détaillée établie par l'institution.

2.6.6. Contrôle des communications téléphoniques

Le CEPD a été consulté à propos d'un projet impliquant le contrôle des communications téléphoniques dépassant un seuil prédéfini.

Le système envisagé était basé sur un seuil prédéterminé (nombre d'heures toléré, ou coût toléré des communications téléphoniques) qui serait proposé au personnel. À la fin de chaque mois, les cadres recevraient une liste des employés travaillant pour eux et dont les communications à destination de l'étranger ou de téléphones mobiles (communications privées et/ou professionnelles) ont dépassé le seuil atteint au cours du mois précédent.

Le CEPD a reconnu que la légalité du traitement de ces données est couverte par l'exercice légitime de l'autorité publique dont est investi l'institution ou l'organe de gérer efficacement l'utilisation des outils de télécommunication au sein de cette institution ou de cet organe (article 5, point a), du règlement, soutenu par les dispositions de l'article 37, paragraphe 2). Mais le CEPD a aussi considéré qu'un contrôle généralisé, par opposition à un contrôle plus sélectif, n'était pas nécessaire en permanence.

Même si le CEPD a accepté la finalité légitime de la gestion budgétaire, il a estimé que le contrôle de l'utilisation du téléphone à des fins privées, même sans communiquer les détails des appels passés, pourrait éventuellement être considéré comme une atteinte au droit à la vie privée des membres du personnel.

À cet égard, le CEPD a demandé que l'institution ou l'organe veille à ce que la valeur seuil déclenchant l'envoi de la liste à la direction soit suffisamment élevée pour éviter les contrôles injustifiés et permettre d'identifier les personnes uniquement en cas d'abus manifeste ou répété du système. Le CEPD a également invité l'institution ou organe à examiner dans quelle mesure d'autres indicateurs pourraient servir à identifier les mesures possibles.

Le CEPD a donc invité l'institution à réexaminer le système proposé et à envisager la possibilité d'utiliser d'autres méthodes moins intrusives.

2.6.7. Traitement supplémentaire de données en vue de leur transfert à AMEX - Autorité européenne de sécurité des aliments

L'Autorité européenne de sécurité des aliments (EFSA) traite les déclarations annuelles d'intérêts (DdI) de certaines personnes participant aux activités de l'EFSA afin de vérifier que ces personnes

Le contrôle de l'utilisation du téléphone à des fins privées pourrait en principe être considéré comme une violation du droit à la vie privée des membres du personnel.

n'ont pas de conflit d'intérêts susceptibles d'interférer avec leurs activités pour l'EFSA.

Au cours du contrôle préalable de ces opérations de traitement des données (dossier 2008-0737), le DPD de l'EFSA a demandé conseil au CEPD concernant l'utilisation de la base de données des déclarations d'intérêts aux fins de communiquer à son agence de voyages, AMEX, les données d'identification de ses experts extérieurs.

Le DPD de l'EFSA a demandé au CEPD si le traitement supplémentaire des données reprises dans la base de données des déclarations d'intérêts aux fins de communiquer à l'agence de voyages les données d'identification d'experts extérieurs serait conforme à l'article 4, paragraphe 1, point b), du règlement.

Cette disposition précise que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne peuvent être traitées ultérieurement de manière incompatible avec ces finalités.

Dans son avis, le CEPD a conclu que tout traitement supplémentaire par l'EFSA de données reprises dans la base de donnée des déclarations d'intérêts aux fins de fournir les données d'identification de personnes susceptibles de bénéficier des services de voyage d'AMEX répondrait à une finalité différente qui ne serait pas jugée compatible avec la finalité originale de la collecte et du traitement de ces données. Par conséquent, ce traitement supplémentaire par l'EFSA ne serait pas conforme à l'article 4, paragraphe 1, point b), du règlement.

Le CEPD a également souligné que le rôle et les responsabilités d'AMEX vis-à-vis de ces données ne sont pas décrits de façon suffisamment claire dans l'accord de protection des données conclu entre les parties. Cet accord ne précise notamment pas clairement pour quelles raisons et dans quelles conditions AMEX fait office de sous-traitant et/ou de responsable du traitement. Des garanties correctes doivent être adoptées pour protéger les droits des personnes concernées et pour sécuriser les transferts depuis AMEX vers d'autres destinataires, conformément aux lois en vigueur en matière de protection des données.

2.6.8. Délais de conservation des documents médicaux - Collège des chefs d'administration

En novembre 2006, le président du Collège des chefs d'administration (le Collège) a demandé l'avis du CEPD concernant une note rédigée par la Commission à propos des délais de conservation de certains documents médicaux. Le 26 février 2007, le CEPD a rendu un avis soulignant que le délai de

Le délai de conservation de 30 ans pour les documents médicaux devrait être considéré comme un maximum.

30 ans indiqué dans la note ne doit pas être le délai *minimum* de conservation des documents médicaux. Au contraire, à quelques exceptions près, de portée limitée, ce délai doit être considéré comme la période de conservation *maximale*. En outre, le CEPD a considéré que l'application de l'article 4 du règlement requiert d'examiner la nature des documents médicaux afin de déterminer les délais de conservation adaptés pour chaque type de document.

La question du délai de conservation des documents médicaux a été évoquée une nouvelle fois en septembre 2010, lorsque le Comité de préparation pour les affaires sociales (CPAS), le sous-comité compétent du Collège, a rédigé un rapport portant sur différents cas avec des délais de conservation spécifiques des documents médicaux. En octobre 2010, le Collège a consulté le CEPD à propos de ce rapport. Le CEPD examine actuellement la question et exprimera sa position sur cette consultation en tenant compte de son avis de février 2007 et de la position adoptée dans le cadre d'avis de contrôle préalable antérieurs.

2.6.9. Dispositions d'application concernant le délégué à la protection des données

*Le règlement relatif à la protection des données impose à chaque institution ou organe de l'Union européenne d'adopter des **dispositions d'application relatives aux tâches, fonctions et compétences du DPD**. En juillet 2010, le CEPD a publié des **lignes directrices** pour faciliter la rédaction de dispositions d'application dans les cas où ces dispositions n'auraient pas encore été adoptées ou devraient être révisées.*

En mai 2010, l'Agence exécutive du Conseil européen de la recherche (ERCEA) a soumis au CEPD, pour consultation, ses dispositions d'application concernant le rôle du DPD. Ces règles couvraient également le rôle des responsables du traitement et les règles régissant l'exercice de leurs droits par les personnes concernées. Le CEPD a salué cette approche inclusive, d'autant plus que l'ERCEA a adopté les meilleures pratiques proposées au fil des ans par le CEPD, comme par exemple:

- le maintien d'un inventaire anonyme des demandes écrites émanant d'une personne concernées en vue de faire valoir un droit (accès, rectification, blocage, etc.);
- la collaboration avec le service informatique et le service de sécurité de l'information de l'Agence afin de compléter les sources d'information du DPD.

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et la Cour des comptes ont présenté une version révisée de leurs dispositions d'application au CEPD pour consultation. Ces consultations étaient conformes aux lignes directrices publiées par le CEPD.

2.7. Lignes directrices thématiques

L'expérience acquise grâce à l'application du règlement relatif à la protection des données a permis au personnel du CEPD de traduire leur expertise en une orientation générale pour les institutions et organes dans les domaines du recrutement, des données relatives à la santé, des enquêtes administratives et des procédures disciplinaires ainsi que de la vidéosurveillance. Le CEPD prépare actuellement des lignes directrices pour l'évaluation du personnel et le traitement des données personnelles dans les procédures anti-harcèlement.

2.7.1. Lignes directrices relatives aux enquêtes administratives et aux procédures disciplinaires

En avril 2010, le CEPD a publié des lignes directrices relatives au traitement des données à caractère personnel dans le cadre d'enquêtes administratives et de procédures disciplinaires entamées par les institutions et les organes de l'UE.

L'objectif de ces lignes directrices est d'harmoniser les bonnes pratiques dans ce domaine et de faciliter le respect des dispositions du règlement. Ces lignes directrices présentent, de façon claire et concise, le résultat des positions du CEPD telles qu'elles ont été examinées dans les avis de contrôle préalable. Elles présentent également un certain nombre de recommandations concernant chaque principe fondamental du règlement.

Une recommandation importante concerne le **droit d'accès et de rectification** d'une personne concernée. Même si ces droits peuvent parfois être limités, le responsable du traitement des données

doit veiller à ce que ces restrictions soient nécessaires et adoptées au cas par cas. En outre, le responsable du traitement doit veiller à ce que les droits d'accès et de rectification ainsi que le droit à l'information soient garantis par d'autres moyens.

Le CEPD a également souligné le manque d'approche harmonisée en ce qui concerne le **délai de conservation des données disciplinaires**, ce qui entraîne un conflit avec les principes de protection des données et d'autres droits fondamentaux de la personne concernée. Cette différence s'explique par des lacunes importantes à l'annexe IX du statut des fonctionnaires et par l'absence de politique commune des institutions et des organes de l'UE concernant la conservation de ces données.

Enfin, le CEPD a souligné la nécessité de prendre en considération la question spécifique de **l'interception des communications**, en mettant l'accent sur la base juridique de la mise sur écoute des communications vocales et sur la possibilité de le faire sans mandat ou autorisation judiciaire.

Ces lignes directrices devront être utilisées par les agences dans leur notification au CEPD de procédures dans ce domaine en vue d'un contrôle préalable, mais elles devront également servir de guide pratique pour toutes les institutions et tous les organes. La prochaine étape consistera, pour le CEPD, à rendre un avis commun concernant les notifications de contrôle préalable soumises par les agences dans la perspective de ces lignes directrices.

2.7.2. Lignes directrices en matière de vidéosurveillance

En mars 2010, le CEPD a publié une série de lignes directrices pratiques destinées aux institutions et aux organes de l'Union européenne concernant la façon d'utiliser la vidéosurveillance de façon responsable avec des mesures de protection effectives. Ces lignes directrices énoncent les principes permettant d'évaluer la nécessité de recourir à la vidéosurveillance et fournissent des orientations sur la façon d'en réduire l'impact sur la vie privée et les autres droits fondamentaux.

Un projet de consultation a été publié en juillet 2009, et il est repris dans le rapport annuel du CEPD pour 2009. Le processus de consultation a suscité un retour d'information sur la façon d'améliorer le projet de lignes directrices et de renforcer la coopération avec les parties prenantes.

Les lignes directrices indiquent que les décisions quant à l'installation de caméras et la manière de les utiliser ne doivent pas être prises en se basant uniquement sur les besoins de sécurité. Au lieu de cela, **ces besoins doivent être mis en balance avec le respect des droits fondamentaux de l'individu**. Cela étant dit, la sécurité et le respect des droits fondamentaux ne doivent pas s'exclure mutuellement. Grâce à une approche pragmatique basée sur les principes de la sélectivité et de la proportionnalité, les systèmes de surveillance peuvent répondre aux besoins de sécurité tout en respectant la vie privée.

Dans les limites prévues par la législation sur la protection des données, chaque institution et organe européen dispose d'une marge d'appréciation sur la manière de concevoir son propre système. Les lignes directrices ont été conçues pour permettre une personnalisation. Cette flexibilité doit empêcher qu'une interprétation rigide ou bureaucratique des préoccupations concernant la protection des données ne vienne entraver la satisfaction des besoins réels de sécurité ou la réalisation d'autres objectifs légitimes.

Parallèlement, chaque institution doit également **démontrer que des procédures sont en place afin d'assurer la conformité** avec les exigences de protection des données. D'un point de vue organisationnel, les pratiques recommandées comprennent l'adoption d'une série de garanties en matière de protection des données devant être décrites dans la politique de vidéosurveillance de l'institution, ainsi que des audits périodiques pour vérifier la conformité. Les institutions sont encouragées à réaliser des analyses d'impact, tandis que le contrôle préalable par le CEPD restera obligatoire pour la vidéosurveillance impliquant des risques inhérents importants (par ex. la surveillance dissimulée ou les systèmes de surveillance préventive dynamique).

Les institutions de l'Union ont jusqu'au 1er janvier 2011 pour démontrer leur conformité avec les lignes directrices du CEPD.

Période transitoire

Les lignes directrices s'appliquent aux systèmes existants et futurs: chaque institution est tenue de mettre ses pratiques existantes en conformité avec les lignes directrices pour le 1er janvier 2011. Le CEPD est resté disponible quand des conseils supplémentaires étaient requis sur des questions spécifiques.

Le CEPD a également apporté son aide aux institutions qui avaient déjà soumis leurs notifications de contrôle préalable avant la publication des lignes directrices. Il existe neuf cas de ce type. En juillet 2010, le CEPD a publié des recommandations préliminaires dans ces dossiers, étant entendu que le respect de ces recommandations ne dispense pas une institution de procéder à une analyse interne approfondie des lignes directrices, de ses pratiques et de son statut de conformité. Les commentaires du CEPD sont destinés à aider les institutions concernées à concentrer leur attention sur les éléments les plus importants. Les problèmes nécessitant une attention spécifique sont par exemple la surveillance dissimulée et les délais de conservation.

Dans une perspective semblable, le CEPD a également communiqué des orientations préliminaires à l'OLAF, dont le système de vidéosurveillance est le seul à avoir fait l'objet d'un contrôle préalable par le CEPD avant la publication des lignes directrices (la raison étant qu'il s'agissait d'une véritable notification de contrôle préalable impliquant un nouveau système et qu'il fallait donc s'en occuper en priorité).

Le CEPD a aussi continué de fournir des orientations aux autres institutions en ce qui concerne l'interprétation et la mise en œuvre des lignes directrices. Il a continué de traiter les réclamations et les consultations, y compris une réclamation portant sur des pratiques de surveillance dissimulée dans une institution et une enquête administrative concernant les restrictions d'utilisation de séquences de vidéosurveillance en tant qu'éléments de preuve lorsque ces images ont été obtenues d'une façon contraire aux règles applicables en matière de protection des données.

2.8. La politique de conformité et d'application du CEPD

En décembre 2010, le CEPD a adopté un document stratégique intitulé «Contrôler et garantir le respect du règlement (CE) n° 45/2001».

Cette politique marque un changement de rythme fondamental en matière d'application du règlement. Jusqu'à présent, le CEPD a préféré formuler des recommandations et encourager le respect du règlement plutôt que d'adresser une mise en garde ou une admonestation aux responsables du traitement ou donner des instructions légalement

contraignantes. Après avoir agi ainsi pendant cinq ans, le CEPD pense que l'heure est venue d'adopter une approche plus ferme de l'application du règlement, surtout dans les cas de violations graves, délibérées ou répétées des principes de protection des données. C'est ainsi que cette politique fixe un certain nombre de critères visant à garantir l'exercice proactif, cohérent et transparent de ses pouvoirs d'exécution.

Ce document définit le cadre dans lequel le CEPD contrôle, mesure et garantit le respect des règles de protection des données dans l'administration européenne. Il explique la nature des différents pouvoirs d'exécution conférés au CEPD et décrit les facteurs déterminants et déclencheurs de toute mesure formelle qu'il serait susceptible de prendre.

Cette politique vise à **encourager le respect volontaire et les bonnes pratiques** et à créer des incitations suffisantes en matière de conformité en:

- soulignant à qui la responsabilité échoit;
- expliquant comment le CEPD soutient le respect des règles;
- expliquant ce que fera le CEPD en cas de non-conformité.

Cette politique met aussi largement l'accent sur le **principe de «responsabilisation»** afin d'encourager le respect des règles et l'adoption de bonnes pratiques au sein de l'administration de l'UE. La «responsabilisation» nécessite que les institutions et organes de l'UE, de même que les responsables du traitement des données agissant en leur nom, mettent en place des mesures appropriées et efficaces pour faire en sorte que les principes et les obligations de protection des données soient respectés, et le prouvent au CEPD.

Enfin, ce document décrit l'approche du CEPD en matière de transparence et de publicité dans le contexte de ses activités d'exécution, insistant sur l'importance de ces outils tant pour les parties prenantes que pour la bonne gouvernance. À l'avenir, le CEPD diffusera donc régulièrement des informations relatives à tout renvoi officiel devant le Parlement, le Conseil, la Commission ou la Cour de justice. Qui plus est, il évaluera au cas par cas s'il est opportun de diffuser des informations concernant les autres mesures d'exécution.

Le CEPD espère qu'en lui permettant de se concentrer sur ses responsabilités de contrôle et de garantie de la conformité par une approche de la mise en application ciblée, sélective et basée sur les risques, ce document stratégique facilitera une utilisation plus efficiente et plus efficace des moyens du CEPD.

Le CEPD pense que l'heure est venue d'adopter une approche plus ferme de l'application du règlement.

3 CONSULTATION

3.1. Introduction: vue d'ensemble de l'année et tendances principales

En 2010, la Commission a fait des progrès importants vers un nouveau **cadre juridique modernisé de protection des données en Europe**. La consultation publique lancée en 2009 a été achevée et complétée par d'autres consultations ciblées auprès des principaux acteurs concernés.

En novembre 2010, la Commission a publié sa communication définissant une approche globale en matière de protection des données à caractère personnel dans l'Union européenne, identifiant les priorités principales et les objectifs clés pour la révision des règles actuelles.

Ce projet a été un élément important du programme du CEPD en 2010 et sera l'une des priorités principales des prochaines années.

En 2010, la Commission et le Conseil ont également consacré des efforts importants à **la mise en œuvre du programme de Stockholm** - Une Europe ouverte et sûre au service des citoyens, adopté par le Conseil européen en décembre 2009. Ce programme définit les orientations stratégiques de la planification législative et opérationnelle dans le domaine dans l'espace de liberté, de sécurité et de justice, et se concentre sur les intérêts et les besoins des citoyens.

*Le programme de Stockholm souligne que **les mesures de sécurité et de respect de la loi doivent aller de pair avec le respect des droits fondamentaux, y compris la protection des données**. Il reconnaît également la nécessité de protéger les données personnelles dans une société mondiale caractérisée par une évolution technologique rapide et des échanges d'informations sans frontières.*

Le CEPD a suivi de près plusieurs initiatives directement liées à la mise en œuvre du programme de Stockholm. Le CEPD s'est notamment penché sur des questions critiques de protection des données liées à la stratégie de sécurité intérieure de l'UE, à la gestion de l'information dans l'espace de liberté, de sécurité et de justice ainsi qu'à la politique antiterroriste européenne. Dans l'ensemble, les développements ayant trait au programme de Stockholm ont dominé le programme de travail du CEPD et continueront de le faire au cours des prochaines années.

L'interface entre la vie privée et les développements technologiques est également un domaine dans lequel le CEPD est intervenu de façon significative. En mai 2010, la Commission a publié sa communication relative à une stratégie numérique pour l'Europe, l'objectif étant de fixer les priorités de l'Union dans les domaines de l'internet et des technologies numériques. Plusieurs de ces initiatives sont extrêmement pertinentes pour la protection des données et sont suivies de près par le CEPD. Le CEPD est également convaincu que les nouvelles technologies ne représentent pas uniquement des nouveaux

défis pour le respect de la vie privée et la protection des données, mais qu'elles offrent aussi de nouvelles possibilités de protection des données personnelles.

Il est donc essentiel d'intégrer les exigences de respect de la vie privée dans la conception, l'exploitation et la gestion des systèmes informatiques tout au long du cycle de vie des informations. C'est pourquoi le CEPD préconise vivement l'inclusion du principe de «respect de la vie privée dès la conception» (Privacy by Design) dans le nouveau cadre juridique.

Le CEPD a également été consulté à propos de différentes initiatives dans le domaine de la **coopération internationale en matière de sécurité et de maintien de l'ordre**, comme l'accord général UE - États-Unis relatif à l'échange de données à des fins de maintien de l'ordre et l'accord relatif à l'échange de données financières aux fins du programme de surveillance du financement du terrorisme (TFTP). Il est également intervenu dans le contexte de l'accord commercial anti-contrefaçon (ACAC) et de plusieurs accords relatifs à l'échange des dossiers passagers (PNR)

Le CEPD a également été actif dans d'autres domaines, comme les échanges de données à grande échelle dans le contexte du Système d'information sur le marché intérieur, l'utilisation de scanners de sûreté dans les aéroports et la coopération en matière fiscale.

La grande diversité des domaines de politique dans lesquels le CEPD est consulté démontre plus encore que le traitement des données est devenu un élément de plus en plus important d'un grand nombre d'initiatives législatives. Ces initiatives posent souvent des questions importantes en matière de protection des données et, de ce fait, justifient le rôle du CEPD en tant que conseiller des institutions de l'Union européenne.

3.2. Cadre d'action et priorités

3.2.1. Mise en œuvre de la politique de consultation

Même si les méthodes de travail du CEPD dans le domaine de la consultation ont évolué au fil des ans, l'approche fondamentale des interventions n'a pas changé. Le document stratégique adopté en mars 2005 et intitulé «Le CEPD en tant que conseiller des institutions communautaires à l'égard des propositions de législation et documents connexes»([8]) reste d'actualité, bien qu'il faille désormais le lire à la lumière du traité de Lisbonne.

Les avis formels du CEPD - fondés sur l'article 28, paragraphe 2, ou l'article 41 du règlement (CE) n° 45/2001 - sont les principaux instruments et contiennent une analyse complète de tous les éléments relatifs à la protection des données qui figurent dans une proposition de la Commission ou tout autre instrument pertinent.

En règle générale, le CEPD formule des avis sur les textes non législatifs (comme les documents de travail de la Commission, les communications ou les recommandations) lorsque la protection des données en est un élément important. Il rédige occasionnellement des commentaires par écrit à des fins plus limitées, afin de faire passer un message rapide et fondamental, de se concentrer sur un ou plusieurs aspects techniques, voire même de synthétiser ou de répéter des observations antérieures.

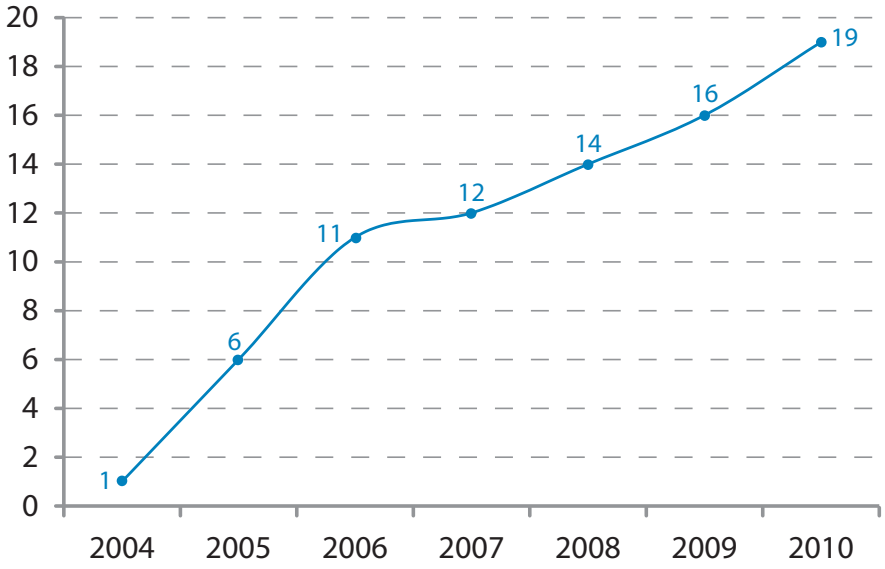
Il peut également recourir à d'autres outils tels que des présentations orales, des courriers explicatifs, des conférences de presse ou des communiqués de presse. En 2010, par exemple, le CEPD a organisé une conférence de presse sur «L'avenir du cadre juridique de protection des données de l'UE» en combinaison avec la présentation du rapport annuel 2009.

Le CEPD est disponible à tous les stades de l'élaboration des politiques et du processus législatif et utilise toute une série d'autres instruments dans son rôle consultatif. Même s'il doit pour cela entretenir des contacts étroits avec les institutions de l'UE, il est essentiel qu'il conserve son indépendance.

Les contacts avec la Commission ont lieu aux différents stades de la préparation des propositions, et

([8]) Disponible sur le site internet du CEPD sous Publications > Documents.

Évolution des avis législatifs 2004-2010



leur intensité dépend du sujet et de l'approche des services de la Commission. C'est notamment le cas des projets à long terme comme l'initiative eJustice ou la révision du cadre de protection des données, auxquels le CEPD a contribué à différents stades.

Des contacts réguliers avec les services des institutions concernées ont également eu lieu en phase de suivi. Dans certains cas, le CEPD et son personnel ont été étroitement impliqués dans les discussions et les négociations au Parlement et au Conseil. Dans d'autres cas, la Commission a été le principal interlocuteur en phase de suivi. Le processus législatif concernant le règlement Frontex, le suivi de la stratégie numérique (par exemple en matière de neutralité du réseau) et le système d'information sur le marché intérieur sont d'autres exemples d'une implication intensive ayant abouti à des commentaires supplémentaires de la part du CEPD en 2010.

3.2.2. Résultats en 2010

En 2010, l'augmentation rapide du nombre d'avis s'est poursuivie. Le CEPD a émis 19 avis sur une grande variété de sujets.

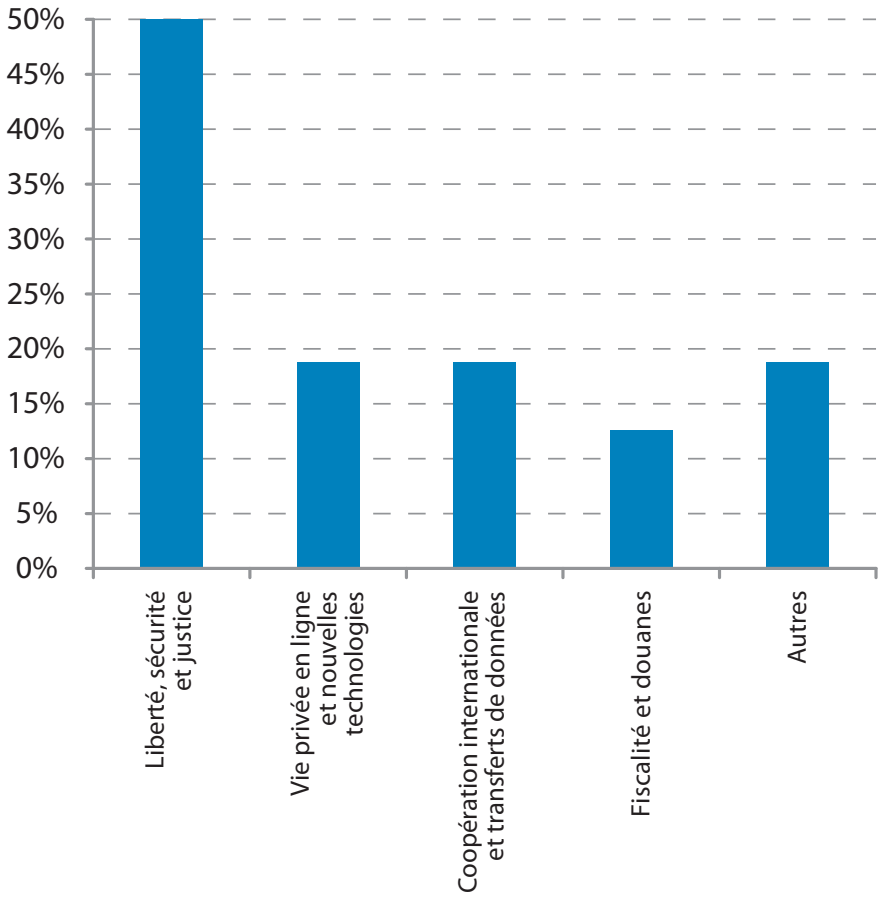
Grâce à ces avis et aux autres instruments utilisés, le CEPD a mis en œuvre les priorités pour 2010, telles que définies dans l'inventaire. Ces 19 avis couvraient différents domaines de la politique de l'UE.

L'inventaire 2010 définissait quatre principaux domaines d'attention:

- le nouveau cadre juridique en matière de protection des données;
- l'espace de liberté, de sécurité et de justice;
- la coopération internationale et les transferts de données;
- les développements technologiques.

Le CEPD a accordé une attention importante à tous ces domaines en 2010. Conformément à l'inventaire 2010, le CEPD s'est concentré principalement sur les initiatives auxquelles l'inventaire avait attribué une priorité élevée (c'est-à-dire les initiatives «rouges»). Le CEPD a émis un avis ou réagi d'une autre façon

Principaux domaines de politique des avis législatifs en 2010



pour 13 des 15 propositions prioritaires adoptées dans le courant de l'année 2010([9]).

Le contenu des avis du CEPD et des autres contributions dans le domaine de la consultation est exposé plus en détail ci-dessous.

3.3. Révision du cadre européen en matière de protection des données

La révision du cadre européen en matière de protection des données était déjà l'une des premières priorités du CEPD en 2009, au moment où les discussions relatives à la réforme ont commencé officiellement. En 2010, la réforme a suscité un intérêt plus vif avec la publication, en novembre 2010, de la communication de la Commission définissant une approche globale en matière de protection des données à caractère personnel dans l'Union européenne. Le CEPD a accordé une attention particu-

([9]) Dans deux de ces cas (révision du règlement (CE) n° 831/2002 concernant l'accès aux données confidentielles à des fins scientifiques et décision-cadre du Conseil relative aux attaques visant les systèmes d'information), un avis n'a pas été jugé nécessaire à ce stade.

Le nouveau cadre de protection des données doit être ambitieux et améliorer réellement l'efficacité des instruments de protection des données dans une société mondialisée et entraînée par les technologies.

lière à ce dossier tout au long de l'année 2010 et fait passer ses messages de diverses façons.

Le CEPD a organisé une **conférence de presse** *ad hoc* immédiatement après la publication de la communication de la Commission afin d'exprimer publiquement son avis concernant le nouveau cadre juridique. À cette occasion, le CEPD a souligné l'importance de cette révision, dont il estime qu'elle arrive à point nommé, et il a donné son point de vue concernant les principaux points du nouveau cadre.

*Le CEPD a insisté sur la nécessité d'une **protection des données forte et efficace** dans une société où les informations à caractère personnel sont utilisées dans des proportions incommensurables, souvent sans que les personnes concernées en aient conscience. Le CEPD a salué la communication de la Commission mais a prévenu qu'il n'y avait pas de **place pour l'erreur**: les défis sont considérables, et les solutions proposées doivent être tout aussi **ambitieuses** et améliorer l'efficacité des instruments de protection des données.*

Le CEPD a également exprimé son avis sur les principaux aspects du nouveau cadre. Il a notamment souligné:

- son soutien en faveur d'un **rapprochement accru** des législations nationales en matière de protection des données;
- la nécessité d'une approche **technologiquement neutre**;
- l'inclusion des principes de **respect de la vie privée dès la conception** (***Privacy by Design***) **et de responsabilisation** (***Accountability***);
- l'instauration d'une obligation de notifier les atteintes à la sécurité couvrant tous les secteurs concernés;
- l'**inclusion** des domaines de **la police et de la justice** dans le cadre général.

Le CEPD a approfondi ces points de vue dans un avis global adopté en janvier 2011.

La Commission devrait adopter une proposition législative à part entière dans le courant de l'année 2011. Le CEPD continuera de suivre le processus législatif de très près en 2011 et fournira de nouvelles contributions en fonction des besoins.

3.4. Espace de liberté, de sécurité et de justice

En 2010, le CEPD a suivi avec beaucoup d'attention les développements liés à la mise en œuvre du **programme de Stockholm** et formulé des recommandations sur un certain nombre d'initiatives législatives et non législatives liées directement ou indirectement à l'espace de liberté, de sécurité et de justice.

3.4.1. Stratégie de sécurité intérieure de l'Union européenne

La stratégie de sécurité intérieure (SSI) définit un modèle de sécurité européen visant à intégrer les actions en matière d'application des lois et de coopération judiciaire, de gestion des frontières et de protection civile. La SSI, approuvée par le Conseil en février 2010 et avalisée par le Conseil européen un mois plus tard, a été suivie d'une communication de la Commission en novembre 2010 ciblant les menaces de sécurité les plus pressantes auxquelles l'Union était confrontée, comme le crime organisé, le terrorisme, la cybercriminalité, la gestion des frontières extérieures de l'Union européenne et les catastrophes civiles.

En raison de la nature potentiellement intrusive des mesures à prendre dans le cadre de cette stratégie, le CEPD a suivi de près les discussions la concernant et les mesures envisagées pour la mettre en œuvre. Dans son avis adopté en décembre 2010, le CEPD a souligné la nécessité de garantir un bon équilibre

Le CEPD a appelé de ses vœux une stratégie de sécurité intérieure efficace soutenue et complétée par un mécanisme solide de protection des données.

entre l'objectif d'assurer la sécurité des citoyens et la protection efficace de leur vie privée et de leurs données personnelles. Le CEPD a également attiré l'attention sur le fait que la SSI présente des liens évidents avec les autres stratégies européennes actuellement en cours d'élaboration au niveau de l'Union, comme la stratégie de gestion de l'information et la révision du cadre européen en matière de protection des données.

Le CEPD a demandé une **approche plus globale et intégrée de la SSI** générant des liens et des interactions explicites entre les différentes initiatives concernées. Il a estimé qu'il n'était pas possible de mettre en place une SSI efficace sans le soutien d'un mécanisme solide de protection des données venant le compléter.

3.4.2. Gestion de l'information

Le programme de Stockholm invite la Commission à évaluer la nécessité de mettre au point un **modèle européen en matière d'échange d'informations** à partir d'une évaluation des instruments existants d'échange d'informations. Ce programme fait également référence à un **système solide de protection des données** en tant que principale condition pour la stratégie européenne de gestion de l'information. En juillet 2010, la Commission a adopté une **communication donnant une vue d'ensemble de la gestion des informations** dans l'espace de liberté, de sécurité et de justice. Le CEPD a formulé un avis sur cette communication en septembre 2010.

Le CEPD soutient pleinement le travail d'évaluation en cours de tous les instruments concernant la gestion de l'information dans l'espace de liberté, de sécurité et de justice. Il a souligné le fait que cette initiative constitue une **première étape dans le processus d'évaluation** et a appelé de ses vœux une **évaluation objective, globale et approfondie** de tous les instruments existants à utiliser dans le cadre de la stratégie de gestion de l'information avant d'en proposer de nouveaux.

Le CEPD a également suggéré de signaler et de prendre en considération toutes les failles et les faiblesses des systèmes dans les travaux futurs en matière de gestion de l'information.

3.4.3. FRONTEX

En février 2010, la Commission a présenté une **proposition de révision du cadre juridique de FRONTEX** afin de renforcer les capacités opérationnelles de cette agence. Dans son avis publié en mai 2010, le CEPD se concentre sur les tâches croissantes de l'agence et leurs conséquences sur la protection des données.

Le CEPD a reproché en particulier à cette proposition de ne pas spécifier si FRONTEX serait autorisée à traiter des données personnelles, et dans quelle mesure. Le CEPD a invité le législateur à fixer des règles claires en matière de protection des données et à clarifier les conditions et les circonstances dans lesquelles FRONTEX serait autorisé à traiter des données.

Le CEPD a également suivi de près les discussions sur ce dossier au Parlement européen. Dans un courrier adressé au rapporteur du Parlement européen, il a avancé des suggestions concrètes visant à instaurer une **base juridique spécifique** traitant de cet aspect dans la proposition, qui fera l'objet de **garanties fortes en matière de protection des données** conformément aux principes de proportionnalité et de nécessité.

Les données personnelles liées à des soupçons non confirmés d'activités terroristes ne devraient pas être stockées indéfiniment.

3.4.4. Politique antiterroriste

La lutte contre le terrorisme est un domaine dans lequel des données personnelles sont souvent traitées à grande échelle de façon préventive.

Dans son avis relatif à la politique antiterroriste, le CEPD a demandé des **initiatives concrètes** en faveur du respect des droits fondamentaux dans ce domaine, et notamment le droit à la protection des données à caractère personnel. Le CEPD a souligné la nécessité de garantir la **cohérence** et des relations claires entre toutes les politiques et les initiatives dans le domaine des affaires intérieures et de la sécurité intérieure. Il a également recommandé que le législateur européen **renforce le rôle de la protection des données dans ce domaine**. Le **principe de nécessité**, notamment, devrait être envisagé de façon explicite dans chaque proposition. Cela devrait en conséquence empêcher tout chevauchement avec les instruments existants. La collecte et l'échange de données personnelles devraient en outre être limités au strict nécessaire pour les objectifs poursuivis.

En outre, une approche complète et globale devrait être proposée en ce qui concerne les **mesures de gel des avoirs** visant certains pays et personnes suspectées de terrorisme, de façon à garantir aussi bien l'efficacité des actions répressives que le respect des droits fondamentaux. En ce qui concerne la coopération internationale, le CEPD a rappelé la nécessité d'assurer la mise en place de protections adéquates dans les échanges de données à caractère personnel avec des pays tiers et des organisations internationales, afin d'assurer un respect adéquat du droit des citoyens à la protection des données dans ce contexte.

3.4.5. Commercialisation et utilisation des précurseurs d'explosifs

Du point de vue de la protection des données, la collecte des données relatives aux transactions suspectes portant sur certaines substances chimiques est l'aspect le plus sensible de la proposition de règlement sur la commercialisation et l'utilisation des précurseurs d'explosifs déposée par la Commission. Le principal objectif de cette proposition est de réduire les risques d'attaques par des terroristes ou autres criminels utilisant des engins explosifs artisanaux. Le CEPD a demandé une clarification des dispositions concernées afin de garantir **que le traitement des données restera proportionné** et afin d'éviter les abus.

Le fait de garantir un degré élevé de protection des données contribue également à lutter contre le racisme, la xénophobie et la discrimination, ce qui peut contribuer à prévenir la radicalisation et le recrutement dans les organisations terroristes.

Les principales recommandations émises par le CEPD sont les suivantes:

- **les données ne doivent pas être utilisées à d'autres fins** que la lutte contre le terrorisme (et d'autres crimes impliquant le détournement de produits chimiques aux fins de la fabrication artisanale d'explosifs);
- **les données ne devraient pas être conservées longtemps**, en particulier si le nombre des destinataires potentiels ou réels est important et/ou si les données devaient être utilisées pour l'extraction de données. Ce point est encore plus important dans les cas où il peut être démontré que la suspicion initiale n'était pas fondée. Le CEPD a demandé que le règlement précise un délai de conservation maximum (ne dépassant a priori pas deux ans) pour toutes les données à caractère personnel concernant des transactions suspectes signalées;
- le **traitement de certaines catégories de données devrait être expressément interdit** afin d'empêcher les pratiques discriminatoires telles que le profilage basé sur la race ou la religion.

3.4.6. Règlement Eurodac

Dans son avis publié en décembre 2010, le CEPD s'est concentré sur le problème de l'«**impossibilité de s'enregistrer**» (un terme qui, dans ce contexte, désigne l'impossibilité pour un demandeur d'asile de fournir des empreintes digitales lisibles). Le CEPD a insisté sur le principe selon lequel l'impossibilité de s'enregistrer ne devrait pas, en soi, porter atteinte aux droits des demandeurs d'asile. Il a notamment rejeté fermement la présomption selon laquelle une personne aux empreintes digitales illisibles a forcément voulu entraver la procédure d'identification, par exemple en s'automutilant.

Cet avis salue également le fait que la proposition actuelle **n'envisage pas la possibilité de donner aux services répressifs un accès à Eurodac**.

Le CEPD a émis des recommandations concernant l'information de la personne concernée: la situation précaire des demandeurs d'asile ou des immigrants en situation irrégulière fait qu'il est d'autant plus important de les informer de façon précise et utile de leurs droits. Cet avis a également couvert l'utilisation des meilleures techniques disponibles pour assurer le respect de la vie privée dès la conception ainsi que l'externalisation de tout ou partie du développement ou de la gestion du système.

Le CEPD avait déjà rendu plusieurs avis dans ce domaine. Les recommandations faites dans cet avis reposaient soit sur de nouveaux développements, soit sur des recommandations faites précédemment mais qui n'avaient pas encore été intégrées.

3.4.7. Abus sexuels d'enfants et pédopornographie

En mai 2010, le CEPD a adopté un avis sur une proposition de directive relative à la lutte contre l'exploitation et les abus sexuels concernant des enfants et contre la pédopornographie.

Dans cet avis, le CEPD a insisté sur la nécessité de garantir la **sécurité juridique** de toutes les parties concernées, y compris les fournisseurs d'accès à l'internet, les victimes et les personnes utilisant le réseau.

Même si la proposition mentionne la nécessité de prendre en considération les droits fondamentaux des utilisateurs finaux, le CEPD a considéré qu'il faudrait y ajouter l'obligation, pour les États membres, de garantir des **procédures harmonisées, claires et détaillées** sous le **contrôle d'autorités publiques indépendantes** pour la lutte contre les contenus illégaux.

Le CEPD n'a pas contesté la nécessité de mettre en place un meilleur cadre prévoyant des mesures adéquates protégeant les enfants contre les abus. Il a néanmoins souligné **l'impact** de certaines des mesures proposées, comme le blocage de sites internet et la mise en place de lignes d'assistance téléphonique, **sur les droits fondamentaux à la vie privée et à la protection des données** des personnes concernées. Le problème soulevé n'est pas spécifique à la lutte contre les abus sexuels d'enfants, mais concerne toute initiative visant à la collaboration du secteur privé aux fins de l'application des lois.

3.4.8. Décision de protection européenne et décision d'enquête européenne

Les initiatives d'un certain nombre d'États membres en vue d'une directive relative à la décision de protection européenne (DPE) et à la décision d'enquête européenne (DEE) se basent sur le programme de Stockholm et prévoient l'échange de données personnelles entre les États membres concernés. Tandis que la DPE vise à améliorer la protection des victimes d'actes criminels (et notamment des femmes), la DEE vise à créer un instrument unique, efficace et souple pour l'obtention d'éléments de preuve dans un autre État membre de l'Union européenne.

Dans son avis, le CEPD a souligné que le traitement des données à caractère personnel, surtout dans le domaine sensible de la liberté, de la sécurité et de justice, doit se conformer aux règles européennes en matière de protection des données.

Une protection efficace des données personnelles est non seulement importante pour les personnes concernées, mais elle contribue également à la réussite de la coopération judiciaire. Elle renforce la coopération judiciaire sur la base de la reconnaissance mutuelle et d'une meilleure qualité des données dans l'échange d'informations.

Parmi les différentes recommandations, le CEPD a demandé l'introduction de mesures adéquates pour garantir la protection des personnes du point

de vue du traitement des données à caractère personnel, de l'équité des procédures et du respect des dispositions en matière de confidentialité et de secret professionnel. Le CEPD a notamment souligné la nécessité de faire en sorte que 1) les systèmes d'authentification permettent uniquement aux personnes autorisées d'avoir accès aux données à caractère personnel, 2) les accès aux données ainsi que les traitements dont elles font l'objet soient identifiés, et 3) que des contrôles d'audit soient mis en œuvre.

Cet avis a aussi donné au CEPD une possibilité notable de souligner la nécessité de mettre en place des **procédures spécifiques** pour faire en sorte que **le CEPD soit aussi consulté** dans les cas où une initiative introduite par un État membre concerne le traitement de données à caractère personnel.

3.5. Vie privée dans les communications électroniques et technologie

3.5.1. Promotion de la confiance dans la société de l'information

En mai 2010, la Commission européenne a adopté la stratégie numérique, qui regroupe une série de politiques et d'actions visant à dynamiser l'économie numérique d'ici à 2020. Le CEPD a adopté un avis intitulé «Promouvoir la confiance dans la société de l'information en encourageant la protection des données et la vie privée». Cet avis constitue la contribution du CEPD à cette stratégie numérique.

L'avis du CEPD souligne que la confiance des consommateurs est un facteur essentiel pour l'émergence et le déploiement réussi des technologies de l'information et de la communication (TIC), dont l'identification par radiofréquence (RFID), les réseaux sociaux, la santé en ligne et la gestion électronique des transports ne sont que quelques exemples.

La confiance n'est possible que face à des TIC fiables, sécurisées et placées sous le contrôle de la personne, et pour autant que la protection des données personnelles et de la vie privée des personnes soit garantie.

L'Union européenne possède un cadre robuste en matière de protection des données qui, en principe, devrait garantir la protection des données personnelles des particuliers. Dans de nombreux cas pourtant, les TIC suscitent de nouvelles préoccupations qui ne sont pas prises en compte dans le cadre actuel. L'avis du CEPD aborde les mesures que l'Union européenne pourrait prendre ou promouvoir afin de renforcer ce cadre. Le CEPD invite notamment la Commission européenne à prendre les mesures suivantes:

- inclure le principe du **respect de la vie privée dès la conception** («Privacy by Design») comme **principe général et contraignant** dans le cadre juridique existant en matière de protection des données. Le respect de la vie privée dès la conception devrait également être préconisé par la stratégie numérique européenne et devenir un principe contraignant des politiques européennes futures, par exemple dans l'e-transport, l'administration en ligne, etc.;

- mettre en œuvre le principe du respect de la vie privée dès la conception en suivant une approche spécifique dans trois **domaines des TIC présentant des risques spécifiques** pour la vie privée et la protection des données: a) **RFID**: proposer des mesures législatives réglementant les principaux problèmes liés à l'utilisation de la RFID dans les cas où l'autorégulation ne donne pas les résultats attendus (par ex. principe d'adhésion (*opt-in*) sur le point de vente) b) **réseaux sociaux**: prévoir l'obligation de définir des paramètres par défaut favorables à la protection de la vie privée; c) **messages publicitaires ciblés**: doter les navigateurs de paramètres par défaut favorables au respect de la vie privée, afin de faciliter l'obtention du consentement des personnes à recevoir des messages publicitaires.

3.5.2. Internet et neutralité du réseau

En juin 2010, la DG INFSO a lancé une consultation publique relative à l'internet ouvert et à la neutralité du réseau en Europe. Cette consultation a soulevé un certain nombre de questions liées aux politiques de gestion du trafic qui permettent aux opérateurs de réseaux et aux fournisseurs d'accès à l'internet de gérer le trafic d'une certaine façon.

En réponse à cette consultation, le CEPD a formulé des commentaires afin d'attirer l'attention de la DG

INFSO sur les problèmes de protection des données et de respect de la vie privée qui se posent lorsque les fournisseurs d'accès et les opérateurs de réseaux s'engagent dans des politiques de gestion du trafic.

Le CEPD a mis en évidence deux aspects liés à la mise en œuvre des mécanismes de gestion du trafic. Premièrement, ces mécanismes permettent aux fournisseurs d'examiner le contenu des messages ou des transmissions. Deuxièmement, ils leur permettent d'attribuer ces informations à un utilisateur particulier. Le CEPD a souligné la nécessité, dans le cadre de ce genre de mesures, de respecter le cadre juridique européen en matière de protection des données. Plus précisément, il a rappelé que le cadre européen en matière de protection des données impose d'obtenir le **consentement libre et informé des utilisateurs**. Il a fourni des orientations pratiques quant aux conditions à respecter pour obtenir ce consentement.

3.5.3. Directive sur la conservation des données

Au cours d'une conférence organisée par la Commission en décembre 2010, le CEPD a délivré un discours évoquant l'«heure de vérité» de la directive sur la conservation des données, dans lequel il a demandé de saisir l'occasion pour **démontrer clairement la nécessité et la justification de cette directive**.

Le CEPD a souligné qu'une atteinte aussi considérable à la vie privée nécessite une justification solide. Le CEPD a donc demandé à la Commission européenne de profiter de l'exercice d'évaluation pour **démontrer la nécessité** de cette directive. Des faits et chiffres concrets doivent permettre d'évaluer si les résultats présentés dans l'évaluation auraient pu être obtenus par des moyens moins intrusifs.

Un nouvel instrument ou un instrument modifié au niveau de l'Union en matière de conservation des données doit indiquer clairement son champ d'application et offrir la sécurité juridique au citoyen. Cela signifie qu'il devrait aussi réglementer les possibilités d'accès et d'utilisation par les autorités répressives, et ne laisser aux États membres aucune possibilité d'utiliser les données pour d'autres finalités.

La directive sur la conservation des données impose aux fournisseurs publics de communications électroniques (opérateurs de téléphonie, de téléphonie mobile et fournisseurs d'accès à l'internet) de conserver des données relatives au trafic, à la localisation et aux abonnés à des fins de recherche, de détection et de poursuite d'infractions pénales graves.

Le CEPD a invité la Commission à démontrer la nécessité de conserver les données de communication à une échelle aussi vaste.

Arrêt du Tribunal constitutionnel allemand

Le 2 mars 2010, le Tribunal constitutionnel allemand a rendu un **arrêt rejetant la loi allemande transposant la directive sur la conservation des données**. Le tribunal allemand a estimé que les données enregistrées auraient dû faire l'objet de conditions plus strictes que celles prévues par le législateur allemand. Dans son arrêt, le Tribunal a formulé des critères plus restrictifs pour l'accès aux données et leur utilisation. Ces critères devraient être repris dans la législation nationale allemande pour permettre le respect de l'obligation de conservation des données sans enfreindre les droits fondamentaux prévus par la Constitution allemande.

Dans un communiqué de presse, le CEPD a souligné que cet arrêt devait être perçu comme une source d'inspiration pour les autres États membres de l'Union européenne et comme une contribution précieuse à l'évaluation de la directive sur la conservation des données, notamment à la lumière du nouveau cadre juridique mis en place par le traité de Lisbonne.

3.5.4. Déchets d'équipements électriques et électroniques

Le respect de la vie privée et la protection des données sont intrinsèquement liés aux mesures de sécurité visant les dispositifs capables de stocker un volume croissant de données à caractère personnel. Le CEPD a souligné cet aspect dans son avis d'avril 2010 concernant la proposition de refonte de la directive relative aux déchets d'équipements électriques et électroniques (DEEE) présentée par la Commission.

Même s'il partage l'objectif de cette proposition d'améliorer les politiques écologiques dans le domaine des DEEE, le CEPD a souligné que cette initiative s'attache uniquement aux risques environnementaux liés à l'élimination des DEEE, sans prendre en considération les **risques en matière de protection des données** qui peuvent accompagner une **élimination, une revalorisation ou un recyclage inadaptés** des DEEE.

Un risque accru de perte et de dispersion des données personnelles se présente lorsque des données personnelles relatives aux utilisateurs des appareils et/ou à des parties tierces restent enregistrées dans des équipements informatiques et de télécommunications (ordinateurs personnels, ordinateurs portables et appareils de communications électroniques) au moment de leur élimination.

Au vu de ces risques, le CEPD a souligné l'importance d'adopter des **mesures de sécurité** adéquates à chaque étape du traitement des données personnelles, y compris au moment de l'élimination des appareils contenant des données personnelles (du début à la fin).

Il faudrait par ailleurs prendre correctement en considération les principes du «**respect de la vie privée dès la conception**» et de la «**sécurité assurée dès la conception**» et les inclure dans la proposition pour faire en sorte que des mesures de sécurité et de respect de la vie privée soient intégrées par défaut dans la conception des équipements électriques et électroniques.

Les données à caractère personnel stockées dans les déchets d'équipements électroniques doivent bénéficier d'une protection adéquate.

3.5.5. Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)

Dans un avis publié en décembre 2010, le CEPD a salué l'extension du mandat de l'ENISA et l'élargissement de ses tâches actuelles tel que proposé par la Commission européenne, et il a souligné le fait que la sécurité du traitement des données est un élément essentiel de la protection des données. À cet égard, il a soutenu la proposition de renforcer les compétences de l'Agence en intégrant les autorités de protection des données et les organes répressifs en tant que parties intéressées à part entière.

Le CEPD a recommandé une plus grande précision concernant l'élargissement des tâches de l'Agence afin d'éviter l'incertitude juridique et la nécessité de mettre en place des canaux de coopération solides avec les parties intéressées de l'Agence afin de garantir la cohérence et une coopération étroite.

Le CEPD a également souligné la nécessité d'intégrer les recommandations de sécurité et les bonnes pratiques dans les activités internes de l'Agence. Cela permettra à l'ENISA de mieux tester et promouvoir ces techniques auprès d'autres organes et agences.

Le nouveau règlement relatif à l'ENISA prolongera son mandat de cinq ans et renforcera ses compétences.

3.5.6. e-Justice

Le CEPD collabore étroitement avec les équipes de la Commission et du Conseil impliquées dans l'élaboration et la mise en œuvre du plan d'action e-Justice. Cette initiative vise à moderniser et à rationnaliser la façon dont les citoyens perçoivent les informations juridiques afin de leur permettre de profiter d'un «guichet unique multilingue en ligne pour l'accès aux informations en matière de justice».

Le site a été lancé en juillet 2009 avec des fonctionnalités limitées. Il devrait par la suite intégrer davantage de services conformément à la feuille de route ambitieuse fixée par le Conseil, qui prévoit notamment les fonctionnalités suivantes: services d'informations, paiements en ligne, procédure européenne d'injonction de payer, règlement des petits litiges, recherche de praticiens et recherche d'informations dans les registres publics interconnectés.

Étant donné que certains de ces services seront probablement amenés à traiter des volumes importants de données à caractère personnel, le CEPD a recommandé, dès le départ, l'inclusion de garanties adéquates de protection des données dans les instruments juridiques fournissant la base légale et dans l'infrastructure informatique assurant les services.

3.5.7. Septième programme-cadre pour la recherche et le développement technologique, y compris le projet Turbine

En appliquant les possibilités d'interaction énumérées dans son document stratégique d'avril 2008 intitulé «Le CEPD et la recherche et le développement technologique dans l'UE»([10]), le CEPD a facilité les contacts et la coopération entre les autorités nationales de protection des données et les consortiums travaillant sur des projets de recherche en 2010.

Le cas de TURBINE([11])

En 2008, après avoir analysé les éléments du projet européen «TrUsted Revocable Biometric IdeNtitiEs» (Turbine) visant à effectuer des recherches dans le domaine de la **biométrie révocable**, le CEPD a décidé de répondre favorablement à la demande d'un consortium de produire un avis sur ce projet européen([12]). Le CEPD s'est réjoui de la pertinence de ce projet pour les questions de protection des données et a considéré qu'il reflétait les priorités identifiées dans son rapport annuel.

Entre mai et octobre 2010, le consortium de projet a fourni au CEPD tous les documents pertinents

([10]) Disponible sur le site internet du CEPD, sous Publications > Documents.

([11]) www.turbine-project.eu

([12]) Voir rapport annuel 2008, p. 70.

concernant les aspects de protection des données des recherches effectuées dans le cadre du projet Turbine. Le CEPD a aussi eu plusieurs discussions avec des représentants du consortium afin d'obtenir des clarifications supplémentaires et, lorsque cela était nécessaire, des documents supplémentaires. Les maquettes développées par Turbine et mises en œuvre au cours de l'été 2010 ont été considérées comme un élément important de l'analyse. Les points essentiels de l'avis du CEPD ont été présentés à l'occasion de la dernière conférence du projet organisée à Bruxelles en janvier 2011.

Le septième programme-cadre: point de départ du principe de protection intégrée de la vie privée dès la conception des systèmes.

3.6. Coopération internationale et transferts de données

3.6.1. Dossiers passagers

En 2010, comme les années précédentes, le traitement des dossiers passagers (*Passenger Name Records*, PNR) par les autorités répressives a soulevé des questions de protection des données du point de vue de l'Europe.

En ce qui concerne **l'accord PNR conclu avec les États-Unis**, le CEPD a répété certaines préoccupations qu'il avait exprimées précédemment dans ses interventions devant la Cour de justice et dans des avis adoptés avec le groupe de travail «Article 29» et dont la version définitive de l'accord ne tenait pas suffisamment compte. Le CEPD a notamment souligné que cet accord ne se focalise pas sur les personnes présentant un risque, mais qu'il envisage plutôt la collecte massive de données à caractère personnel et une évaluation des risques appliquée à tous les individus. L'accord PNR avec l'Australie suscite par contre moins de préoccupations en matière de respect de la vie privée.

Le CEPD a également pris position concernant une proposition de la Commission visant à exposer sa **stratégie extérieure en matière de PNR**. Cette proposition décrit les principes généraux - y compris une série de normes en matière de protection des données - sur lesquels tous les accords en matière de dossiers passagers conclus avec un pays tiers devraient se baser. Dans son avis, le CEPD a salué l'approche horizontale suivie par la Commission et soutenu résolument l'objectif d'arriver à un degré élevé et uniforme de protection des données applicable à tous les mécanismes existants et futurs en matière de PNR.

Cependant, pour être acceptables, les conditions de collecte et de traitement des données PNR devraient être **considérablement restreintes**. Tout comme dans le cas de l'accord PNR avec les États-Unis, le CEPD était particulièrement inquiet de **l'utilisation des mécanismes d'échange de dossiers passagers pour l'évaluation des risques et le profilage**. Il a exprimé de sérieuses inquiétudes quant à la **nécessité et à la légitimité** de certains aspects importants des mécanismes proposés. Selon lui, l'utilisation proactive des données PNR de tous les passagers à des fins d'évaluation des risques nécessite des justifications et des garanties plus explicites.

En ce qui concerne le contenu des normes proposées de protection des données, le CEPD a appelé à **davantage de précision** concernant les **normes minimales** applicables à tous les accords PNR. Des conditions plus strictes devraient s'appliquer notamment au traitement des données sensibles, aux conditions des transferts ultérieurs et à la conservation des données. Le CEPD a également souligné la nécessité, dans tout accord PNR, de conférer aux personnes des **droits directement exécutoires**.

Les données à caractère personnel de tous les passagers sont utilisées à des fins d'évaluation des risques. Cette approche pose de sérieux problèmes de nécessité et de proportionnalité.

3.6.2. Programme de surveillance du financement du terrorisme (TFTP)

Le CEPD a exprimé de vives inquiétudes concernant le projet d'accord de la Commission européenne avec les États-Unis relatif au programme de surveillance du financement du terrorisme (TFTP). Cet **accord** permet aux autorités américaines, dans leurs enquêtes antiterroristes, d'accéder aux données financières d'origine européenne gérées par la société belge **SWIFT**. Après la décision du Parlement européen d'opposer son veto à l'accord provisoire au milieu du mois de février, le nouveau projet devait apaiser les préoccupations en matière de vie privée et de protection des données.

*Le CEPD a considéré qu'il n'y a **pas encore de preuves suffisantes** démontrant la **nécessité et la proportionnalité** d'un accord portant une telle atteinte à la vie privée, qui, à de nombreux égards, fait double emploi avec certains accords européens et internationaux antérieurs dans ce domaine.*

Le CEPD a souligné que la **nécessité** de l'accord proposé devait être établie sans équivoque, compte tenu des autres instruments existants moins invasifs en termes de respect de la vie privée (par exemple l'accord d'assistance juridique mutuelle entre l'UE et les États-Unis). Le CEPD a exprimé des préoccupations particulières relatives au projet visant à permettre des **transferts de volumes considérables de données bancaires** aux autorités américaines (transferts massifs).

Cet avis signale également les principaux éléments nécessitant une amélioration du point de vue de la protection des données, par exemple:

- veiller au remplacement des **transferts massifs** par des mécanismes permettant de filtrer les données des transactions financières dans l'UE, et de faire en sorte que seules les données pertinentes et nécessaires soient envoyées aux autorités américaines;
- diminuer considérablement le **délai de stockage** des «données non extraites» que les autorités n'ont pas consultées pour leurs enquêtes en matière de terrorisme;
- confier à une **autorité judiciaire publique** la mission qui consiste à apprécier les demandes du Trésor américain, conformément au mandat de négociation et au cadre européen actuel en matière de protection des données;
- veiller à ce que les **droits à la protection des données** des personnes concernées soient **effectivement applicables**, en particulier sur le territoire américain;
- améliorer les **mécanismes de contrôle et de suivi indépendants**

Certains de ces points ont été abordés par la Commission européenne, le Parlement européen et le Conseil dans la procédure finale. Un accord légèrement révisé est entré en vigueur le 1er août 2010.

Le CEPD a exprimé ses préoccupations concernant le projet de permettre des transferts de volumes considérables de données bancaires aux autorités américaines.

3.6.3. Accord international EU - États-Unis en matière de partage d'informations et de protection des données à caractère personnel

Le CEPD participe aux discussions relatives à la rédaction d'un accord international en matière de protection des données entre l'Union européenne et les États-Unis. Cet accord prévoirait des **garanties de haut niveau** applicables à l'échange de données personnelles dans le domaine de la **coopération policière et judiciaire en matière pénale**.

Depuis 2007, le CEPD a suivi de près le travail du Groupe de contact de haut niveau composé de représentants de l'Union et des États-Unis et a participé activement aux différentes phases des travaux préparatoires. Il a formulé un avis en novembre 2008 et participé aux réunions et à la consultation publique organisées par la Commission. En ce qui concerne le mandat de négociation élaboré par la Commission, le CEPD a soutenu l'inclusion d'exigences essentielles en matière de protection des données dans le projet, comme la clarté de finalité et le champ d'application, des dispositions relatives aux droits exécutoires des personnes concernées et une supervision indépendante.

3.6.4. Accord commercial anti-contrefaçon

Tout au long de l'année 2010, l'Union européenne a mené des négociations visant à finaliser un accord commercial international anti-contrefaçon (ACAC). Cet accord, adopté en décembre 2010, visait à renforcer l'application des droits de propriété intellectuelle, y compris sur l'internet.

Au cours de ces négociations, vivement critiquées pour leur manque de transparence, il est apparu que certaines dispositions du projet d'accord étaient peut-être contraires aux droits des personnes au respect de la vie privée et à la protection des données.

Le CEPD, qui n'avait jamais été consulté à ce sujet, s'est inquiété tout particulièrement des dispositions prévues de l'ACAC légitimant un **contrôle à grande échelle des utilisateurs d'internet** et de l'obligation faite aux fournisseurs d'accès à l'internet d'adopter des «**politiques de déconnexion d'internet en trois temps**»([13]).

([13]) Ces politiques prévoient typiquement la suppression de l'accès à l'internet après des avertissements préalables pour partage ou téléchargement allégué de contenus protégés par les droits d'auteur.

Le CEPD s'est tout particulièrement inquiété des dispositions de l'ACAC prétendant légitimer un contrôle à grande échelle des utilisateurs de l'internet.

Pour apaiser ces inquiétudes, le CEPD a adopté en février 2010 un avis comportant les recommandations suivantes:

- **examiner des moyens moins intrusifs de combattre le piratage sur l'internet**: le CEPD a estimé que les politiques basées sur l'approche «trois infractions» ne sont pas nécessaires pour atteindre l'objectif du respect des droits de propriété intellectuelle. Il a demandé d'envisager des solutions moins intrusives ou, à tout le moins, de réduire la portée du contrôle envisagé et de lui préférer un contrôle ciblé.

- **appliquer des garanties adéquates à tous les transferts de données dans le contexte de l'ACAC**: dans la mesure où l'ACAC implique des échanges internationaux de données à caractère personnel entre des autorités et/ou des organisations privées basées dans les pays signataires, le CEPD a demandé à l'UE de mettre en œuvre des mesures de garantie adéquates pour tous les transferts de données réalisés dans le cadre de l'ACAC. Ces garanties devraient prendre la forme d'accords contraignants entre les expéditeurs (UE) et les destinataires dans les pays tiers.

3.7. Fiscalité et douanes

3.7.1. Coopération en matière fiscale

Le premier avis formulé par le CEPD en 2010 portait sur une proposition de la Commission visant à améliorer la coopération administrative entre les États membres dans le domaine fiscal. Cette proposition portait sur les impôts indirects mais ne couvrait pas la TVA ni les droits d'accises, qui sont régis par d'autres instruments législatifs.

L'un des principaux objectifs de la proposition était d'améliorer l'échange d'informations entre les États membres. Dans la plupart des cas, il s'agissait d'informations concernant des personnes physiques. Les règles en matière de protection des données étaient donc d'application.

Dans son avis publié en janvier 2010, le CEPD a déclaré que la proposition de la Commission était un bon exemple du **manque de sensibilisation aux exigences en matière de protection des données**, puisque la question de la protection des données avait été presque entièrement ignorée. De ce fait, la proposition contenait plusieurs éléments contraires aux exigences en matière de protection des données. Ces lacunes sont mises en évidences et débattues dans l'avis du CEPD.

Parmi d'autres remarques, le CEPD a invité le législateur à définir plus clairement la responsabilité de la Commission en ce qui concerne la maintenance et la sécurité du réseau prévu pour l'échange d'informations. Il a également demandé au législateur de spécifier les informations personnelles susceptibles d'être échangées, de mieux définir les finalités de l'échange d'informations et d'évaluer la nécessité des transferts, ou du moins de veiller au respect du principe de nécessité.

3.7.2. Coopération douanière UE-Japon

En février 2010, la Commission a adopté une proposition de décision du Conseil relative à une position à prendre par l'Union au sein du comité mixte de coopération douanière UE- Japon concernant la reconnaissance mutuelle des programmes relatifs aux opérateurs économiques agréés dans l'Union européenne et au Japon([14]). L'article IV de l'annexe de cette proposition concerne les **échanges d'informations et la communication**. Cette annexe prévoit l'échange systématique par voie électronique d'informations et de données connexes concernant notamment les membres du programme.

La directive 95/46/CE et le règlement (CE) n° 45/2001 contiennent des règles similaires, en leurs articles 25-26 et 9 respectivement, concernant les flux transfrontaliers de données à caractère personnel. Le principe énoncé dans ces textes est que des **données à caractère personnel ne peuvent être transférées** d'un État membre à un pays tiers **que si ce pays tiers** assure une **protection adéquate** (ou si des garanties adéquates sont adoptées, ou encore dans les cas où l'une des exceptions prévues est d'application).

Même si le projet d'exposé des motifs de cette proposition affirme que le régime japonais de protection est adéquat, la procédure fixée par la directive pour déterminer qu'un pays tiers garantit un degré de protection adéquat n'a pas été respectée. Par conséquent, la déclaration faite dans le projet d'exposé des motifs est contraire à la directive.

([14]) COM(2010)55 final

Le CEPD recommande par conséquent de supprimer la déclaration d'adéquation du régime japonais au point 5(1) du projet d'exposé des motifs, puisque cette déclaration ne respecte pas les exigences du règlement (CE) n° 45/2001 et de la directive 95/46/CE. Il a également recommandé d'explorer les différentes possibilités offertes par le règlement et la directive afin d'assurer le respect des règles en matière de transferts internationaux.

3.8. Accès public, y compris les procédures judiciaires

3.8.1. Accès public aux documents contenant des données à caractère personnel

Depuis le début de ses activités, le CEPD a toujours géré la relation parfois compliquée entre les règles européennes en matière **d'accès public aux documents** et les règles européennes en matière **de protection des données**. Pour ce faire, le CEPD a tout d'abord proposé des orientations aux institutions de l'UE. En 2005, par exemple, le CEPD a publié un document de référence sur ce sujet intitulé «Accès du public aux documents et protection des données», contenant des lignes directrices destinées aux institutions et organes de l'UE.

Le CEPD a également défendu son approche en tant que partie intervenante dans la principale affaire portant sur ce sujet: *Bavarian Lager / Commission*. Dans cette affaire une personne avait demandé l'accès public au procès-verbal d'une réunion de la Commission, y compris les noms des participants. L'accès à ces noms lui avait été refusé en vertu des règles sur la protection des données. Le Tribunal a suivi la position du CEPD, mais la Cour de justice, dans son arrêt du 29 juin 2010, en appel, a annulé l'arrêt du Tribunal et adopté une interprétation différente des règles européennes applicables.

Une partie de l'analyse présentée dans le document de référence de 2005 n'est désormais plus valide à la lumière de la décision de la Cour. C'est pourquoi le CEPD a préparé un bref document supplémentaire à ce sujet, finalisé et publié début 2011.

L'adoption d'une approche proactive réduit le nombre des situations dans lesquelles les institutions doivent décider de divulgations publiques dans une demande d'accès public, comme ce fut le cas dans l'affaire *Bavarian Lager*. Ce document donne des conseils sur la façon de conserver un juste équilibre, à la fois dans les situations proactives et réactives.

> Dans ce document supplémentaire, le CEPD souligne la nécessité d'une **approche proactive** dans ce domaine. En bref, cela signifie que les institutions doivent indiquer clairement aux personnes concernées, avant la collecte de leurs données personnelles ou au plus tard au moment de celle-ci, dans quelle mesure le traitement de ces données comporte ou est susceptible de comporter une divulgation publique. Le CEPD est d'avis que les institutions sont tenues d'agir de la sorte par respect des bonnes pratiques.

Plusieurs affaires judiciaires en cours ont été suspendues dans l'attente de l'arrêt *Bavarian Lager*. Toutes ces affaires ont redémarré après l'arrêt de la Cour de juin 2010. Le CEPD est intervenu dans plusieurs de ces affaires. Dans les cas où cela s'avérait pertinent, le CEPD en a profité pour exprimer son point de vue concernant l'application à ces autres situations de l'arrêt rendu par la Cour dans l'affaire *Bavarian Lager*. Le CEPD a également apporté une contribution de ce type à une nouvelle procédure dans ce domaine.

L'arrêt Bavarian Lager a aussi entraîné le rejet de la première action lancée à l'encontre du CEPD devant le Tribunal.

3.8.2. Autres actions en justice

Un autre arrêt impliquant le CEPD a été rendu le 15 juin 2010 par le Tribunal de la fonction publique dans l'affaire *Pachtitis / Commission*. Cette affaire portait, entre autres, sur le refus de la Commission de donner au demandeur l'accès aux questions d'un test d'accès auquel il avait participé. Le CEPD est intervenu parce que les règles en matière de traitement des données avaient été invoquées et que ce dossier soulevait une question intéressante concernant la portée du droit d'accès d'une personne à ses propres données personnelles. Le CEPD est intervenu aux côtés du requérant. Celui-ci a obtenu gain de cause, mais la question relative à la protection des données n'a pas été résolue. C'est pourquoi le CEPD s'est retiré de l'appel interjeté par la suite par la Commission devant le Tribunal.

En juillet 2010, le Tribunal de la fonction publique a invité le CEPD à intervenir dans une affaire concernant le transfert de données médicales entre deux

institutions de l'Union européenne. C'est la première fois que le CEPD était invité par le Tribunal à intervenir dans une affaire. Le CEPD a accepté l'invitation et préparé un mémoire en intervention dans lequel il clarifiait les dispositions applicables du règlement relatif à la protection des données.

3.9. Autres questions diverses

3.9.1. Système d'information sur le marché intérieur

EEn juillet 2010, le CEPD a adressé un courrier à la direction générale «Marché intérieur et services» de la Commission (DG MARKT). Dans ce courrier, le CEPD a fait le point des réalisations et des progrès encore à faire sur les points mentionnés dans le rapport de la Commission sur l'état de la protection des données dans le système d'information sur le marché intérieur (IMI).

L'IMI est une application en ligne qui permet aux États membres de coopérer les uns avec les autres afin d'améliorer la mise en œuvre de la législation relative au marché intérieur. Cette coopération nécessite également d'enregistrer et d'échanger certaines données à caractère personnel. L'IMI permet notamment aux autorités nationales, régionales et locales des États membres de l'UE de communiquer rapidement et facilement avec leurs homologues dans d'autres pays européens. L'IMI aide les utilisateurs à trouver le bon contact dans les autorités publiques d'un autre pays et à communiquer avec lui au moyen d'un ensemble prétraduit de questions et réponses normalisées. L'IMI est conçu comme un système flexible pouvant servir différents éléments de la législation relative au marché intérieur.

Le CEPD a salué les progrès accomplis jusqu'à présent et encouragé la Commission à mettre en œuvre des **garanties supplémentaires**, dans le respect des principes du **respect de la vie privée dès la conception**, et à poursuivre si nécessaire sa coopération avec les autorités de protection des données des États membres. Il est important de noter que le CEPD a également invité la Commission à adopter un nouvel instrument législatif, de préférence dans le cadre de la procédure législative ordinaire, afin de mettre en place un cadre plus complet de protection des données pour l'IMI et de garantir la sécurité juridique et un degré plus élevé de protection des données.

À la veille de l'élargissement de l'IMI, une base juridique solide et des garanties supplémentaires en matière de protection des données sont nécessaires.

3.9.2. Scanners de sûreté

En février 2010, un représentant du CEPD a visité le site d'essai d'un scanner de sûreté à l'aéroport de Schiphol, aux Pays-Bas. L'objectif de cette visite était d'obtenir des informations complémentaires sur la «deuxième génération de systèmes» visant à améliorer la protection des données et à mettre en œuvre le principe de respect de la vie privée dès la conception.

En juillet 2010, le CEPD a formulé des observations[15] sur la communication relative à l'utilisation de scanners de sûreté dans les aéroports adoptée par la Commission en juin[16].

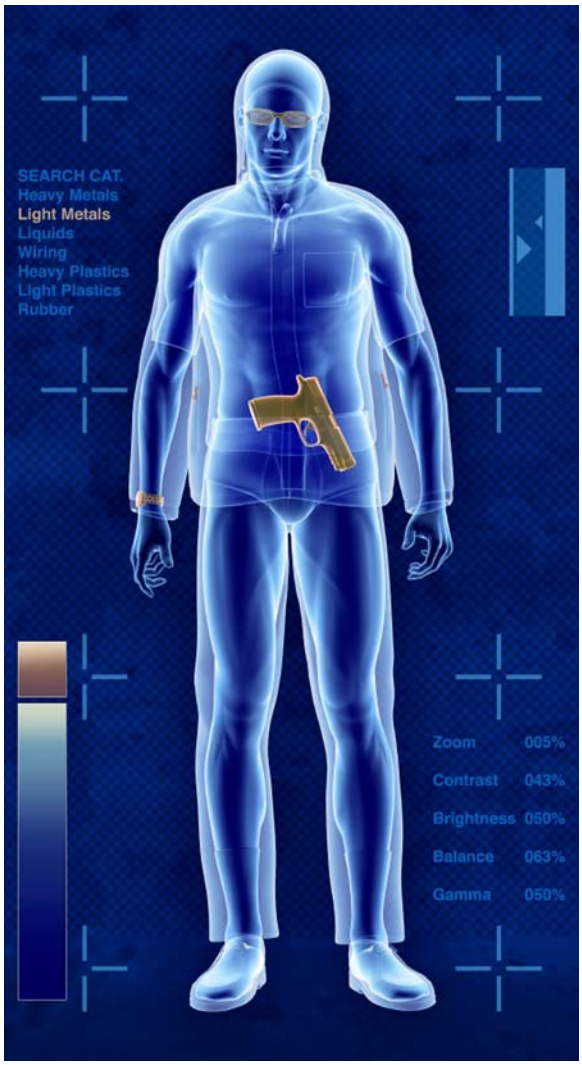
> Dans ces observations, le CEPD a souligné que le **consentement** ne devrait **pas** servir à légitimer le traitement de données à caractère personnel en l'absence d'une base juridique autorisant ce traitement.

Il a également souligné que, dans le cas des scanners de sûreté, les «**meilleures techniques disponibles**» désigneraient le stade le plus efficace et le plus avancé dans le développement des activités et de leurs méthodes de fonctionnement, indiquant l'adéquation pratique de techniques particulières à fournir un seuil de détection bien défini et conforme au cadre européen de respect de la vie privée et de protection des données.

Le CEPD continuera de suivre de près les évolutions législatives et techniques liées aux scanners de sûreté et apportera une contribution adéquate aux nouvelles mesures que la Commission européenne compte adopter en 2011.

(15) http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-07-01_Security_scanners_EN.pdf

(16) Communication COM (2010) 311 final



Des scanners corporels aux scanners de sûreté, la solution réside dans le respect de la vie privée dès la conception.

3.9.3. Systèmes de garantie des dépôts

Les systèmes de garantie des dépôts remboursent leurs dépôts aux déposants à hauteur d'un maximum de 100 000 euros en cas de faillite d'un établissement de crédit. Les règles européennes relatives à ces systèmes existent depuis 1994. Cet instrument a été renforcé peu après l'éclatement de la crise financière en 2008. En juillet 2010, la Commission a présenté une autre proposition visant à simplifier et à harmoniser les règles nationales pertinentes en la matière.

Le remboursement des dépôts via ces systèmes de garantie nécessite de traiter les données des déposants. Les règles en matière de protection des données sont donc applicables, pour autant que ces déposants soient des personnes physiques. Les données sont échangées entre un établissement de crédit et un système de garantie des dépôts, mais aussi entre les différents systèmes de garantie des dépôts, que ce soit au sein d'un même État membre ou entre différents États membres.

Le CEPD a publié un bref avis concernant cette proposition en septembre 2010. Dans cet avis, le CEPD se dit généralement satisfait de la façon dont la proposition aborde les aspects liés à la protection des données. Par exemple, la proposition vise à ce que les données personnelles concernées ne soient utilisées qu'aux fins pour lesquelles elles ont été échangées, à savoir le remboursement des dépôts.

Le CEPD se réjouit particulièrement du fait que les données ne peuvent être utilisées que sous une forme anonyme pour la réalisation des «simulations de crise». Au moment de la rédaction de cette proposition, le CEPD avait de fait mis en doute la nécessité d'utiliser des données personnelles pour la réalisation de ces tests.

3.9.4. Initiative citoyenne

L'initiative citoyenne est l'une des innovations introduites par le traité de Lisbonne. Elle permet à des citoyens de l'Union, au nombre d'un million au moins et ressortissants d'un nombre significatif d'États membres, d'inviter la Commission à soumettre une proposition législative sur un sujet concernant leurs intérêts. La collecte d'au moins un million de déclarations de soutien nécessite de recueillir des données personnelles.

> Dans son avis d'avril 2010, le CEPD a souligné que le respect intégral des règles relatives à la protection des données contribuerait largement à la fiabilité, à l'impact et au succès de ce nouvel instrument important.

L'une des recommandations concernait l'obligation, pour l'organisateur d'une initiative qui compte utiliser un système de collecte en ligne, de demander à l'autorité compétente de certifier la sécurité de ce système. En ce qui concerne le moment de cette requête, le CEPD a suggéré d'obliger les organisateurs à l'introduire avant de commencer à recueillir les déclarations de soutien et non après la collecte. Le CEPD a également recommandé au législateur de veiller à ce que:

- les données personnelles recueillies par l'organisateur ne puissent être utilisées à une

autre fin que le soutien indiqué de l'initiative citoyenne concernée;

- les données reçues par l'autorité compétente ne soient utilisées qu'aux fins de vérifier l'authenticité des déclarations de soutien à une initiative citoyenne donnée.

3.9.5. Enquêtes et prévention des accidents et des incidents dans l'aviation civile

L'avis du CEPD s'est concentré sur les aspects de la proposition qui ont un impact sur la protection des données à caractère personnel, y compris le **traitement des données qui figurent sur les listes de passagers ou concernent les victimes, leurs familles et les témoins**, aux différents stades de l'enquête et dans le contexte d'un échange d'informations entre les autorités responsables des enquêtes.

Le CEPD s'est réjoui que cette proposition ait pris en considération les aspects liés à la protection des données. Cependant, étant donné le **contexte spécifique** dans lequel les données à caractère personnel sont traitées, à savoir les enquêtes concernant des accidents afin d'améliorer la sécurité aérienne, il conviendrait de prendre des **mesures supplémentaires pour garantir la confidentialité des données**. Ces mesures devraient comprendre des dispositions exigeant la suppression ou l'anonymisation des données à caractère personnel le plus rapidement possible dès lors qu'elles ne sont plus nécessaires à une enquête.

Selon le CEPD, des garanties plus strictes sont nécessaires pour protéger les personnes touchées directement ou indirectement par un accident grave ou qui ont perdu des proches.

Le CEPD a notamment fait les recommandations suivantes:

- préserver par principe le caractère confidentiel de la liste des passagers, tout en donnant la possibilité aux États membres de la publier dans certains cas et sur des bases légitimes après avoir obtenu le consentement des familles;
- prévoir un délai restreint de conservation des données à caractère personnel;
- soumettre la transmission des données à caractère personnel aux représentants de pays tiers à la condition que ceux-ci présentent un niveau de protection adéquat;
- clarifier les rôles et les responsabilités de la Commission européenne et de l'AESA dans la perspective de l'application de la législation en matière de protection des données.

3.10. Un regard sur l'avenir

3.10.1. Développements technologiques

Dans des rapports annuels antérieurs([17]), le CEPD avait déjà souligné la **convergence croissante** entre le «**monde réel**» et le «monde de l'internet/numérique» ou la **société de l'information**. De fait, la distinction entre le monde physique et le monde numérique a tendance à s'estomper. Cette tendance s'est accélérée en 2010 à mesure que la convergence a été stimulée par de nouveaux outils innovants introduits à plus grande échelle. Jusqu'à présent, les individus ont pu vivre dans des réalités parallèles leur permettant de séparer leurs identités virtuelles de leur identité dans le monde réel. Cette distinction devient de moins en moins possible et, qu'il le veuille ou non, l'individu entre aujourd'hui dans un environnement sans frontière entre le monde électronique et le monde réel, mondes qui pourtant restent soumis à des cadres réglementaires différents.

Cette tendance s'est matérialisée de façon toute particulière dans les **réseaux sociaux**, qui continuent de s'étendre. La population mondiale consacre plus de 110 milliards de minutes par an à l'utilisation de ces réseaux([18]) et, pour la première fois, un réseau social est devenu le site internet le plus fréquenté aux États-Unis([19]), devant les moteurs de recherche.

([17]) Rapport annuel 2007, p. 56, et rapport annuel 2009. p. 64.

([18]) http://blog.nielsen.Commission/nielsenwire/global/social-media-accounts-for-22-percent-of-time-online/#

([19]) http://www.hitwise.Commission/us/press-center/press-releases/facebook-was-the-top-search-term-in-2010-for-sec/

Les évolutions suivantes ont encore accentué ce phénomène:

- Les **appareils mobiles intelligents**([20]) sont l'un des piliers principaux des nouveaux ponts entre le monde physique et le monde numérique. Ils sont toujours allumés, omniprésents et capables de partager, de modifier et de traiter l'information en temps réel. Leur puissance de traitement est impressionnante et ils exploitent les ressources presque illimitées offertes par le «nuage». Ils sont capables d'enregistrer des images et des séquences vidéo à haute définition, de marquer individuellement des objets et des personnes et de relier des coordonnées géographiques à des contenus multimédias contenant des lieux, des événements et des personnes. Les utilisateurs sont connectés au réseau en permanence; ils traitent des données à caractère personnel ou leurs données à caractère personnel font l'objet de traitements.

- La **technologie de reconnaissance faciale**, limitée jusqu'à présent aux environnements contrôlés, est en plein boom et commence à être utilisée dans les réseaux sociaux et sur les téléphones intelligents. La combinaison de la force brute de millions d'utilisateurs des réseaux sociaux «armés» d'appareils mobiles intelligents téléchargeant des photos sur lesquelles ils marquent les visages des personnes augmente radicalement le champ d'application de la technologie de reconnaissance faciale et contribue même à son amélioration. Cette nouvelle tendance émergente pourrait même permettre la création de bases de données biométriques d'une ampleur sans précédent sur la base des plates-formes de réseaux sociaux.

Le concept de **réalité augmentée** basée sur des plates-formes telles que les téléphones intelligents permettra d'introduire des informations supplémentaires en ligne dans la réalité d'une personne. Il est déjà possible de visiter une ville et d'obtenir des informations supplémentaires à propos de monuments «identifiés» par des appareils mobiles intelligents. En conjonction avec la reconnaissance faciale et les réseaux sociaux décrits ci-dessus, il sera très bientôt possible de prendre la photo de quelqu'un dans la rue et d'obtenir des informations détaillées sur cette personne en temps réel.

À l'avenir, la **technologie portable** constituera elle aussi un pont favorisant la fusion entre la vie physique quotidienne d'une personne et des paysages numériques qui ne sont pas nécessairement régis par le même cadre. Elle reliera des données à caractère personnel sensibles (température, pression artérielle, pouls, taux de sucre, etc.) à des applications et services en ligne.

Ces mondes sans frontière et interconnectés offrent des avantages sans précédent aux citoyens, entreprises et gouvernements, mais comportent également des **menaces sans précédent** qu'il faudra gérer de façon adéquate. Ainsi le vol **d'identité dans le monde virtuel** aura bientôt des conséquences similaires à celles du vol d'identité dans le monde réel. De ce point de vue, la disponibilité de volumes massifs de données à caractère personnel sur un réseau, le manque d'attention accordée aux failles de sécurité concernant les données à caractère personnel (qui se présentent souvent sans que nous en ayons conscience) et la disponibilité croissante de services commerciaux, publics et sociaux auxquels les identifications virtuelles donnent accès en ligne constituent un mélange potentiellement dangereux. Les identités traditionnelles «papier» ne sont plus une solution de repli satisfaisante lorsqu'une identité électronique est compromise, car ces deux identités sont de plus en plus intégrées.

Malgré cet estompement des frontières entre le monde virtuel et le monde réel, les règles en vigueur dans les deux univers ne sont pas similaires. Prenons l'exemple d'un compteur intelligent: la production, la commercialisation et l'utilisation d'un compteur électrique font l'objet d'une série de règles spécifiques visant à protéger le consommateur; cependant, dès lors que ce même compteur est connecté au réseau et commence à décrire le comportement d'une personne, devenant ainsi un compteur intelligent - en enregistrant et en stockant l'heure à laquelle cette personne consomme de l'électricité, par exemple, ce qui permet de savoir si celle-ci est ou non chez elle - ces règles risquent de ne plus s'appliquer. La **révision du cadre de protection des données** pourrait être le bon moment pour aborder ces problèmes. Un cadre juridique doit contribuer à la mise en œuvre des protections nécessaires que les citoyens s'attendent à trouver dans ce nouvel environnement, qui doit être jugé fiable.

([20]) http://www.enisa.europa.eu/media/news-pictures/smartphones-video-clip

3.10.2. Priorités pour 2011

En décembre 2010, le CEPD a publié son cinquième inventaire public en tant que conseiller sur les propositions de législation de l'UE, dans lequel il fixe ses priorités en matière de consultation pour l'année suivante. Comme au cours des années précédentes, le CEPD compte donner son avis sur toutes les propositions législatives ayant un impact important sur la protection des données. Il peut aussi examiner certaines mesures non législatives, si celles-ci posent des problèmes substantiels en matière de protection des données.

Les principales priorités du CEPD, telles qu'elles sont identifiées dans son inventaire, sont les suivantes:

- *La **révision du cadre juridique en matière de protection des données**, qui sera l'une des premières priorités du CEPD en 2011.*
- *Les différentes initiatives visant à poursuivre la **mise en œuvre du programme de Stockholm dans l'espace de liberté, de sécurité et de justice**, comme la mise en place d'un système entrée-sortie et le programme des voyageurs enregistrés, la proposition de directive sur l'utilisation du PNR à des fins policières et la mise en place d'un TFTP européen. Le CEPD suivra également de près les négociations en vue d'accords de protection des données avec des pays tiers. Dernier point mais non des moindres, le CEPD participera activement à la révision de la directive sur la conservation des données.*
- *Les **initiatives dans le domaine technologique** susceptibles d'avoir un impact sur la vie privée et la protection des données à caractère personnel seront examinées de près. Le CEPD continuera de suivre la mise en œuvre de la **stratégie numérique** pour l'Europe.*
- ***Toutes les autres initiatives** susceptibles d'avoir un impact important sur la protection des données, comme les initiatives dans le domaine des **transports** (par ex. utilisation de scanners corporels dans les aéroports, série de mesures sur la mobilité virtuelle) et les échanges de données à grande échelle susceptibles d'avoir lieu dans le Système d'information sur le marché intérieur.*

4 COOPÉRATION

4.1. Groupe de travail «Article 29»

Le groupe de travail «Article 29» est un organe consultatif indépendant institué par l'article 29 de la directive sur la protection des données (95/46/CE). Il fournit à la Commission européenne des conseils indépendants en matière de protection des données et contribue au développement de politiques harmonisées de protection des données dans les États membres de l'UE([21]).

Sa mission, décrite à l'article 30 de la directive, peut être résumée comme suit:

- donner à la Commission européenne, au nom des États membres, un avis autorisé sur les questions relatives à la protection des données;
- promouvoir l'application uniforme des principes généraux de la directive dans tous les États membres par la coopération entre les autorités de contrôle compétentes en matière de protection des données;
- conseiller la Commission à propos de toute espèce de mesure ayant une incidence sur les droits et libertés des personnes physiques eu égard au traitement des données à caractère personnel;
- formuler des recommandations destinées au grand public, et en particulier aux institutions de l'UE, sur toute question concernant la protection des personnes à l'égard du traitement des données à caractère personnel dans l'Union européenne.

([21]) Le Groupe de travail est composé de représentants des autorités nationales de contrôle de chaque État membre, d'un représentant de l'autorité créée pour les institutions et les organismes de l'Union (c'est-à-dire le CEPD) et d'un représentant de la Commission. Cette dernière assure également le secrétariat du groupe. Les autorités nationales de contrôle de l'Islande, de la Norvège et du Liechtenstein (partenaires EEE) sont représentées en tant qu'observatrices.

Le CEPD, membre du groupe de travail «Article 29» depuis 2004, estime qu'il s'agit là d'un forum très important pour la coopération avec les autorités nationales de contrôle. Il est par ailleurs bien clair que le groupe devrait jouer un rôle central dans la mise en œuvre homogène de la directive et l'interprétation de ses principes généraux.

En 2010, le groupe de travail a concentré ses activités sur quatre thèmes stratégiques principaux définis dans son programme de travail 2010-2011, à savoir:

- mettre en œuvre la directive et préparer un cadre juridique complet pour l'avenir;
- faire face à la mondialisation;
- réagir aux défis technologiques;
- renforcer l'efficacité du groupe de travail et des autorités de protection des données.

À cette fin, le groupe a adopté divers documents, parmi lesquels:

- l'avis 2/2010 sur la **publicité comportementale en ligne** (WP 171);

- l'avis 5/2010 sur la proposition des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des **applications RFID** (WP 175);

- l'avis 7/2010 sur la communication de la Commission européenne relative à la **démarche globale en matière de transfert des données des dossiers passagers** (PNR) aux pays tiers (WP 178)

Le groupe de travail et le CEPD ont collaboré étroitement dans des dossiers liés à la mise en œuvre de la directive 95/46/CE et à l'interprétation de certaines de ses dispositions essentielles. Le CEPD a apporté une contribution active dans différents domaines, par exemple:

- l'avis 1/2010 sur les notions de «**responsable du traitement**» et de «**sous-traitant**» (WP 169)

- l'avis n° 3/2010 sur le **principe de la responsabilisation** (WP 173);

- l'avis 8/2010 sur le **droit applicable** (WP 179);

Le CEPD coopère également avec les autorités nationales de contrôle dans la mesure nécessaire à l'accomplissement de leurs devoirs respectifs, notamment en échangeant toutes informations utiles, en leur demandant ou leur fournissant une aide à l'accomplissement de leurs fonctions (article 46, point f), tiret i, du règlement). Cette coopération se fait au cas par cas.

La coopération directe avec les autorités nationales est un élément d'importance croissante dans le contexte du développement de grands systèmes internationaux tels qu'Eurodac, qui requièrent une approche coordonnée du contrôle (voir points 4.2 et 4.3).

4.2. Supervision coordonnée d'Eurodac

La supervision efficace d'Eurodac repose sur une coopération étroite entre les autorités nationales de protection des données et le CEPD.

Le groupe de coordination du contrôle d'Eurodac - composé de représentants des autorités nationales chargées de la protection des données et du CEPD - a basé ses activités sur la mise en œuvre du programme de travail adopté début 2010.

Ce programme de travail porte sur différentes questions tout en mettant l'accent sur les problèmes communs ou sensibles face auxquels le groupe peut apporter une valeur ajoutée et jouer un rôle déterminant. Plusieurs activités dépendent cependant de l'adoption des nouveaux règlements Eurodac/Dublin. Elles seront effectuées au moment opportun.

Les activités du groupe sont désormais organisées selon un calendrier permettant une meilleure planification. Les travaux à accomplir ces prochaines années sont répartis en activités à mettre en œuvre:

- tous les quatre ans: par exemple, un audit de sécurité complet doit être réalisé par les autorités de protection des données au niveau national et au niveau de l'UE. La préparation coordonnée de cet audit par le groupe permettra une plus grande efficacité et des résultats plus comparables;

- tous les deux ans; par exemple, des inspections coordonnées. Cela nécessite de préparer et d'effectuer des inspections coordonnées à intervalles réguliers;

- annuellement: des activités plus courtes d'établissement des faits, avec une portée plus limitée que les inspections coordonnées, seront entreprises en fonction des besoins identifiés par le groupe;

- en permanence: il s'agit principalement des activités de suivi nécessaires au niveau structurel, comme le suivi des évolutions législatives et politiques, des recherches spéciales et des recommandations antérieures.

Au sein de ces catégories, plusieurs types d'activités ont été sélectionnés et lancés en 2010.

Le groupe s'est réuni à trois reprises à Bruxelles en mars, octobre et décembre 2010. Lors de la réunion de mars, le Groupe a réélu M. Peter Hustinx (CEPD) à sa présidence et élu Mme Elisabeth Wallin (de l'autorité suédoise de protection des données) vice-présidente.

Le groupe a entamé les **travaux préparatoires de l'audit complet de sécurité**. Un sous-groupe a été désigné et a entamé les travaux en identifiant les délicats, comme la rédaction d'une liste d'objectifs de sécurité. Ce sous-groupe a également travaillé sur les défis liés à la nécessité de fournir des résultats comparables. Ce travail se poursuivra en 2011.

Une **nouvelle inspection coordonnée** a été lancée fin 2010. Le groupe a sélectionné la question de la suppression anticipée de données et discuté d'un questionnaire et d'une méthodologie. Les résultats sont attendus pour 2011. La question de la suppression anticipée de données a été jugé importante étant donné son incidence sur la qualité des données contenues dans Eurodac et sur la protection des personnes qui ne devraient plus figurer dans la base de données.

L'interaction avec les parties intéressées a connu un début très positif lors de la réunion de décembre, à laquelle ont participé des représentants du Haut-commissariat des Nations unies pour les réfugiés et du Conseil européen pour les réfugiés et les exilés. Les parties intéressées extérieures ont présenté leurs travaux et leurs priorités et échangé leurs points de vue avec le groupe sur des questions telles que l'avenir du système de Dublin, les informations à communiquer aux demandeurs d'asile ou la défense de leurs droits. Les parties intéressées ont également expliqué leurs objections à la possibilité de donner aux autorités répressives un accès à Eurodac. Cet échange de points de vue s'est révélé extrêmement utile et devrait se répéter régulièrement.

Le contrôle coordonné d'Eurodac est crucial pour protéger les droits des personnes vulnérables que sont par exemple les demandeurs d'asile.

4.3. Supervision du système d'information douanier (SID)

Le Système d'information douanier (SID) a pour objectif de créer un système d'alerte dans le cadre de la lutte antifraude afin de permettre aux États membres qui introduisent des données dans le système de demander à un autre État membre de procéder à une détection et un signalement, une surveillance discrète, un contrôle spécifique ou une analyse opérationnelle et stratégique.

Le SID enregistre des informations relatives aux produits de base, aux moyens de transport, aux personnes et aux entreprises, aux marchandises et aux liquidités détenues, saisies ou confisquées afin d'aider à prévenir, à rechercher et à poursuivre les opérations qui sont contraires aux réglementations douanière ou agricole. Ce dernier aspect est contrôlé par une autorité de contrôle commune composée de représentants des autorités nationales de protection des données.

Le groupe de coordination du contrôle du SID est conçu comme une plate-forme dans laquelle les autorités responsables du contrôle du SID en vertu du règlement (CE) n° 766/2008([22]) - à savoir le CEPD et les autorités nationales de protection des données - collaborent dans le respect de leurs priorités afin de garantir un contrôle coordonné du SID.

Ce groupe de coordination:

a) analyse les problèmes de mise en œuvre liés aux activités du SID;

b) analyse les difficultés rencontrées lors des vérifications par les autorités de contrôle;

c) analyse les difficultés d'interprétation ou d'application du règlement SID;

d) formule des recommandations en vue d'apporter des solutions communes aux problèmes existants; et

e) s'efforce d'améliorer la coopération entre les autorités de contrôle.

En 2010, le CEPD a organisé deux réunions du groupe de coordination du contrôle du SID (en mars et en décembre). Cette réunion a rassemblé les représentants des autorités nationales chargées de la protection des données ainsi que des représentants de l'Autorité de contrôle commune des douanes et du secrétariat chargé de la protection des données.

Lors de la réunion de décembre, ce groupe a adopté le règlement qui régira ses travaux futurs relatifs au SID et discuté des mesures à prendre éventuellement en 2011-2012 afin de garantir un contrôle global de la protection des données dans ce système.

4.4. Coopération policière et judiciaire: coopération avec les ACC et le GTPJ

Le CEPD coopère également avec les autorités chargées du contrôle de certains organes ou de certains systèmes informatiques à grande échelle de l'UE, comme les autorités de contrôle communes d'Europol et d'Eurojust et les autorités de contrôle communes pour le système d'information Schengen et les anciens aspects du «troisième pilier» du Système d'information douanier (CIS). Cette coopération prend la forme d'échanges d'informations réciproques sur des points présentant un intérêt commun, comme dans les cas où le CEPD et les ACC contrôlent chacun une partie différente d'un même système.

([22]) Règlement (CE) n° 766/2008 du Parlement européen et du Conseil du 9 juillet 2008 modifiant le règlement (CE) no 515/97 du Conseil relatif à l'assistance mutuelle entre les autorités administratives des États membres et à la collaboration entre celles-ci et la Commission en vue d'assurer la bonne application des réglementations douanière et agricole

En 2010, cette coopération a principalement porté sur le SID. Étant donné que le CEPD et l'ACC du SID partagent un rôle de contrôle dans le même système, il est logique de coordonner autant que possible leurs activités. Dans cet esprit, le CEPD a invité des représentants de l'ACC à participer aux réunions organisées à propos du contrôle coordonné du SID (voir point 4.3).

Le CEPD participe également aux réunions et aux activités du groupe de travail sur la police et la justice (GTPJ). Le GTPJ a travaillé sur plusieurs dossiers en 2010, comme le développement d'une politique commune de contrôle ou les accords «de type Prüm» (accords bilatéraux d'échange de données). Le GTPJ a également collaboré avec le groupe de travail «Article 29» pour formuler une «contribution commune des autorités européennes de protection des données» représentées dans ces groupes de travail sur l'accord UE - États-Unis en matière de protection des données. Ce travail a illustré la nécessité d'une collaboration poussée entre les deux groupes dans un contexte où la distinction entre les anciens premier et troisième piliers devient moins pertinente.

Enfin, le GTPJ a abordé le sujet de son propre avenir à la lumière des évolutions mentionnées ci-dessus et au vu de l'implication croissante du groupe de travail "Article 29" dans des domaines traditionnellement traités par le GTPJ.

4.5. Conférence européenne

Les autorités chargées de la protection des données des États membres de l'UE et le Conseil de l'Europe se rencontrent annuellement lors d'une conférence de printemps, pour discuter de questions d'intérêt commun ainsi que pour échanger des informations et faire part de leur expérience sur différents sujets.

La Conférence européenne des commissaires à la protection des données s'est tenue à **Prague les 29 et 30 avril 2010** sur le thème «*Weighing up the past, thinking of the future*» (Évaluer le passé, imaginer l'avenir). Cette conférence a été accueillie par l'autorité tchèque chargée de la protection des données.

Elle comprenait des séances consacrées à différents sujets, par exemple: 1) L'internet des objets; contrôle omniprésent dans l'espace et le temps - avec une présentation par le Contrôleur adjoint; 2) Les enfants face aux toiles d'araignées des réseaux 3) La protection des données à caractère personnel à la croisée des chemins - avec une présentation par le CEPD; 4) Le secteur public: partenaire respecté ou sous-traitant privilégié?

Comme on pouvait s'y attendre, le **futur cadre en matière de protection des données** actuellement en préparation par la Commission européenne a été au cœur des discussions. Plusieurs résolutions ont été adoptées, concernant notamment:

- l'accord envisagé entre l'Union européenne et les États-Unis sur les normes de protection des données dans le domaine de la coopération policière et judiciaire en matière pénale;
- les scanners corporels;
- la protection des enfants;
- l'avenir du respect de la vie privée.

4.6. Conférence internationale

Les autorités chargées de la protection des données et les commissaires à la protection de la vie privée d'Europe et d'autres régions du monde, notamment le Canada, l'Amérique latine, l'Australie, la Nouvelle-Zélande, Hong Kong, le Japon et d'autres territoires de la région Asie-Pacifique, se réunissent tous les ans à l'automne depuis plusieurs années.

Cette année, la conférence internationale des commissaires à la protection des données a été organisée par l'autorité israélienne de protection des données et s'est tenue à **Jérusalem du 26 au 29 novembre 2010**. Son thème central était intitulé «Vie privée: générations».

Plusieurs sessions plénières ont été organisées pour traiter des questions suivantes:

- Où en sommes-nous aujourd'hui? Le glissement intergénérationnel en matière de perception de la vie privée;
- À l'ordre du jour de la réglementation: le point de vue des régulateurs;

- Respect de la vie privée dès la conception (*Privacy by Design*);

- L'avenir du respect de la vie privée: incidence des normes de respect de la vie privée sur la réglementation.

Cette conférence a également analysé plus en profondeur les perspectives des différentes générations concernant la vie privée et la protection des données. Un des thèmes importants abordés au cours de cette conférence a été la façon dont les lois et les mécanismes d'autorégulation influencent la technologie, et inversement. L'émergence des réseaux sociaux a aussi été au cœur de la conférence.

Le CEPD et le Contrôleur adjoint ont fait des présentations et présidé différentes séances lors de cette conférence.

La séance à huis clos des commissaires a adopté plusieurs résolutions, dont la plus importante est un appel à l'organisation d'une conférence intergouvernementale en vue d'élaborer un instrument international contraignant sur le respect de la vie privée et la protection des données à caractère personnel.

La 33ème conférence internationale aura lieu au Mexique en novembre 2011.

4.7. Organisations internationales (atelier de Florence)

En collaboration avec l'Université européenne, le CEPD a organisé le 3ème atelier sur la protection des données dans les organisations internationales. Cet atelier a été organisé à Florence du 27 au 28 mai 2010. Il a rassemblé des organisations internationales importantes telles que le HCR, l'OMD, l'OIM, la CPI et bien d'autres encore. Les discussions ont abordé différents problèmes rencontrés par les organisations internationales qui s'efforcent d'assurer un bon niveau de protection des données dans des contextes parfois difficiles et sans base juridique claire. Les organisations qui ont déjà atteint un degré élevé de protection des données ont souligné les nombreux avantages que celle-ci apporte à leurs activités principales (notamment la sécurité des données et la légitimité).

À l'issue de cet atelier, le CEPD a fait circuler un questionnaire visant à faire le point des mécanismes de protection des données (ou de leur absence) au sein des organisations internationales participantes. L'accent a été mis sur la façon d'assurer une protection des données réelle et effective plutôt que sur des mécanismes législatifs spécifiques.

C'est pourquoi ce questionnaire se base sur les travaux déjà réalisés dans les forums internationaux de protection des données sur la notion de responsabilité en tant qu'outil permettant d'encourager les contrôleurs des données à réduire le risque de non-conformité en adoptant des mécanismes pratiques pour une protection efficace des données. Ce concept est particulièrement bien adapté dans le contexte des organisations internationales, puisqu'il s'applique quel que soit l'environnement juridique dans lequel les données sont traitées.

Les réponses serviront de base pour les actions futures dans ce contexte. De nombreux participants ont exprimé clairement le souhait de voir des ateliers de ce type organisés de façon régulière à l'avenir.

5 COMMUNICATION

5.1. Introduction

L'information et la communication jouent un rôle essentiel pour assurer la **visibilité** des principales activités du CEPD, mieux faire entrevoir le travail accompli par ce dernier et accroître la sensibilisation à la protection des données en général. Cet aspect est d'autant plus important qu'il est nécessaire de sensibiliser davantage au rôle et à la mission du CEPD au niveau européen, même si des progrès significatifs ont déjà été réalisés dans ce sens. Des indicateurs tels que le nombre des demandes d'information soumises par les citoyens de l'UE, le nombre des enquêtes des médias et des demandes d'entretien, le nombre des abonnés à la newsletter, ainsi que le nombre des invitations à venir s'exprimer à des conférences et le trafic sur le site internet, montrent bien que le CEPD est devenu un point de référence pour les questions de protection des données au niveau de l'Union européenne.

La visibilité accrue du CEPD dans le paysage institutionnel a une pertinence particulière pour ses trois principaux rôles, à savoir le rôle de supervision à l'égard de l'ensemble des institutions et des organes communautaires procédant à des traitements de données à caractère personnel, le rôle consultatif vis-à-vis des institutions (Commission, Conseil et Parlement) intervenant dans la conception et l'adoption de nouveaux instruments législatifs et de nouvelles politiques susceptibles d'avoir un effet sur la protection des données à caractère personnel, et enfin le rôle de coopération avec les autorités nationales de supervision et les divers organes de supervision dans le domaine de la sécurité et de la justice.

En 2010, le CEPD a poursuivi ses activités visant à améliorer encore sa communication et ses outils d'information. L'introduction de l'allemand en tant que troisième langue en complément de l'anglais et du français pour les communiqués de presse et autres activités de communication a représenté une évolution majeure à cet égard. Cela est d'autant plus important que l'allemand est la langue maternelle parlée par le plus grand nombre de personnes dans l'Union européenne. L'objectif global est donc d'atteindre un public plus large et de donner à la presse et aux citoyens germanophones la possibilité de suivre les activités du CEPD dans leur propre langue.

5.2. Caractéristiques de la communication

La politique de communication du CEPD doit être conçue en fonction de caractéristiques particulières pertinentes du point de vue de l'âge, de la taille et des compétences de l'institution. Il convient donc de suivre une stratégie sur mesure et d'avoir recours aux outils les plus appropriés pour cibler les publics concernés, ces outils devant pouvoir être adaptés à un certain nombre de contraintes et d'exigences.

5.2.1. Principaux publics et groupes cibles

À la différence de la plupart des autres institutions et organes de l'UE, dont les politiques et les activités de communication doivent être conduites à un niveau général et s'adresser à l'ensemble des citoyens de l'Union, le champ d'action direct du CEPD est beaucoup plus restreint. Il s'adresse avant tout aux institutions et aux organes européens, aux personnes concernées en général et au personnel de l'UE en particulier, aux acteurs politiques de l'UE ainsi qu'aux homologues du secteur de la protection des données. Il n'est donc pas nécessaire que la politique de communication du CEPD suive une stratégie de «communication de masse». La sensibilisation des citoyens de l'UE aux questions liées à la protection des données, au niveau des États membres, repose sur une approche plus indirecte passant par exemple par les autorités nationales chargées de la protection des données.

Le CEPD contribue toutefois lui aussi à mieux se faire connaître du grand public, notamment grâce à un certain nombre d'outils de communication (site internet, newsletter et événements de sensibilisation), en entretenant des contacts réguliers avec les parties intéressées (accueil d'étudiants dans les bureaux du CEPD, par exemple) et en participant à des événements publics, réunions et autres conférences.

5.2.2. Politique linguistique

La politique de communication du CEPD doit aussi tenir compte de la nature spécifique de son champ d'activités. Les questions liées à la protection des données peuvent être considérées comme relativement techniques et obscures pour les non-spécialistes, et le langage utilisé dans la communication doit être adapté en conséquence. S'agissant des outils d'information et de communication visant toutes sortes de public, il convient de communiquer dans un style clair et intelligible qui évite tout jargon inutile. Des efforts constants sont donc fournis dans ce sens, en particulier dans la communication envers le grand public et la presse généraliste, afin de corriger l'image excessivement «juridique» du domaine de la protection des données.

Si le public visé est plus informé (par exemple les experts de la protection des données, les acteurs de l'UE), un langage plus spécialisé est davantage justifié. Il peut donc être nécessaire d'utiliser différents styles de communication et des schémas de langage différents pour communiquer les mêmes nouvelles.

5.3. Relations avec les médias

Le CEPD doit également être aussi accessible que possible pour les journalistes, de façon à ce que le public puisse suivre son travail. Il informe régulièrement les médias au moyen de communiqués de presse, d'interviews, de discussions de fond et de conférences de presse. La gestion des demandes formulées par les médias permet de renforcer ses contacts réguliers avec ceux-ci.

5.3.1. Communiqués de presse

En 2010, le service de presse a publié 19 communiqués de presse. La plupart de ces communiqués concernent le travail du CEPD dans le domaine de la consultation et, plus spécifiquement, les **nouveaux avis législatifs** présentant un intérêt immédiat pour le grand public. Ils couvrent des thèmes tels que la stratégie européenne de réforme en matière de protection des données, les négociations relatives à l'accord commercial anti-contrefaçon (ACAC), l'accord UE - États-Unis relatif au programme de surveillance de financement du terrorisme (TFTP), la gestion de l'information dans l'espace de liberté, de sécurité et de justice, la vie privée et la confiance dans la société de l'information, la stratégie extérieure de l'Union européenne relative aux dossiers passagers, le processus d'évaluation de la directive sur la conservation des données et la stratégie de sécurité intérieure de l'Union européenne. Les arrêts pertinents de la Cour de justice de l'Union européenne ont également fait l'objet de communiqués de presse, tels l'affaire «Bavarian Lager» et l'arrêt relatif à l'indépendance des autorités chargées de la protection des données.

Des communiqués de presse ont également été diffusés concernant les **principales activités dans le domaine de la supervision**, notamment à propos de l'adoption des lignes directrices sur la vidéosurveillance et d'une politique globale en matière de supervision et de mise en application.

Les communiqués de presse sont publiés sur le site internet du CEPD et dans la base de données des communiqués de presse de la Commission européenne (RAPID) en anglais et en français. Une version allemande a été introduite en 2010, pour refléter l'introduction de l'allemand en tant que troisième langue utilisée dans les activités de communication du CEPD. Les communiqués de presse sont diffusés au sein d'un réseau régulièrement mis à jour de journalistes et de parties intéressées. Les informations fournies dans les communiqués de presse contribuent généralement à la production d'une

couverture médiatique importante par la presse générale et spécialisée. Ils sont également fréquemment publiés sur des sites internet institutionnels et non institutionnels, notamment ceux des institutions et organes de l'UE, des groupes de défense des libertés civiles, des institutions académiques et des entreprises de technologies de l'information.

5.3.2. Interviews

En 2010, le CEPD a donné environ 20 **interviews** à des journalistes de la presse écrite, de la radiotélévision et des médias électroniques en Europe, un grand nombre de demandes émanant de la presse allemande, autrichienne, néerlandaise et américaine.

Cela a donné lieu à de nombreux articles dans la presse nationale, internationale et européenne, générale ou spécialisée dans les technologies de l'information ainsi qu'à des interviews à la radio et à la télévision (par ex. télévision nationale autrichienne, radio néerlandaise et autrichienne).

Ces interviews ont abordé des questions horizontales comme les dérives vers une société de surveillance et les défis actuels et à venir dans le domaine de la protection de la vie privée et des données à caractère personnel. Ils ont également abordé des thèmes plus spécifiques qui ont fait la une des journaux en 2010, comme l'accord TFTP avec les États-Unis, la révision du cadre juridique européen en matière de protection des données et de respect de la vie privée, les inquiétudes relatives aux sites de réseaux sociaux et les applications de géolocalisation, ou encore l'utilisation des scanners corporels dans les aéroports.

5.3.3. Conférences de presse

Une conférence de presse a été organisée le 15 novembre 2010 à Bruxelles à propos de la révision des règles européennes en matière de protection des données et de respect de la vie privée. Peter Hustinx et Giovanni Buttarelli ont abordé en particulier la communication de la Commission concernant une stratégie pour renforcer les règles de l'Union en matière de protection des données, publiée début novembre 2010. Cette conférence de presse a également été l'occasion de présenter le rapport annuel 2009 du CEPD et de décrire les principaux aspects des activités du CEPD en 2009 du point de vue de ses tâches de supervision, de consultation et de coopération (voir point 5.7.1).

5.3.4. Demandes formulées par les médias

Des demandes formulées par les médias parviennent régulièrement au CEPD et comprennent

Conférence de presse du CEPD sur la révision du cadre juridique de l'UE en matière de protection des données (Bruxelles, 15 novembre 2010)

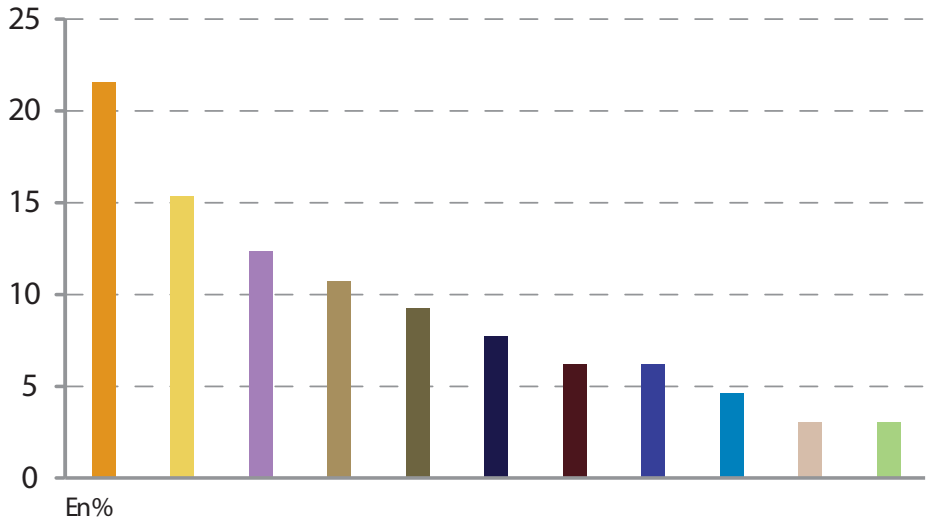
généralement des demandes de commentaires et des demandes de clarification ou d'information. En 2010, l'attention des médias s'est portée principalement sur la question de la vie privée en ligne, notamment en ce qui concerne les nouvelles applications en ligne comme les applications de géolocalisation, les moteurs de recherche et les réseaux sociaux - un domaine arrivant en tête du nombre de demandes. La presse s'est aussi beaucoup intéressée à l'accord avec les États-Unis concernant le traitement et le transfert de données financières dans le cadre du programme de surveillance du financement du terrorisme (TFTP).

Parmi les autres dossiers intéressant les médias, on peut citer la révision du cadre européen en matière de protection des données, la directive sur la conservation des données, la directive sur la vie privée dans les communications électroniques et sa disposition relative aux failles de sécurité, les activités de supervision du CEPD, y compris ses lignes directrices relatives à la vidéosurveillance, la question de la sécurité des données, les données biométriques dans les passeports et dans le système d'information Schengen, les transferts internationaux de données, y compris les décisions d'adéquation de la Commission vis-à-vis de pays tiers et l'utilisation de scanners corporels dans les aéroports.

5.4. Demandes d'informations et de conseils

Le nombre des demandes d'informations ou d'aide soumises par les citoyens a légèrement décliné en 2010 (141 demandes contre 174 en 2009). Cela s'explique principalement par la baisse du nombre des demandes portant sur des questions de protection des données au niveau national et pour lesquelles le CEPD n'est pas compétent. Cette évolution pourrait être perçue comme un résultat des efforts investis dans la clarification des compétences du CEPD à travers ses différents outils d'information et de communication.

Principaux sujets des demandes émanant de la presse en 2010



- Vie privée en ligne (*)
- Accord SWIFT/TFTP
- Révision du cadre européen de protection des données
- Directive sur la conservation des données
- Directive sur la vie privée dans les communications électroniques
- Activités de supervision du CEPD (**)
- Sécurité des données
- Données biométriques (***)
- Transferts internationaux de données (****)
- Scanners corporels
- Accord ACAC

(*) y compris les nouvelles applications en ligne, les moteurs de recherche et les réseaux sociaux.

(**) y compris les lignes directrices en matière de vidéosurveillance.

(***) y compris le système d'information Schengen.

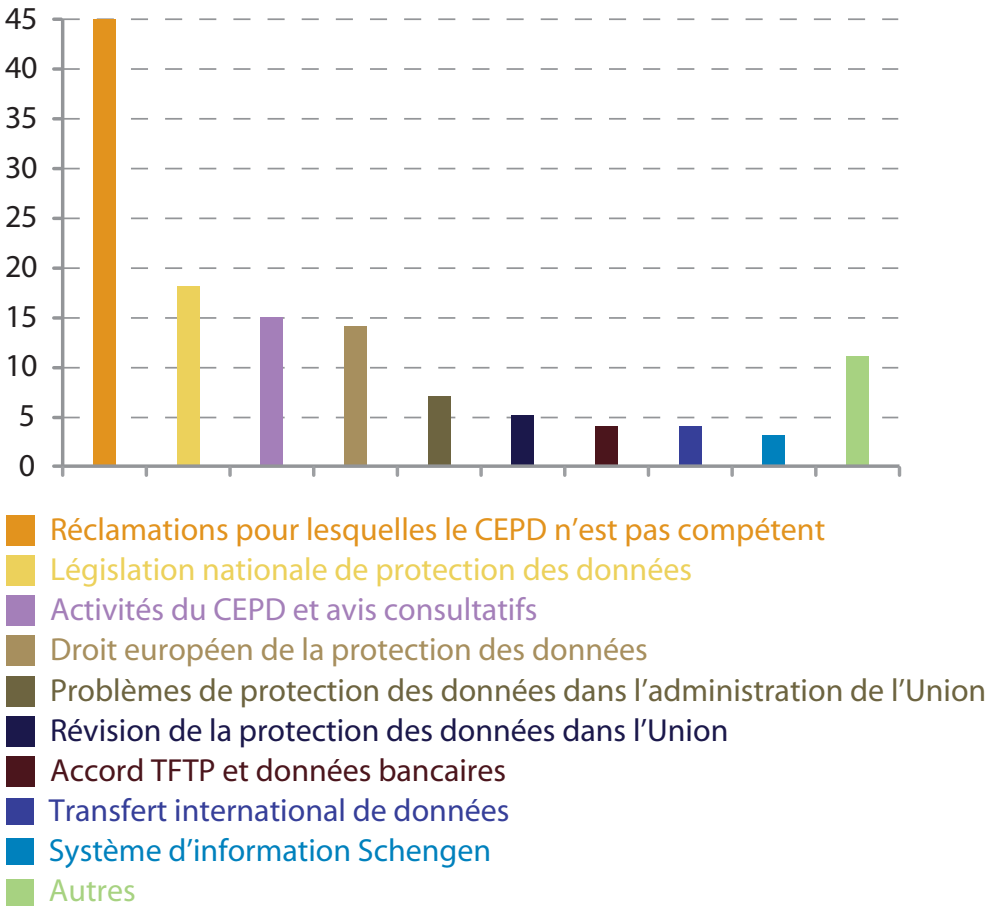
(****) y compris les décisions d'adéquation de la Commission.

Les demandes d'information émanent d'un large éventail de personnes et d'acteurs, qui vont des parties prenantes dont l'activité est liée à l'UE et/ou qui travaillent dans le domaine de la protection de la vie privée ou des données et dans le secteur de l'information (cabinets juridiques, consultants, groupes de pression, ONG, associations, universités, etc.) aux citoyens souhaitant obtenir plus d'informations sur les questions relatives à la protection de la vie privée ou qui demandent une assistance pour résoudre les problèmes auxquels ils sont confrontés dans ce domaine.

La première catégorie de demandes reçues en 2010 concerne les plaintes des citoyens de l'UE pour lesquelles le CEPD n'est pas compétent. Elles portaient la plupart du temps sur des violations présumées de la protection des données par les pouvoirs publics, par des entreprises publiques ou privées et par des services et technologies en ligne, comme les jeux de hasard en ligne, les blogs, les services de géolocalisation, les réseaux sociaux et les outils de messagerie. Les autres sujets concernés sont par exemple la sécurité des données bancaires, le droit d'accès aux documents détenus par les administrations nationales, la diffusion de données personnelles à des parties tierces sans le consentement de la personne concernée et des demandes d'appel contre la décision d'une autorité nationale chargée de la protection des données. Comme ces types de plaintes ne relèvent pas de la compétence du CEPD, une réponse est envoyée précisant le mandat du CEPD et conseillant à la personne de s'adresser à l'autorité compétente, en général l'autorité nationale de protection des données de l'État membre concerné.

La deuxième catégorie de demandes reçues en 2010 concerne la législation en matière de protection des données dans les États membres de l'UE et/ou sa mise en œuvre au niveau national. Dans ces dossiers, le CEPD conseille à la personne concernée de contacter l'autorité de protection des données concernée et, le cas échéant, l'unité de protection des données de la Commission européenne.

Principaux domaines de demandes d'information émanant du public en 2010



Les autres catégories de demandes d'informations relevaient la plupart du temps de la compétence du CEPD et ont donc reçu des réponses sur le fond. Il s'agit notamment de demandes concernant les activités du CEPD, en particulier ses activités de politique et de consultation, la législation européenne en matière de protection des données, les questions de protection des données au sein de l'administration européenne, la révision du cadre européen en matière de protection des données, l'accord TFTP et les données bancaires, les transferts internationaux de données et l'accès au système d'information Schengen.

5.5. Visites d'étude

Dans le cadre des efforts fournis pour renforcer sa visibilité et l'interaction avec le monde universitaire, le CEPD accueille régulièrement des groupes d'étudiants spécialisés dans les domaines du droit européen, de la protection des données et/ou de la sécurité des technologies de l'information. En 2010, le CEPD a accueilli sept groupes d'étudiants venus de différents pays européens. Ainsi, en octobre 2010, le bureau du CEPD a accueilli un groupe d'étudiants en droit international et européen de la fondation Friedrich Ebert, en Allemagne pour leur présenter ses fonctions et ses activités et évoquer avec eux les questions de protection des données en connexion avec le programme de Stockholm. Il y a eu aussi d'autres groupes de visiteurs composés d'étudiants autrichiens de MBA en administration publique et d'étudiants de l'université de Tilburg aux Pays-Bas, de la fondation Rosa Luxembourg en Allemagne et de l'université de Grenoble en France.

Pour atteindre un public plus jeune, le bureau du CEPD a également accueilli un groupe d'étudiants autrichiens de l'enseignement secondaire, avec lesquels les membres du personnel ont évoqué des questions de protection des données présentant un intérêt pour eux, comme les préoccupations de vie privée dans le contexte des réseaux sociaux en ligne.

5.6. Outils d'information en ligne

5.6.1. Site internet

Le site internet est l'outil de communication et d'information le plus important du CEPD. Il est mis à jour pratiquement tous les jours. C'est aussi sur le site que les visiteurs peuvent accéder aux documents élaborés dans le cadre des activités du CEPD (par exemple avis relatifs à des contrôles préalables et propositions d'actes législatifs européens, priorités de travail, publications, discours du contrôleur et du contrôleur adjoint, communiqués de presse, newsletter, informations sur les événements).

Évolution du site internet

En 2010, la modification la plus importante apportée au site internet a été l'introduction d'une version allemande, en plus des versions anglaise et française existantes. Cette initiative s'inscrit dans la décision de publier toutes les communications externes dans ces trois langues (au moins) afin de mieux répondre aux besoins d'information du public et des parties intéressées.

La page d'accueil a également été réorganisée afin de donner plus de visibilité aux dernières actualités relatives aux activités du CEPD.

D'autres améliorations du site internet sont prévues, par exemple:

- l'introduction d'un formulaire de réclamation en ligne afin de faciliter le processus de soumission des réclamations et d'accélérer le traitement des réclamations par les services du CEPD;
- une refonte de la rubrique relative aux avis faisant suite à un contrôle préalable afin d'améliorer les possibilités de recherche et la navigation à travers les différentes catégories thématiques;
- une présentation simplifiée du registre des notifications;
- l'introduction d'une rubrique «kit presse» destinée à fournir aux professionnels des médias des informations et des ressources pertinentes qu'ils pourront utiliser dans leurs articles et reportages.

Trafic et navigation

Dans le cadre des efforts continus pour améliorer la performance du site internet, de nombreux éléments, parfois moins visibles que d'autres, ont été améliorés en 2009 (par exemple l'outil de recherche avancée).

Une analyse des données sur le trafic et la navigation montre que le site internet a accueilli au total 108 215 visiteurs uniques en 2010, dont plus de 12 000 par mois en février et en mars. Cela représente une augmentation assez significative par rapport à 2009. Après la page d'accueil, les pages les plus souvent consultées ont été les rubriques «Contact», «Supervision» et «Consultation», tandis que les pages «Actualités» et «Événements» étaient également populaires. Les statistiques montrent également que la plupart des visiteurs accèdent au site via une adresse directe, un onglet, un lien dans un courrier électronique ou un lien sur un autre site (portail Europa ou site internet d'une autorité nationale de protection des données). Les liens à partir des moteurs de recherche sont utilisés par un nombre très restreint de visiteurs. Ces chiffres nous font penser que le site internet du CEPD est consulté par un noyau de visiteurs réguliers qui ont confiance en son contenu.

5.6.2. Newsletter

La newsletter du CEPD reste un outil précieux pour diffuser des informations sur les dernières activités du CEPD et attirer l'attention sur les ajouts récents au site internet. Elle fournit des informations sur les derniers avis en date du CEPD concernant les propositions législatives européennes et les contrôles préalables. Elle inclut également des informations sur les événements et les conférences organisés dans le domaine de la protection des données, ainsi que les discours et interventions du contrôleur et du contrôleur adjoint. Les newsletters sont disponibles sur le site internet du CEPD. Une fonction d'abonnement automatique figure sur la page concernée.

Cinq numéros de la newsletter du CEPD ont été publiés en 2010, soit en moyenne un tous les deux mois. Jusqu'en 2010, la newsletter était publiée en anglais et en français. Une version allemande a été introduite en 2010 pour toucher un public plus large et refléter l'utilisation de trois langues de travail au sein du service presse du CEPD.

Le nombre d'abonnés est passé de 1 200 personnes à la fin de 2009 à environ 1 500 à la fin de 2010. Parmi les abonnés figurent notamment des membres du Parlement européen, du personnel de l'UE et des autorités nationales chargées de la protection des données, ainsi que des journalistes, des universitaires, des sociétés du secteur des télécommunications et des cabinets juridiques.

5.6.3. Intranet

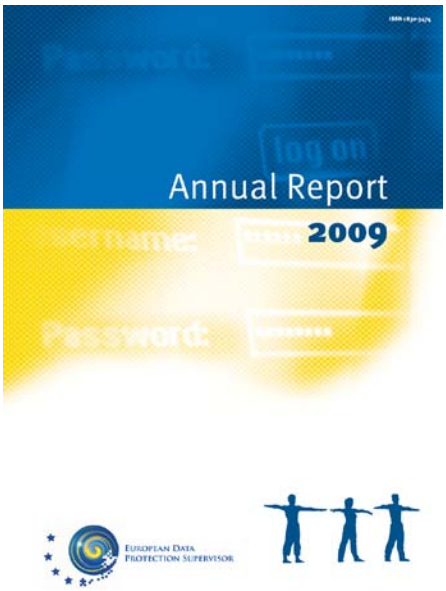
Afin d'améliorer la communication interne et de simplifier l'échange d'informations entre les différents secteurs du bureau du CEPD, un intranet a été développé avec l'aide du service concerné du Parlement européen. Ce nouveau portail sera pleinement opérationnel début 2011.

5.7. Publications

5.7.1. Rapport annuel

Le rapport annuel constitue la principale publication du CEPD. Il présente un aperçu des activités du CEPD au cours de l'année concernée dans les principaux domaines opérationnels que sont la supervision, la consultation et la coopération, et fixe les principales priorités pour l'année suivante. Il décrit en outre les réalisations en termes de communication externe et l'évolution de la situation en ce qui concerne l'administration, le budget et le personnel.

Ce rapport peut présenter un intérêt particulier pour différents groupes et différentes personnes aux niveaux international, européen et national, les personnes concernées en général, et les agents de l'UE en particulier, le système institutionnel de l'UE, les autorités chargées de la protection des données, les spécialistes, les groupes d'intérêt et les ONG actives dans ce domaine, ainsi que les journalistes et toute personne recherchant des informations sur la protection des données à caractère personnel au niveau de l'UE.



Rapport annuel 2009 du CEPD

En 2010, plusieurs améliorations de forme et de fond ont été apportées au rapport afin d'obtenir une publication plus facile à lire tout en veillant à ce que les principaux résultats et les conclusions du rapport ressortent clairement.

Le contrôleur et le contrôleur adjoint ont présenté le rapport annuel 2009 du CEPD à la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen le 15 novembre 2010. Les principaux éléments de ce rapport ont également été présentés à la presse lors de la conférence de presse organisée le même jour sur l'avenir du cadre européen en matière de protection des données (voir point 3.3).

5.7.2. Publications thématiques

Des travaux préparatoires ont également commencé en vue de la publication de «fiches d'information» thématiques portant sur des questions de protection des données d'importance stratégique. L'objectif sera de fournir des orientations ciblées au grand public comme aux parties intéressées. La première série de fiches d'information couvrira des sujets tels que la directive sur la protection de la vie privée dans les communications électroniques, l'accord SWIFT/TFTP et les dossiers passagers.

5.8. Actions de sensibilisation

Le CEPD tient à saisir toutes les occasions de mettre en lumière l'importance croissante du respect de la vie privée et de la protection des données et de faire mieux connaître les droits des personnes concernées et les obligations de l'administration européenne en matière de respect de la vie privée et de protection des données.

5.8.1. Journée de la protection des données

Les États membres du Conseil de l'Europe et les institutions et organes européens ont célébré le 28 janvier 2010 la quatrième Journée de la protection des données. Cette date marque l'anniversaire de l'adoption de la convention du Conseil de l'Europe pour la protection des données à caractère personnel (convention 108), le premier instrument international juridiquement contraignant dans le domaine de la protection des données.

Ces dernières années, cette manifestation a été l'occasion pour le CEPD de souligner l'importance de la vie privée et de la protection des données, et plus particulièrement de sensibiliser le personnel de l'UE à ses droits et obligations en la matière. Lors de chaque Journée de la protection des données, un stand d'information est monté dans les locaux du Parlement européen, de la Commission européenne et du Conseil, en collaboration avec les délégués à la protection des données de ces institutions. Les visiteurs ont la possibilité de poser des questions aux membres du bureau du CEPD et au délégué à la protection des données et de participer à un quiz pour tester leurs connaissances de la protection des données dans l'Union européenne.

Le CEPD a renouvelé cette activité spécifique en 2010 tout en consacrant davantage d'efforts à la sensibilisation du personnel des institutions européennes. Un débat organisé à l'heure du déjeuner et intitulé «Vie privée et protection des données: quels impacts pour vous?» a eu lieu à la Commission européenne le 28 janvier 2010. Peter Hustinx a fait une présentation au personnel de la Commission et répondu à ses questions concernant les droits de protection des données et la façon de les exercer au sein de l'administration de l'Union européenne.

Un message vidéo du contrôleur et du contrôleur adjoint a également été diffusé aux parties prenantes institutionnelles et mis à disposition sur le site internet afin de présenter le rôle du CEPD et de décrire les défis à venir.

Le CEPD a également participé à différents événements organisés à Bruxelles à l'occasion de la Journée de la protection des données, comme la conférence et la cérémonie de remise des prix qui ont conclu la campagne «Priorité à la confidentialité» («Think Privacy») lancée par European Schoolnet et Microsoft. Dans le cadre de cette campagne, un concours «Priorité à la confidentialité» a invité les jeunes de 15 à 19 ans à soumettre une présentation multimédias sur le thème «La vie privée est un droit fondamental - Traitez-là avec précaution».

Les 29 et 30 janvier 2010, le CEPD a participé à la conférence internationale «Ordinateurs, vie privée et protection des données» visant à créer un pont entre les décideurs politiques, les universitaires, les praticiens et les activistes afin de discuter des problèmes émergents en matière de respect de la vie privée, de protection des données et de technologies de l'information. Pour cette quatrième édition, le thème de la conférence était «Un élément de choix», en référence aux nombreuses possibilités qui s'offrent à la politique en matière de protection

Peter Hustinx, CEPD, prenant la parole à l'occasion de la conférence et de la cérémonie de remise des prix de la campagne «Think Privacy» (Bruxelles, 28 janvier 2010)

des données. Les membres du secrétariat du CEPD ont participé à des tables rondes et Peter Hustinx a prononcé le discours de clôture de la conférence.

5.8.2. Journée portes ouvertes de l'UE

Le 8 mai 2010, le bureau du CEPD a participé, comme chaque année, à la Journée portes ouvertes des institutions européennes organisée au Parlement européen à Bruxelles.

La Journée portes ouvertes de l'Union européenne offre une excellente occasion de sensibiliser le public à la nécessité de protéger la vie privée et les informations à caractère personnel.

Le CEPD disposait d'un stand situé dans le bâtiment principal du Parlement européen, et des membres de son secrétariat étaient sur place pour répondre aux questions posées par les visiteurs. Comme lors de la Journée de la protection des données, différents supports ont été distribués aux visiteurs, ainsi qu'un quiz sur la protection de la vie privée et des données au niveau européen.

Visiteurs complétant un quiz sur la protection des données pendant la Journée «Portes ouvertes» de l'Union européenne.

6 ADMINISTRATION, BUDGET ET PERSONNEL

6.1. Introduction

Mme Monique Leens, responsable de l'administration du secrétariat du CEPD depuis sa création, a pris sa retraite en juin 2010. Elle a apporté une contribution essentielle à la mise en place du CEPD au cours des six dernières années, et le CEPD lui souhaite de profiter pleinement d'une retraite bien méritée. Depuis son départ, M. Christopher Docksey, détaché temporairement du service juridique de la Commission européenne, occupe le poste de directeur *ad interim* du CEPD. Le secrétariat a été renforcé par le recrutement de M. Leonardo Cervera Navas, également de la Commission européenne, en tant que responsable des ressources humaines, du budget et de l'administration.

Les effectifs ont considérablement augmenté en 2010. Après la publication des listes de réserve des concours généraux sur la protection des données organisés par le CEPD, douze nouveaux fonctionnaires ont été recrutés. Il a fallu pour cela trouver des espaces de bureaux supplémentaires, mais aussi adopter une nouvelle structure organisationnelle capable de répondre aux besoins d'une organisation plus importante assumant des responsabilités nouvelles et complexes.

La réorganisation du CEPD, qui a commencé par une note interne en avril 2010, s'est poursuivie tout au long de l'année et a bénéficié de l'intervention d'un consultant en management externe. Ce travail devrait se poursuivre en 2011 en mettant notamment l'accent sur la stratégie et la gestion des performances.

6.2. Budget

En 2010, l'autorité budgétaire a accordé un budget de 7 104 351 euros au CEPD, soit une augmentation de 6,62 % par rapport à l'année précédente.

Cette augmentation a répondu aux besoins d'une organisation de plus grande taille aux effectifs plus nombreux, ayant de nouvelles activités et assumant de nouvelles responsabilités après l'entrée en vigueur du traité de Lisbonne. Outre les rémunérations et les dépenses liées aux bâtiments, une grande partie du budget est consacrée aux traductions. En effet, les avis du CEPD sur les propositions législatives sont traduits dans toutes les langues officielles de l'UE et publiés au Journal officiel de l'Union européenne. Les avis sur les contrôles préalables et les autres documents publiés sont également traduits dans les langues de travail du CEPD (anglais, français et allemand).

La déclaration d'assurance (DAS) 2009 de la Cour des comptes européenne ne demandait pas de changements importants. Le rapport final ne contenait que deux recommandations, portant sur l'amélioration des normes de contrôle interne par l'adoption d'un système de vérification *a posteriori*, et sur la création d'un registre central permettant de noter toutes les exceptions éventuelles aux procédures financières standard.

La Commission européenne a continué de fournir une assistance dans le domaine financier en 2010, en particulier en ce qui concerne les services comptables, le comptable de la Commission ayant également été désigné comptable du CEPD. Dans

ce contexte, la direction générale Budget de la Commission européenne a procédé à la validation des procédures des systèmes comptables locaux et rendu un rapport positif. La principale recommandation de ce rapport a été de nommer un conseiller en comptabilité.

Toutes les recommandations contenues dans les rapports de la Cour des comptes européenne et de la Commission ont été mises en œuvre comme suit:

a) un nouveau système interne de vérification financière a été ajouté au workflow financier;

b) un conseiller comptable a été désigné;

c) un registre central des exceptions a été mis en place; et

d) un système de vérification *a posteriori* est en cours d'adoption.

Après la réorganisation du CEPD, M. Christopher Docksey, directeur ad interim du CEPD, a été nommé ordonnateur délégué. M. Leonardo Cervera Navas, responsable RH, budget et administration, a été nommé ordonnateur par sous-délégation. Cette nouvelle structure apporte une souplesse accrue et renforce le processus d'autorisation des transactions financières du CEPD.

Dans les cas où aucune règle spécifique n'a été prévue, le CEPD applique les règles internes de la Commission relatives à l'exécution du budget.

6.3. Ressources humaines

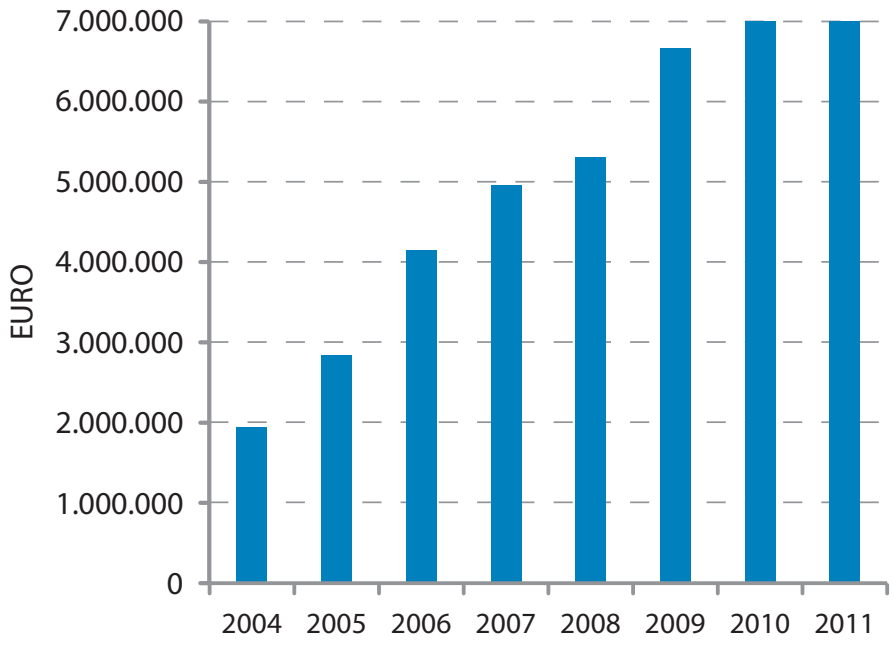
6.3.1. Recrutement

Comme les années précédentes, et comme le montrent les chapitres précédents du présent rapport, la visibilité croissante du CEPD se traduit par une augmentation de la charge de travail et un accroissement des tâches à assumer du point de vue des ressources humaines.

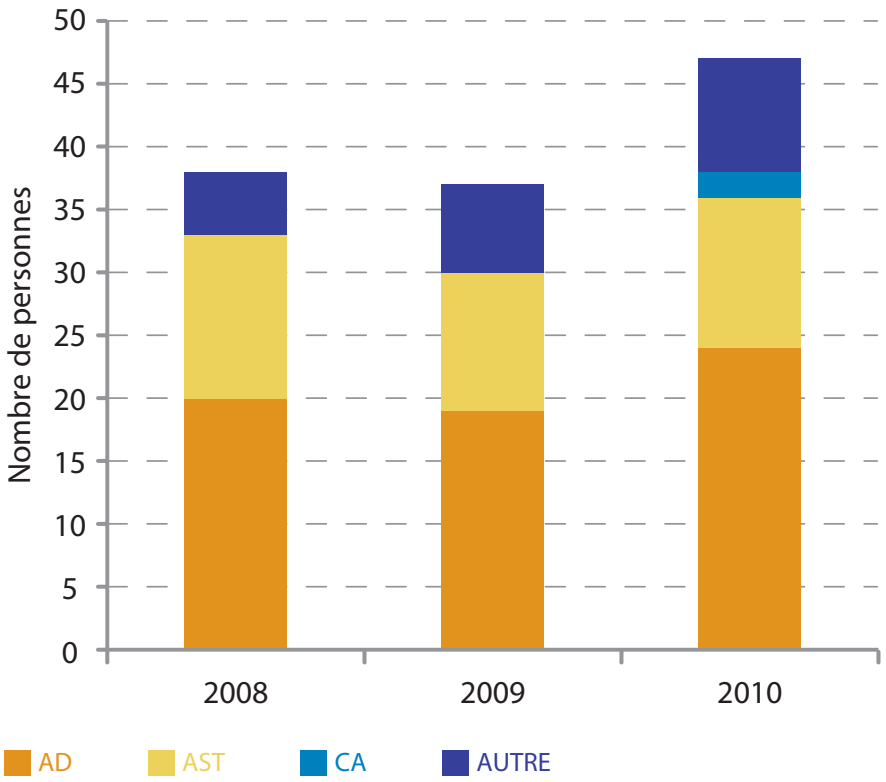
Grâce à un accord de niveau de service, le CEPD bénéficie des services proposés par l'Office européen de sélection du personnel (EPSO) et participe aux travaux de son conseil d'administration en tant qu'observateur. Ainsi, en étroite coopération avec l'EPSO, le CEPD a lancé en 2009 un concours général en matière de protection des données pour recruter du personnel hautement spécialisé. Trois listes de réserve ont été publiées à l'été 2010 pour les grades AD9, AD6 et AST3. La validité de ces listes de réserve a été prolongée jusqu'au moins fin 2011.

À la suite de la publication de ces listes, le CEPD s'est lancé dans une grande procédure de recrutement et a organisé des entretiens avec les candidats des listes de réserve et avec des fonctionnaires d'autres

Évolution du budget du CEPD 2004-2011



ÉVOLUTION DES EFFECTIFS DU CEPD PAR CATÉGORIE



institutions conformément à l'article 29 du statut du personnel. En 2010, le CEPD a recruté 12 fonctionnaires et recouru pour la première fois à une nouvelle catégorie de personnel: les agents contractuels. En plus du processus de sélection des candidats issus des listes CAST, deux agents contractuels ont également été recrutés. Une secrétaire intérimaire a également été recrutée en 2010 pour répondre à des besoins temporaires. Au total, le CEPD a recruté 15 nouveaux collègues en 2010.

Enfin, la vacance du poste de directeur du CEPD a été publiée sur le site internet de recrutement interinstitutionnel fin 2010. Cette procédure de recrutement à un poste de haut niveau devrait être achevée au premier semestre 2011.

6.3.2. Programme de stages

Un programme de stages a été créé en 2005 afin d'offrir aux jeunes diplômés universitaires la possibilité de mettre en pratique les connaissances acquises durant leurs études et d'acquérir ainsi une expérience pratique en participant aux activités quotidiennes du CEPD. Celui-ci a ainsi l'occasion d'accroître sa visibilité auprès des jeunes citoyens de l'UE, en particulier auprès des étudiants des universités et des jeunes diplômés spécialisés dans la protection des données.

Le programme principal accueille en moyenne deux stagiaires par session. Deux sessions de cinq mois sont organisées chaque année, de mars à juillet et d'octobre à février. Dans des circonstances exceptionnelles, et dans le respect de critères d'admission stricts, le CEPD peut également accueillir des étudiants en doctorat pour des stages non rémunérés. Tous les stagiaires, rémunérés ou non, ont contribué à la fois au travail théorique et pratique, tout en acquérant une expérience directe.

Sur la base d'un accord de niveau de service conclu avec la Commission, le CEPD a bénéficié d'une assistance administrative de la part du bureau des stages de la direction générale de l'éducation et de la culture de la Commission, qui a continué d'apporter un soutien précieux grâce à l'expérience de son personnel.

6.3.3. Programme pour les experts nationaux détachés

Le programme destiné aux experts nationaux détachés (END) a été lancé en janvier 2006. En moyenne,

deux experts nationaux des autorités de protection des données (APD) des États membres sont détachés chaque année. Le détachement d'experts nationaux permet au CEPD de bénéficier de leurs compétences et de leur expérience professionnelle et d'accroître sa visibilité au niveau national. Dans le même temps, ce programme permet aux END de se familiariser avec les questions de protection des données au niveau de l'UE.

6.3.4. Organigramme

L'organigramme du CEPD est resté inchangé entre sa création en 2004 et 2009, quand les premières mesures de réorganisation ont été prises avec la création du poste de directeur à la tête du secrétariat.

En 2010, l'organigramme du CEPD a connu un profond changement avec la réorganisation du personnel en cinq secteurs (Contrôle et mise en application, Politique législative et consultation, Opérations, planning et assistance, Information et communication, RH, budget et administration), avec des responsables de secteurs nommés à un niveau d'encadrement intermédiaire. Dans la nouvelle structure organisationnelle, le directeur représente le CEPD au niveau de la direction et veille à la mise en œuvre des politiques et à la coordination horizontale des activités. Les contrôleurs gardent la responsabilité finale du management, mais se concentrent désormais davantage sur l'élaboration des politiques et sur les relations interinstitutionnelles.

Ces changements ont donné lieu à un nouvel organigramme disponible sur le site internet du CEPD.

6.3.5. Formacion

L'une des priorités du CEPD pour 2010 était d'offrir à son personnel de meilleures possibilités de formation et de développement professionnel. Un nouvel accord de niveau de service a été signé avec le département RH de la Commission européenne. Cet accord permettra d'accéder par voie électronique au catalogue de formations de la Commission dès le début de l'année 2011. À partir de ce moment, les membres du personnel du CEPD auront un accès direct à SYSLOG Formation et bénéficieront des mêmes possibilités de formation que les fonctionnaires de la Commission.

De nombreux membres du personnel ont suivi des cours de langue et ont eu accès à des formations organisées au niveau interinstitutionnel, ainsi qu'à des formations extérieures si nécessaire. La formation intitulée «Programme d'efficacité personnelle (PEP)», organisée spécifiquement pour le CEPD, a rencontré un succès particulier. Trois secteurs ont suivi cette formation en 2010, et tous les autres membres du personnel la suivront au premier semestre 2011.

À la suite de la réorganisation du CEPD, les nouveaux responsables ont reçu une formation spécifique en management et en accompagnement, aussi bien en tant que responsables qu'en équipe.

Le CEPD a continué de participer aux travaux des comités interinstitutionnels (groupe de travail interinstitutionnel de l'École européenne d'administration (EEA), groupe interinstitutionnel d'évaluation de la formation de l'EEA, comité interinstitutionnel de la formation linguistique), ce qui facilite l'union des forces et permet des économies d'échelle dans un domaine où les institutions de l'Union européenne présentent des besoins similaires. Comme les années précédentes, le CEPD a signé, avec les autres institutions, le protocole sur l'harmonisation des coûts des cours de langue interinstitutionnels et le nouveau protocole de répartition des coûts par institution des projets pédagogiques linguistiques interinstitutionnels.

En 2011, le CEPD poursuivra ses efforts en vue d'améliorer les possibilités de formation et de développement professionnel de son personnel. Il est également prévu de mettre à jour la décision en matière de formation du 18 juillet 2007, en étroite consultation avec le personnel.

6.3.6. Activités sociales

Le CEPD a signé un accord de coopération avec la Commission en vue de faciliter l'intégration et l'installation des nouveaux collègues, par exemple en fournissant une aide juridique pour les questions d'ordre privé (contrats de location, achat d'un logement, etc.) et en leur offrant la possibilité de participer à diverses activités sociales et de réseautage. Les nouveaux arrivés sont accueillis personnellement par le contrôleur, le contrôleur adjoint et le directeur du CEPD. Outre leur parrain, ils rencontrent aussi les membres du secteur RH, budget et administration, qui leur remettent le guide administratif du CEPD et leur communiquent les informations concernant les procédures propres au CEPD.

Le CEPD a également continué de développer la coopération interinstitutionnelle en matière d'accueil des enfants: les enfants du personnel du CEPD ont ainsi accès aux *crèches*, aux garderies et aux centres extérieurs réservés aux enfants du personnel de la Commission, ainsi qu'aux écoles européennes. Le CEPD participe également, en qualité d'observateur, aux réunions du comité consultatif du Parlement européen pour la prévention et la protection au travail, dont l'objectif est d'améliorer l'environnement professionnel.

En 2010, les secteurs nouvellement créés ont organisé leurs propres journées de sortie pour encourager l'esprit d'équipe et aider les nouveaux-venus à s'intégrer. La soirée de Noël du personnel organisée à la fin de l'année a été l'occasion de souhaiter la bienvenue aux nouveaux collègues et de faire le point sur une année intense pleine de changements.

6.4. Fonctions de contrôle

6.4.1. Contrôle interne

Le système de contrôle interne, en vigueur depuis 2006, garantit que les objectifs du CEPD seront réalisés de manière efficace dans le respect des lois et des règlements. Le CEPD a adopté des procédures de contrôle interne spécifiques en fonction de ses besoins, de sa taille et de ses activités. Le système a été conçu pour gérer plutôt que pour éliminer le risque de non-réalisation des objectifs.

Le CEPD a pris acte du rapport d'activités annuel et de la déclaration d'assurance jointe signée par l'ordonnateur délégué. D'une manière générale, le CEPD estime que les systèmes de contrôle interne en place fournissent une assurance raisonnable quant à la légalité et à la régularité des opérations dont l'institution est responsable. Néanmoins, une approche plus ambitieuse a été lancée en 2010. La liste des actions mettant en œuvre les normes de contrôle interne (NCI) a été élargie afin de garantir un contrôle interne plus efficace des processus en place.

Par exemple, de nouveaux manuels ont été adoptés en vue de mieux gérer les processus de contrôle préalable, le traitement des réclamations ou encore les procédures en justice. Les activités telles que les mesures de sensibilisation en matière d'éthique, l'adoption de descriptifs de fonction plus détaillés, de règles internes supplémentaires ou d'un nouveau système de parrainage ont lieu en étroite concertation avec le personnel et avec le plein appui des contrôleurs.

6.4.2. Audit interne

L'auditeur interne de la Commission est également l'auditeur interne du CEPD. Pour garantir la gestion efficace des ressources du CEPD, l'auditeur interne procède à des vérifications régulières des systèmes de contrôle interne de l'institution, ainsi que de ses opérations financières.

Après la visite de suivi du service d'audit interne (SAI) en décembre 2008, un rapport adopté en mai 2009 a confirmé la réalisation des objectifs du CEPD. Ce rapport a toutefois identifié certains points susceptibles d'être améliorés. Certains de ces points ont déjà fait l'objet d'une action, tandis que d'autres sont en cours d'examen parallèlement à la réorganisation du CEPD.

Un exercice d'évaluation des risques par le SAI était prévu pour le début de l'année 2011, en vue d'un audit dans la deuxième partie de l'année.

6.4.3. Sécurité

En décembre 2010, le CEPD a décidé de désigner deux membres de son personnel au poste de responsable local de la sécurité (RLS) et responsable local de la sécurité informatique (RLSI) d'une part, et au poste d'assistant RLS/RLSI d'autre part, à temps partiel dans les deux cas. Des premiers contacts ont été établis avec la Commission européenne et avec les services du Parlement européen, et un premier domaine de coopération a été décidé de commun accord. La procédure d'habilitation de sécurité du personnel concerné a été lancée. La poursuite de la mise en œuvre sera axée sur la sécurité de l'information et la sécurité des technologies de l'information (TI), notamment en ce qui concerne le développement du système interne de gestion des dossiers du CEPD.

En 2011, le CEPD continuera de se baser sur la décision «sécurité» adoptée fin 2008, qui comprend des mesures concernant la gestion des informations confidentielles et de la sécurité informatique, ainsi que les conditions de santé et de sécurité des personnes et des lieux.

6.5. Infrastructure

Sur la base de l'accord de coopération administrative, le CEPD est sis dans les locaux du Parlement européen, qui l'assiste dans les domaines des technologies de l'information (TI) et de l'infrastructure. Au vu de l'augmentation significative des effectifs en 2010, de nouveaux espaces de bureaux ont été libérés avec la collaboration du Parlement européen.

Le bâtiment qui héberge le CEPD a été partiellement rénové en 2010. Cette rénovation, réalisée sous le contrôle du Parlement européen, a permis d'accroître considérablement le niveau de confort et de bien-être au travail. Le manque d'espace reste néanmoins une grande préoccupation pour le CEPD, et ce problème a fait l'objet de plusieurs réunions avec le Parlement européen.

L'institution a continué de gérer de manière indépendante l'inventaire de son mobilier et de ses biens informatiques, avec le concours des services du Parlement européen.

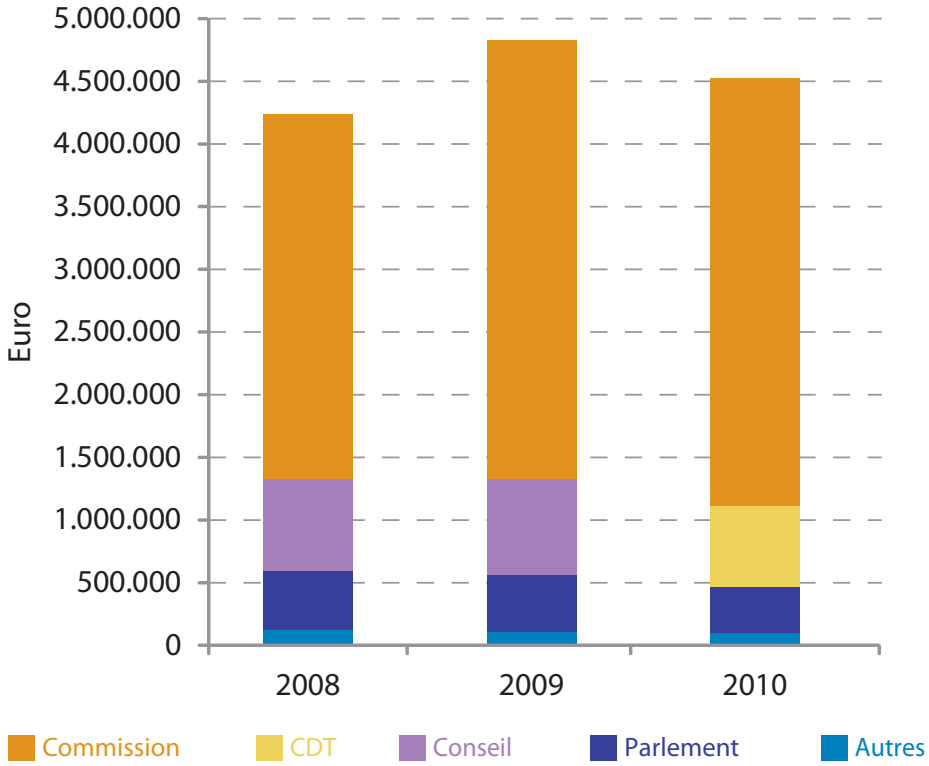
6.6. Environnement administratif

6.6.1. Assistance administrative et coopération interinstitutionnelle

Le CEPD bénéficie de la coopération interinstitutionnelle dans de nombreux domaines en vertu de l'accord conclu en 2004 avec les secrétaires généraux de la Commission, du Parlement et du Conseil, accord qui a été prorogé pour une durée de trois ans en 2006 et de deux ans en 2010. Cette coopération est extrêmement précieuse pour le CEPD en termes d'accroissement de l'efficacité et d'économies d'échelle.

En 2010, la coopération interinstitutionnelle s'est poursuivie avec diverses directions générales de la Commission (DG «Personnel et administration»; DG «Budget»; service d'audit interne; DG «Éducation et culture»), l'Office des paiements (PMO), l'École européenne d'administration (EEA) et différents services du Parlement européen (services de l'information et des technologies, en ce qui

EXÉCUTION DU BUDGET DU CEPD VIA LA COOPÉRATION INTERINSTITUTIONNELLE



concerne plus particulièrement la maintenance et le développement du site internet du CEPD, l'équipement des locaux, la sécurité des bâtiments, les travaux d'impression, le courrier, la téléphonie, les fournitures, etc.). Dans de nombreux cas, cette coopération se fait via des accords de niveau de service régulièrement mis à jour. Le CEPD a également continué de participer aux appels d'offres interinstitutionnels, accroissant ainsi son efficacité dans de nombreux domaines administratifs et évoluant vers plus d'autonomie.

L'accord avec le Conseil européen pour les services de traduction est arrivé à échéance en janvier 2010. Un nouvel accord a été signé avec le Centre de traduction des organes de l'Union européenne, qui se charge des traductions depuis 2010.

Le CEPD est membre de plusieurs comités interinstitutionnels et groupes de travail, notamment le collège des chefs d'administration, le comité de gestion assurance maladie (CGAM), le comité de préparation pour les questions statutaires (CPQS), le comité du statut, le groupe de travail interinstitutionnel de l'EEA, le conseil de direction de l'EPSO et la commission paritaire commune. Le CEPD est membre du Comité de préparation pour les affaires sociales et participe aux réunions de son groupe *ad hoc* sur la mise en œuvre de la Convention des Nations unies relative aux droits des personnes handicapées au sein des institutions de l'Union européenne. Cette participation a contribué à accroître la visibilité du CEPD auprès des autres institutions et encourage l'échange de bonnes pratiques.

6.6.2. Règlement intérieur

L'adoption du règlement intérieur pour le bon fonctionnement du CEPD se poursuit. Lorsque ces dispositions concernent des domaines pour lesquels le CEPD bénéficie de l'assistance de la Commission ou du Parlement européen, elles sont semblables à celles des autres institutions, moyennant quelques adaptations liées à la spécificité des services du CEPD.

Le CEPD est une institution relativement nouvelle qui connaît une évolution rapide. En conséquence, les règles et procédures qui étaient adaptées aux premières années d'activité pourraient s'avérer moins efficaces à l'avenir, dans le cadre d'une structure plus importante et plus complexe. Les règles font donc l'objet d'une évaluation continue qui pourrait entraîner des modifications au cours des prochaines années. Des travaux ont été lancés en 2010 en vue de modifier le code de bonne conduite du CEPD.

6.6.3. Gestion des documents

Un nouveau système de gestion du courrier électronique (GEDA) a été mis en œuvre pour les tâches administratives en 2009, avec l'aide des services du Parlement européen. À l'issue de cette première étape, des études ont été effectuées pour élaborer un système approprié de gestion des documents et des dossiers pour le service de protection des données.

En 2010, le CEPD a rédigé des exigences détaillées en vue d'un système adéquat de gestion des documents et des archives intégrant la gestion des dossiers pour l'institution. Des consultants extérieurs ont été chargés de procéder à une analyse du marché sur la base de ces besoins afin d'identifier les solutions potentielles adéquates. La direction générale de l'innovation et du support technologique (ITEC) du Parlement européen continue de soutenir le CEPD dans ce processus. Une équipe de projet interne a été formée sous la direction du responsable du secteur Opérations, planning et assistance. Cette équipe pluridisciplinaire se compose de membres représentant les cinq différents secteurs.

Parallèlement à ces évolutions technologiques, le secteur Opérations, planning et assistance a continué d'appliquer une gestion précise des archives. Un plan d'archivage pour quatre des cinq secteurs a été adopté, et les procédures d'enregistrement du courrier ont été rationalisées en tenant compte de la nouvelle structure organisationnelle du CEPD. Une attention particulière a également été accordée aux exigences de compte rendu de la direction du CEPD. Des informations spécifiques relatives aux dossiers ont été identifiées et recueillies par tous les secteurs afin d'améliorer le suivi des dossiers.

7 DÉLÉGUÉ À LA PROTECTION DES DONNÉES DU CEPD

7.1. Une nouvelle équipe de DPD pour le CEPD

Comme toutes les autres institutions de l'Union européenne, le CEPD est soumis à des obligations légales spécifiques concernant la protection des données à caractère personnel. Ces obligations sont fixées par le règlement relatif à la protection des données (règlement (CE) n° 45/2001).

En plus de préciser les principes juridiques régissant le traitement de données à caractère personnel par l'Union européenne, ce règlement prévoit que chaque institution ou organe de l'Union européenne doit désigner au moins une personne en tant que délégué à la protection des données (DPD).

En septembre 2010, le CEPD a désigné un **nouveau DPD** et décidé de nommer également un **DPD adjoint**. En procédant à ces désignations, le CEPD insuffle une énergie nouvelle dans ce domaine afin d'évoluer rapidement vers un meilleur niveau de conformité.

Le DPD du CEPD doit relever de nombreux défis: il lui faut en effet se montrer indépendant au sein d'une institution indépendante, répondre aux attentes élevées de collègues particulièrement attentifs et sensibles aux questions de protection des données et apporter des solutions susceptibles de servir de références aux autres institutions.

7.2. Plan d'action et disposition d'application

L'équipe DPD nouvellement nommée a distribué au personnel un **plan d'action** global avec des priorités. Ce plan d'action met en avant quatre domaines principaux auxquels l'équipe de DPD compte accorder une grande attention: les aspects organisationnels, le rôle consultatif, l'information et la sensibilisation.

L'adoption des **dispositions d'application du DPD** en octobre 2010 a marqué une première étape importante. Ces règles s'inspirent des règles de mises en œuvre d'autres institutions et des lignes directrices du CEPD tout en tenant compte des spécificités du CEPD. Ainsi, l'obligation d'obtenir l'accord du CEPD pour révoquer le DPD a été modifiée de façon à requérir l'accord du contrôleur et du contrôleur adjoint. En outre, s'inspirant du document relatif aux normes applicables aux DPD, les dispositions d'application soulignent la nécessité d'une bonne connaissance de la protection des données et de l'indépendance dans le processus de compte rendu.

7.3. Un registre des traitements facilement accessible

L'équipe DPD a procédé à un contrôle minutieux de **l'inventaire des traitements existants** et sensibilisé le personnel pour veiller à ce que toutes les opérations de traitement au sein du CEPD soient notifiées. À cette fin, les responsables du traitement ont été encouragés à préparer les notifications manquantes. Dans les cas où cela s'avérait nécessaire, l'équipe DPD a également aidé à préparer de nouvelles notifications et à compléter les notifications existantes.

Une version électronique du registre des traitements a été mise à disposition en ligne. Cette version électronique contient un hyperlien vers toutes les notifications définitives, ce qui permet un accès aisé à toute personne désireuse de consulter le registre conformément à l'article 26 du règlement relatif à la protection des données.

Le DPD a également mis à jour et amélioré les formulaires de notification qui serviront à notifier les traitements de données à caractère personnel au sein du secrétariat du CEPD.

7.4. Exercice de printemps

L'équipe du DPD a assuré le suivi du dernier «exercice de printemps» (voir point 2.5.2.) et communiqué au CEPD des informations à jour concernant le respect des règles de protection des données au sein de l'institution. La lette envoyée au CEPD début 2011 met en avant les résultats obtenus et souligne l'intention, sur la base du plan d'action du DPD, de renforcer la conformité et la prise de conscience des questions relatives à la protection des données, notamment dans le domaine des ressources humaines.

7.5. Information et sensibilisation

L'équipe DPD accorde une grande importance à la sensibilisation et à la communication relative au respect des règles de protection des données au sein du CEPD, en interne comme en externe.

En ce qui concerne la **communication externe**, une rubrique DPD reprenant des informations de base sur le rôle et les activités du DPD est désormais disponible sur le site internet du CEPD. Les dispositions d'application et le registre des traitements du CEPD sont eux aussi disponibles en ligne.

Par ailleurs, l'équipe du DPD a également participé aux **réunions du réseau des DPD**, qui sont une occasion unique de développer des réseaux, d'aborder des problèmes communs et d'échanger les bonnes pratiques. L'équipe du DPD a également participé activement aux activités organisées dans le cadre de la Journée de la protection des données.

En ce qui concerne la **communication interne**, l'intranet mis en place récemment est une excellente façon de communiquer avec le personnel. La rubrique du DPD sur l'intranet contient des informations utiles pour les membres du personnel: les principaux aspects du rôle du DPD, les dispositions d'application, le plan d'action du DPD ainsi que des informations concernant les activités du DPD. L'équipe du DPD compte également se servir de cet espace virtuel pour accroître la visibilité des informations à communiquer aux personnes concernées conformément aux articles 11 et 12 du règlement. À cet égard, l'équipe du DPD a commencé, via l'intranet, à fournir des références aux déclarations de confidentialité des traitements effectués au sein du CEPD afin de les rendre facilement accessibles à tous les membres du personnel.

8 PRINCIPAUX OBJECTIFS POUR 2011

Les objectifs suivants ont été sélectionnés pour 2011. Les résultats obtenus figureront dans le rapport de l'année prochaine.

8.1. Supervision et mise en application

Conformément au document stratégique sur le respect et la mise en application du règlement adopté en décembre 2010, le CEPD a défini les objectifs suivants en matière de supervision et de mise en application.

- **Sensibilisation**

Le CEPD continuera d'investir du temps et des ressources pour fournir des conseils et des orientations sur les sujets relatifs à la protection des données. Cette action de sensibilisation prendra la forme de documents d'orientation sur des thèmes choisis et d'ateliers de travail ou de séminaires interactifs au cours desquels le CEPD exposera son avis dans un domaine particulier.

- **Rôle du contrôle préalable**

L'arriéré des contrôles préalables *ex post* étant presque résorbé, le CEPD se concentrera sur l'analyse des conséquences liées aux nouvelles opérations de traitement. Le Contrôleur continuera de mettre l'accent sur la mise en application des recommandations figurant dans les avis en vue d'un contrôle préalable et veillera à leur suivi adéquat.

- **Exercices de contrôle et de reporting**

Poursuivant ses activités de contrôle de la conformité des institutions et des organes de l'UE aux règles de protection des données, le CEPD effectuera un exercice de contrôle général au printemps 2011 ainsi que des exercices de contrôle ciblés chaque fois que le niveau de conformité se révélera préoccupant.

- **Inspections**

Le CEPD peut opérer des inspections sur place, dès lors que des motifs sérieux le conduisent à redouter un blocage du mécanisme de respect. Ces inspections sont considérées comme la dernière étape avant l'adoption de mesures d'exécution formelles. Le CEPD procédera également à des inspections et à des audits dans le domaine des systèmes d'information à grande échelle relevant de sa compétence.

8.2. Politique et consultation

Les principaux objectifs sont conformes aux priorités 2011 pour ce domaine, telles que publiées sur le site internet. En outre, des objectifs ont été formulés pour la coopération avec les autorités de protection des données et pour la poursuite du contrôle des systèmes d'information à grande échelle.

- **Étendue des consultations**

Le CEPD continuera de rendre des avis ou de formuler des observations, en temps utile sur les nouvelles propositions législatives et à en assurer un suivi approprié dans tous les domaines pertinents. Il accordera une attention particulière à la révision du cadre juridique de l'UE pour la protection des données, à l'exécution du programme de Stockholm et aux initiatives dans le domaine de la technologie.

- **Révision du cadre juridique**

Le CEPD donnera la priorité à l'élaboration d'un cadre juridique exhaustif pour la protection des données. Il publiera un avis législatif sur la communication de la Commission sur une approche globale de la protection des données à caractère personnel dans l'Union européenne, ainsi que sur toute autre proposition législative ultérieure. Il apportera par ailleurs sa contribution au débat, si cela se révèle nécessaire et approprié.

- **Mise en œuvre du programme de Stockholm**

Le CEPD restera attentif aux diverses initiatives concernant la poursuite de l'application du programme de Stockholm dans le domaine de la liberté, de la sécurité et de la justice. Parmi celles-ci, il y a lieu de citer la mise en place d'un système d'entrée-sortie et le programme relatif aux voyageurs enregistrés, la proposition de directive sur l'utilisation des données des dossiers passagers (PNR) à des fins répressives et l'introduction d'un programme européen de surveillance du financement du terrorisme.

- **Initiatives dans le domaine des technologies**

Le CEPD examinera avec attention les initiatives prises dans le domaine des technologies qui sont susceptibles d'avoir une incidence sur la vie privée et la protection des données. En particulier, il continuera de surveiller la mise en œuvre des volets de la stratégie Europe 2020 liés aux technologies de l'information, tels que cela a été prévu dans le cadre de la stratégie numérique, dont la RFID (*Radio Frequency Identification* - identification par radiofréquence), l'«informatique dématérialisée» (*cloud computing*), l'administration en ligne (*eGovernment*) et l'application des droits de propriété intellectuelle sur l'internet.

- **Autres initiatives**

Le CEPD suivra de près toutes les autres initiatives susceptibles d'avoir des répercussions notables sur la protection des données, comme celles relatives au domaine du transport (utilisation des scanners corporels dans les aéroports, concept d'e-mobilité, etc.). Il portera également son attention sur les échanges de données à grande échelle qui peuvent se produire au sein du système d'information sur le marché intérieur (IMI).

- **Coopération avec les autorités chargées de la protection des données**

Le CEPD continuera de contribuer activement aux activités et aux succès du groupe de travail «Article 29», en faisant en sorte que le programme de travail du groupe soit conforme à ses propres priorités. Il veillera, de surcroît, à assurer une cohérence et à créer des synergies entre les avis qu'il émet et les positions prises par le groupe de travail. Enfin, il maintiendra des relations constructives avec les autorités nationales chargées de la protection des données. En sa qualité de rapporteur pour certains dossiers spécifiques, le CEPD dirigera les travaux et préparera l'adoption des avis du groupe de travail.

- **Contrôle coordonné**

La législation de l'Union impose de procéder à un contrôle coordonné pour Eurodac, pour le système d'information douanier et, à partir de la mi-2011, pour le système d'information sur les visas. Un des objectifs premiers du CEPD consistera à assurer un secrétariat efficace pour les autorités chargées de la protection des données qui participent au contrôle coordonné. En tant que contrôleur des systèmes d'information à grande échelle, le CEPD jouera un rôle actif dans les activités de contrôle coordonné des autorités et effectuera des audits de sécurité réguliers.

8.3. Autres domaines

- **Information et communication**

Le CEPD continuera de développer et d'améliorer ses activités d'information, de communication et de presse en mettant l'accent plus particulièrement sur la sensibilisation, les publications et l'information en ligne. Le CEPD préparera également le terrain pour une révision de sa stratégie de communication, en lançant notamment une consultation auprès des principales parties prenantes.

Cet exercice général sera complété par des évaluations plus ciblées de l'impact des principaux outils d'information et de communication.

- **Organisation interne**

Les principaux objectifs pour 2011 viseront à achever la réorganisation interne, à renouveler les efforts en matière de gestion des performances dans le contexte de la révision stratégique ainsi qu'à mettre au point et en oeuvre de nouveaux outils informatiques. L'accent sera mis sur le contrôle et les procédures internes, sur une meilleure répartition des ressources et sur l'amélioration de l'exécution budgétaire.

- **Gestion des ressources**

Le CEPD continuera d'investir des ressources dans le développement et la mise en oeuvre d'un système de gestion des cas. La priorité sera accordée à la conclusion d'accords de niveau de service avec la Commission européenne, aux fins de la mise en place d'applications informatiques dans le domaine des ressources humaines (dont les systèmes Syslog Formation, Sysper et MIPS (*Mission Processing System*)).

Annexe A —Cadre juridique

L'article 286 du traité CE, adopté en 1997 dans le cadre du traité d'Amsterdam, prévoit que les actes communautaires relatifs à la protection des personnes physiques en ce qui concerne le traitement des données à caractère personnel et la libre circulation de ces données sont applicables aux institutions et organes communautaires et qu'un organe indépendant de contrôle doit être institué.

Les actes communautaires visés dans cette disposition sont la directive 95/46/CE, qui définit le cadre général de la législation en matière de protection des données dans les États membres, et la directive 97/66/CE, une directive particulière qui a été remplacée par la directive 2002/58/CE sur la vie privée et les communications électroniques. Ces deux directives peuvent être considérées comme le résultat d'une évolution du cadre juridique qui a commencé au début des années 70 au sein du Conseil de l'Europe (voir ci-dessous).

En vertu de l'article 286 TCE, le Contrôleur européen de la protection des données a été créé par le règlement (CE) n° 45/2001 du Parlement européen et du Conseil relatif à la protection des personnes physiques en ce qui concerne le traitement des données à caractère personnel par les institutions et organes communautaires et la libre circulation des données, entré en vigueur en 2001([23]). Ce règlement a également décrit les règles appropriées pour les institutions et les organes conformément aux deux directives.

Depuis l'entrée en vigueur du traité de Lisbonne, l'article 286 susmentionné a été remplacé par l'article 16 du traité sur le fonctionnement de l'Union européenne, qui souligne l'importance de la protection des données de manière plus générale. L'article 16 TFUE et l'article 8 de la charte des droits fondamentaux de l'UE - désormais contraignante - prévoient que le respect des règles en matière de protection des données doit être soumis à un contrôle exercé par une autorité indépendante.

Historique du dossier

L'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales consacre le droit au respect de la vie privée et familiale et définit les conditions dans lesquelles ce droit peut faire l'objet de restrictions. Cependant, en 1981, on a jugé nécessaire d'adopter une convention distincte en matière de protection des données, afin de développer une approche positive et structurelle de la protection des droits fondamentaux et des libertés fondamentales, qui peut être affectée par le traitement des données à caractère personnel dans une société moderne. Cette convention, également appelée «Convention 108», a à ce jour été ratifiée par plus de 40 pays membres du Conseil de l'Europe, dont l'ensemble des États membres de l'UE.

La directive 95/46/CE a repris les principes de la Convention 108, en les précisant et en les développant de diverses manières. L'objectif était d'assurer un niveau élevé de protection et de permettre la libre circulation des données à caractère personnel au sein de l'UE. Quand la Commission a présenté la proposition de directive au début des années 90, elle a indiqué que les institutions et les organes de la Communauté devraient être couverts par des garanties légales similaires qui leur permettraient ainsi de participer à la libre circulation des données personnelles soumises à des règles équivalentes de protection. Toutefois il n'existait, jusqu'à l'adoption

([23]) JO L 8 du 12.1.2001, p. 1.

de l'article 286 TCE, aucune base juridique pour un tel instrument.

Le traité de Lisbonne, signé en décembre 2007 et soumis à la ratification de tous les États membres, renforce la protection des droits fondamentaux de diverses manières. Le respect de la vie privée et familiale et la protection des données à caractère personnel sont traités comme des droits fondamentaux distincts aux articles 7 et 8 de la charte des droits fondamentaux de l'UE, qui est devenue juridiquement contraignante. La protection des données est également traitée comme une question horizontale à l'article 16 du traité sur le fonctionnement de l'UE. Il est ainsi manifeste que la protection des données est considérée comme un élément fondamental d'une bonne gestion des affaires publiques. Le contrôle indépendant est un élément essentiel de cette protection.

Règlement (CE) n° 45/2001

En regardant de plus près le règlement, il convient de noter dans un premier temps qu'en vertu de son article 3, paragraphe 1, il s'applique au «traitement de données à caractère personnel par toutes les institutions et tous les organes communautaires, dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire». Cependant, depuis l'entrée en vigueur du traité de Lisbonne et l'abolition de la structure en piliers - qui rendent les références aux «institutions communautaires» et au «droit communautaire» désormais obsolètes - le règlement couvre en principe toutes les institutions et tous les organes de l'Union européenne, sauf disposition contraire spécifique dans d'autres actes législatifs de l'Union. Les conséquences précises de ces changements font encore l'objet d'un examen et pourraient nécessiter une clarification supplémentaire.

Les définitions et la teneur du règlement s'inspirent très largement des principes de la directive 95/46/CE. On pourrait dire que le règlement (CE) n° 45/2001 constitue la mise en œuvre de cette directive au niveau européen. Il traite ainsi des principes généraux tels que le traitement loyal et licite, la proportionnalité et la compatibilité d'utilisation, les catégories particulières de données sensibles, l'information de la personne concernée, les droits de la personne concernée, les obligations des responsables du traitement - en tenant compte, le cas échéant, des circonstances propres au niveau de l'UE -, ainsi que du contrôle, de l'exécution et des recours. Un chapitre particulier est consacré à la protection des données à caractère personnel et de la vie privée dans le cadre des réseaux internes de télécommunications. Ce chapitre constitue en fait la mise en œuvre au niveau européen de la directive 97/66/CE sur la vie privée et les communications électroniques.

Une des caractéristiques intéressantes du règlement est l'obligation qui est faite aux institutions et organes de l'Union de désigner au moins un délégué à la protection des données (DPD). Ces délégués sont chargés d'assurer, d'une manière indépendante, l'application interne des dispositions du règlement, y compris la notification appropriée des opérations de traitement. Des délégués sont désormais en place dans toutes les institutions communautaires et dans la plupart des organes, pour certains depuis plusieurs années. Des travaux importants ont donc été accomplis pour mettre en œuvre le règlement, même en l'absence d'un organe de contrôle. Ces délégués peuvent d'ailleurs être mieux placés pour fournir des conseils ou intervenir à un stade précoce et pour contribuer à la mise au point de bonnes pratiques. Les délégués à la protection des données ayant l'obligation formelle de coopérer avec le CEPD, il s'est formé un réseau très important et fort apprécié, qu'il convient de développer encore (voir point 2.2).

Tâches et compétences du CEPD

Les tâches et les compétences du Contrôleur européen de la protection des données sont clairement énoncées aux articles 41, 46 et 47 du règlement (voir annexe B), à la fois en termes généraux et spécifiques. L'article 41 définit la mission principale du CEPD, qui consiste à veiller à ce que les libertés et les droits fondamentaux des personnes physiques, notamment leur vie privée, en ce qui concerne le traitement des données à caractère personnel, soient respectés par les institutions et organes de l'Union. Il fixe aussi dans leurs grandes lignes certains aspects de cette mission. Ces responsabilités générales sont développées et précisées aux articles 46 et 47, lesquels comportent une énumération détaillée des fonctions et des compétences.

Cette présentation des attributions, fonctions et compétences suit, pour l'essentiel, le même schéma que pour les autorités nationales de contrôle: entendre et examiner les réclamations, effectuer d'autres enquêtes, informer le responsable du traitement et les personnes concernées, effectuer des contrôles préalables lorsque les opérations de traitement

présentent des risques particuliers, etc. Le règlement habilite le CEPD à obtenir accès à toutes les informations utiles et aux locaux pertinents lorsque cela est nécessaire pour ses enquêtes. Le CEPD peut aussi imposer des sanctions et saisir la Cour de justice. Ces activités de contrôle sont examinées de façon plus approfondie dans le chapitre 2 du présent rapport.

Certaines tâches revêtent une nature particulière. La tâche consistant à conseiller la Commission et les autres institutions communautaires à propos des nouvelles dispositions législatives - confirmée à l'article 28, paragraphe 2, par l'obligation formelle qui est faite à la Commission de consulter le CEPD lorsqu'elle adopte une proposition de législation relative à la protection des données à caractère personnel - concerne aussi les projets de directive et les autres mesures destinées à s'appliquer au niveau national ou à être transposées en droit national. Il s'agit d'une fonction stratégique qui permet au CEPD de se pencher, très tôt, sur les implications possibles au regard de la protection de la vie privée et d'envisager d'autres solutions éventuelles, y compris dans l'ancien troisième pilier (coopération policière et judiciaire en matière pénale). Surveiller les faits nouveaux qui présentent un intérêt et qui pourraient avoir une incidence sur la protection des données à caractère personnel et intervenir dans les affaires portées devant la Cour de justice constituent d'autres tâches importantes. Ces activités consultatives du CEPD sont examinées plus en détail dans le chapitre 3 du présent rapport.

La coopération avec les autorités nationales de contrôle et avec les organes de contrôle relevant de l'ancien troisième pilier a une incidence similaire. En tant que membre du groupe de travail «Article 29» sur la protection des données, qui a été institué pour conseiller la Commission européenne et pour développer des politiques harmonisées, le CEPD a la possibilité de contribuer aux travaux réalisés à ce niveau. La coopération avec les organes de contrôle relevant de l'ancien troisième pilier lui permet d'observer les faits nouveaux qui surviennent dans ce contexte et de contribuer à l'élaboration d'un cadre plus cohérent et homogène pour la protection des données à caractère personnel, quel que soit le «pilier» ou le contexte particulier concerné. Cette coopération est traitée plus en détail au chapitre 4 du présent rapport.

Annexe B. — Extrait du règlement (CE) n° 45/2001

Article 41 — Le Contrôleur européen de la protection des données

1. Il est institué une autorité de contrôle indépendante dénommée le Contrôleur européen de la protection des données.

2. En ce qui concerne le traitement de données à caractère personnel, le Contrôleur européen de la protection des données est chargé de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, soient respectés par les institutions et organes communautaires.

Le Contrôleur européen de la protection des données est chargé de surveiller et d'assurer l'application des dispositions du présent règlement et de tout autre acte communautaire concernant la protection des libertés et droits fondamentaux des personnes physiques à l'égard des traitements de données à caractère personnel effectués par une institution ou un organe communautaire ainsi que de conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel. À ces fins, il exerce les fonctions prévues à l'article 46 et les compétences qui lui sont conférées à l'article 47.

Article 46 — Fonctions

Le Contrôleur européen de la protection des données:

a) entend et examine les réclamations et informe la personne concernée des résultats de son examen dans un délai raisonnable;

b) effectue des enquêtes, soit de sa propre initiative, soit sur la base d'une réclamation et informe les personnes concernées du résultat de ses enquêtes dans un délai raisonnable;

c) contrôle et assure l'application du présent règlement et de tout autre acte communautaire relatifs à la protection des personnes physiques à l'égard du traitement de données à caractère personnel par une institution ou un organe communautaire, à l'exclusion de la Cour de justice

des Communautés européennes dans l'exercice de ses fonctions juridictionnelles;

d) conseille l'ensemble des institutions et organes communautaires, soit de sa propre initiative, soit en réponse à une consultation pour toutes les questions concernant le traitement de données à caractère personnel, en particulier avant l'élaboration par ces institutions et organes de règles internes relatives à la protection des libertés et droits fondamentaux des personnes à l'égard du traitement des données à caractère personnel;

e) surveille les faits nouveaux présentant un intérêt, dans la mesure où ils ont une incidence sur la protection des données à caractère personnel, notamment l'évolution des technologies de l'information et des communications;

f) i) coopère avec les autorités nationales de contrôle mentionnées à l'article 28 de la directive 95/46/CE des pays auxquels cette directive s'applique dans la mesure nécessaire à l'accomplissement de leurs devoirs respectifs, notamment en échangeant toutes informations utiles, en demandant à une telle autorité ou à un tel organe d'exercer ses pouvoirs ou en répondant à une demande d'une telle autorité ou d'un tel organe;

ii) coopère également avec les organes de contrôle de la protection des données institués en vertu du titre VI du traité sur l'Union européenne en vue notamment d'améliorer la cohérence dans l'application des règles et procédures dont ils sont respectivement chargés d'assurer le respect;

g) participe aux activités du groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive 95/46/CE;

h) détermine, motive et rend publiques les exceptions, garanties, autorisations et conditions mentionnées à l'article 10, paragraphe 2, point b), à l'article 10, paragraphes 4, 5 et 6, à l'article 12, paragraphe 2, à l'article 19 et à l'article 37, paragraphe 2;

i) tient un registre des traitements qui lui ont été notifiés en vertu de l'article 27, paragraphe 2, et enregistrés conformément à l'article 27, paragraphe 5, et fournit les moyens d'accéder aux registres tenus par les délégués à la protection des données en application de l'article 26;

j) effectue un contrôle préalable des traitements qui lui ont été notifiés;

k) établit son règlement intérieur.

Article 47 — Compétences

1. Le Contrôleur européen de la protection des données peut:

a) conseiller les personnes concernées dans l'exercice de leurs droits;

b) saisir le responsable du traitement en cas de violation alléguée des dispositions régissant le traitement des données à caractère personnel et, le cas échéant, formuler des propositions tendant à remédier à cette violation et à améliorer la protection des personnes concernées;

c) ordonner que les demandes d'exercice de certains droits à l'égard des données soient satisfaites lorsque de telles demandes ont été rejetées en violation des articles 13 à 19;

d) adresser un avertissement ou une admonestation au responsable du traitement;

e) ordonner la rectification, le verrouillage, l'effacement ou la destruction de toutes les données lorsqu'elles ont été traitées en violation des dispositions régissant le traitement de données à caractère personnel et la notification de ces mesures aux tiers auxquels les données ont été divulguées;

f) interdire temporairement ou définitivement un traitement;

g) saisir l'institution ou l'organe concerné et, si nécessaire, le Parlement européen, le Conseil et la Commission;

h) saisir la Cour de justice des Communautés européennes dans les conditions prévues par le traité;

i) intervenir dans les affaires portées devant la Cour de justice des Communautés européennes.

2. Le Contrôleur européen de la protection des données est habilité à:

a) obtenir d'un responsable du traitement ou d'une institution ou d'un organe communautaire l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires à ses enquêtes;

b) obtenir l'accès à tous les locaux dans lesquels un responsable du traitement ou une institution ou un organe communautaire exerce ses activités s'il existe un motif raisonnable de supposer que s'y exerce une activité visée par le présent règlement.

Annexe C — Liste des abréviations

ACAC	Accord commercial anti-contrefaçon
SID	Système d'information douanier
CC	Cour des comptes
CdR	Comité des régions
CPAS	Comité de préparation pour les affaires sociales
DAS	Déclaration d'assurance
DG INFSO	Direction générale de la société de l'information et des médias
DG MARKT	Direction générale du marché intérieur et des services
DIGIT	Direction générale de l'informatique
APD	Autorité chargée de la protection des données
CPD	Coordinateur de la protection des données
DPD	Délégué à la protection des données
EEA	École européenne d'administration
AESA	Agence européenne de la sécurité aérienne
CE	Communautés européennes
BCE	Banque centrale européenne
ECDC	Centre européen pour la prévention et de contrôle des maladies
CJE	Cour de justice européenne
AEE	Agence européenne pour l'environnement
EFSA	Autorité européenne de sécurité des aliments
BEI	Banque européenne d'investissement
DEE	Décision d'enquête européenne
ENISA	Agence européenne chargée de la sécurité des réseaux et de l'information
CEDH	Convention européenne des droits de l'homme
DPE	Décision de protection européenne
EPSO	Office européen de sélection du personnel
ERCEA	Agence exécutive du Conseil européen de la recherche
UE	Union européenne
RAPS	Système d'alerte précoce et de réaction
FRA	Agence des droits fondamentaux de l'Union européenne
RH	Ressources humaines
SAI	Service d'audit interne
TIC	Technologies de l'information et de la communication
IMI	Système d'information sur le marché intérieur
OIM	Organisation internationale pour les migrations
SSI	Stratégie de sécurité intérieure

TI	Technologies de l'information
CCR	Centre commun de recherche
ORC	Opération de retour conjointe
ACC	Autorité de contrôle commune
CGAM	Comité de gestion du régime commun d'assurance maladie
LIBE	Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen
RLSI	Responsable local de la sécurité informatique
RLS	Responsable local de la sécurité
OHMI	Office de l'harmonisation dans le marché intérieur
OLAF	Office européen de lutte antifraude
PNR	Dossier passager (Passenger Name Record)
R&D	Recherche et développement
RFID	Identification par radiofréquence
SIS	Système d'information Schengen
END	Expert national détaché
CSO	Centre de service et d'opération
s-TESTA	Services télématiques transeuropéens sécurisés entre administrations
SWIFT	Société de télécommunications interbancaires mondiales
TFTP	Programme de surveillance du financement du terrorisme
TFUE	Traité sur le fonctionnement de l'Union européenne
TURBINE	TrUsted Revocable Biometrics IdeNtitiEs
HCR	Haut commissariat des Nations unies pour les réfugiés
VIS	Système d'information sur les visas
OMD	Organisation mondiale des douanes
WP 29	Groupe de travail «Article 29» sur la protection des données
GTPJ	Groupe de travail sur la police et la justice

Annexe D — Liste des délégués à la protection des données

ORGANISATION	NOM	ADRESSE ELECTRONIQUE
Parlement européen (PE)	Jonathan STEELE	Data-Protection@europarl.europa.eu
Conseil de l'Union européenne (Consilium)	Pierre VERNHES	Data.Protection@consilium.europa.eu
Commission européenne (CE)	Philippe RENAUDIÈRE	Data-Protection-officer@ec.europa.eu
Cour de justice des Communautés européennes (CURIA)	Marc SCHAUSS	Dataprotectionofficer@curia.europa.eu
Cour des comptes européenne	Johan VAN DAMME	Data-Protection@eca.europa.eu
Comité économique et social européen (CESE)	Maria ARSENE	Data.Protection@eesc.europa.eu
Comité des régions (CdR)	Rastislav SPÁC	Data.Protection@cor.europa.eu
Banque européenne d'investissement (EIB)	Jean-Philippe MINNAERT	Dataprotectionofficer@eib.org
Médiateur européen	Loïc JULIEN	DPO-euro-ombudsman@ombudsman.europa.eu
Contrôleur européen de la protection des données (CEPD)	Alfonso SCIROCCO, Sylvie PICARD (DPD adjointe)	alfonso.scirocco@edps.europa.eu
Banque centrale européenne (BCE)	Frederik MALFRÈRE	DPO@ecb.int
Office européen de lutte antifraude (OLAF)	Laraine LAUDATI	Laraine.Laudati@ec.europa.eu
Centre de traduction des organes de l'Union européenne (CdT)	Benoît VITALE	Data-Protection@cdt.europa.eu
Office de l'harmonisation dans le marché intérieur (OHMI)	Ignacio DE MEDRANO CABALLERO	DataProtectionOfficer@oami.europa.eu
Agence des droits fondamentaux de l'Union européenne (FRA)	Nikolaos FIKATAS	Nikolaos.Fikatas@fra.europa.eu
Agence européenne des médicaments (EMEA)	Vincenzo SALVATORE	Data.Protection@emea.europa.eu
Office communautaire des variétés végétales (OCVV)	Véronique DOREAU	Doreau@cpvo.europa.eu
Fondation européenne pour la formation (ETF)	Liia KAARLOP	Liia.Kaarlop@etf.europa.eu
Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)	Emmanuel MAURAGE	Dataprotection@enisa.europa.eu
Fondation européenne pour l'amélioration des conditions de travail (Eurofound)	Markus GRIMMEISEN	MGR@eurofound.europa.eu

>>>

ORGANISATION	NOM	ADRESSE ELECTRONIQUE
Observatoire européen des drogues et des toxicomanies (EMCDDA)	Cecile MARTEL	Cecile.Martel@emcdda.europa.eu
Autorité européenne de sécurité des aliments (EFSA)	Claus RÉUNIS	Dataprotectionofficer@efsa.europa.eu
Agence européenne pour la sécurité maritime (AESM)	Malgorzata NESTEROWICZ	Malgorzata.Nesterowicz@emsa.europa.eu
Centre européen pour le développement de la formation professionnelle (Cedefop)	Spyros ANTONIOU	Spyros.Antoniou@cedefop.europa.eu
Agence exécutive «Éducation, audiovisuel et culture» (EACEA)	Hubert MONET	eacea-data-protection@ec.europa.eu
Agence européenne pour la sécurité et la santé au travail (OSHA)	Terry TAYLOR	Taylor@osha.europa.eu
Agence communautaire de contrôle des pêches (ACCP)	Clara FERNANDEZ/ Rieke ARNDT	cfca-dpo@cfca.europa.eu
Autorité de surveillance du GNSS européen (ASG)	Triinu VOLMER	Triinu.Volmer@gsa.europa.eu
Agence ferroviaire européenne (ERA)	Guido STÄRKLE (DPD faisant fonction)	Dataprotectionofficer@era.europa.eu
Agence exécutive pour la santé et les consommateurs (EAHC)	Beata HARTWIG	Beata.Hartwig@ec.europa.eu
Centre européen pour la prévention et le contrôle des maladies (ECDC)	Elisabeth ROBINO	Elisabeth.Robino@ecdc.europa.eu
Agence européenne pour l'environnement (AEE)	Gordon McINNES	Gordon.McInnes@eea.europa.eu
Fonds européen d'investissement (FEI)	Jobst NEUSS	J.Neuss@eif.org
Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures (Frontex)	Sakari VUORENSOLA	Sakari.Vuorensola@frontex.europa.eu
Agence européenne de la sécurité aérienne (AESA)	Francesca PAVESI	Francesca.Pavesi@easa.europa.eu
Agence exécutive pour la compétitivité et l'innovation (EACI)	Elena FIERRO SEDANO	Elena.Fierro-Sedano@ec.europa.eu
Agence européenne du réseau transeuropéen de transport (AE RTE-T)	Zsófia SZILVÁSSY	Zsofia.Szilvassy@ec.europa.eu
Agence européenne des produits chimiques (ECHA)	Alain LEFÈBVRE	Minna.Heikkila@echa.europa.eu
Agence exécutive du Conseil européen de la recherche (ERCEA)	Donatella PIATTO	Donatella.Piatto@ec.europa.eu
Agence exécutive pour la recherche (REA)	Evangelos TSAVALOPOULOS	Evangelos.Tsavalopoulos@ec.europa.eu

>>>

ORGANISATION	NOM	ADRESSE ELECTRONIQUE
Fusion à des fins énergétiques (Entreprise commune pour ITER et le développement de l'énergie de fusion)	Radoslav HANAK	Radoslav.Hanak@f4e.europa.eu
Entreprise commune Sesar (SESAR)	Daniella PAVKOVIC	Daniella.Pavkovic@sesarju.eu
Entreprise commune Artemis	Anne SALAÜN	Anne.Salaun@artemis-ju.europa.eu
Entreprise commune Clean Sky	Silvia POLIDORI	Silvia.Polidori@cleansky.eu
Initiative Médicaments innovants (IMI)	Estefania RIBEIRO	Estefania.Ribeiro@imi.europa.eu
Entreprise commune Piles à combustible et hydrogène	Nicolas BRAHY	Nicolas.Brahy@fch.europa.eu
Institut européen d'innovation et de technologie (EIT)	Camilo SOARES	Camilo.Soares@ext.ec.europa.eu

Annexe E — Liste des avis rendus à la suite d'un contrôle préalable

Analyse empirique des corrélations entre les variables du système de travail et le processus décisionnel - OHMI

Avis du 22 novembre 2010 sur la notification d'un contrôle préalable reçue de l'Office de l'harmonisation dans le marché intérieur (OHMI), le 22 juillet 2010, sur l'«analyse empirique des corrélations entre les variables du système de travail et le processus décisionnel» (dossier 2010-0468)

Procédures relatives au recrutement d'agents - BEI

Avis du 11 novembre 2010 sur la notification d'un contrôle préalable concernant les procédures relatives au recrutement d'agents (dossier 2009-0254)

Procédure de recrutement et outil de candidature électronique - AESA

Lettre du 19 octobre 2010 sur la notification d'un contrôle préalable concernant le traitement intitulé «procédure de recrutement et outil de candidature électronique de l'AESA» (dossier 2010-0466)

Procédures relatives aux enquêtes pour fraude - BEI

Avis du 14 octobre 2010 sur la notification d'un contrôle préalable concernant les procédures relatives aux enquêtes pour fraude au sein du groupe BEI (dossier 2009-0459)

Détachement d'experts nationaux - CdR

Lettre du 5 octobre 2010 sur la notification d'un contrôle préalable concernant le détachement d'experts nationaux au Comité des régions (dossier 2010-0515)

Traitement des donné personnelles dans le cadre de déductions de salaire en cas de grève - BCE

Avis du 28 septembre 2010 sur la notification de contrôle préalable concernant le traitement de données à caractère personnel dans le cadre de déductions de salaire en cas de grève (dossier 2009-0514)

Sélection et recrutement du personnel - AESC

Lettre du 24 septembre 2010 relative à une notification de contrôle préalable concernant la sélection et au recrutement du personnel (agents temporaires détachés ou non par la Commission européenne, agents contractuels, personnel intérimaire et stagiaires) à l'Agence exécutive pour la santé et les consommateurs (dossier 2010-0346)

Sélection de réviseurs externes - Commission (Office des publications)

Avis du 6 septembre 2010 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Commission européenne concernant la «Liste des participants à un examen pour réviseurs contractuels» (dossier 2010-400)

Inspections de sécurité - Commission européenne (Centre commun de recherche, Ispra)

Avis du 6 septembre 2010 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Commission européenne concernant les «Inspections de sécurité sur le site du CCR d'Ispra» (dossier 2009-682)

Système européen de surveillance («TESSy») - ECDC

Avis du 3 septembre 2010 sur la notification d'un contrôle préalable concernant le système européen de surveillance (TESSy) du Centre européen de prévention et de contrôle des maladies (ECDC) (dossier 2009-0474)

Politique de l'AESA visant à protéger la dignité de la personne et à prévenir le harcèlement moral et sexuel

Avis du 29 juillet 2010 sur la notification d'un contrôle préalable concernant «la politique de l'AESA visant à protéger la dignité de la personne et à prévenir le harcèlement moral et sexuel» (dossier 2010-318)

Mise en œuvre de la procédure informelle de traitement des cas de harcèlement psychologique et sexuel - CESE

Avis du 28 juillet 2010 sur la notification d'un contrôle préalable à propos du dossier «Mise en œuvre de la procédure informelle de traitement des cas de

harcèlement psychologique et sexuel au sein du Comité» (dossier 2010-321)

Sélection et recrutement d'agents temporaires et contractuels, d'experts nationaux détachés et de stagiaires - ECHA

Lettre du 27 juillet 2010 sur la notification de contrôle préalable concernant la Sélection et le recrutement d'agents temporaires et contractuels, d'experts nationaux détachés et de stagiaires à l'ECHA (dossier 2010-0109)

Traitement de données à caractère personnel dans le contexte d'un suivi des processus de qualité - Conseil

Avis du 26 juillet 2010 sur la notification d'un contrôle préalable concernant le traitement de données à caractère personnel dans le contexte d'un suivi des processus de qualité (dossier 2009-0295)

Suites administratives données aux absences pour maladie injustifiées - Conseil

Avis du 22 juillet 2010 sur la notification d'un contrôle préalable à propos du dossier «Suites administratives données aux absences pour maladie injustifiées» (dossier 2009-0687)

Procédure d'attestation des fonctionnaires - OEDT

Lettre du 22 juillet 2010 relative à une notification de contrôle préalable concernant les activités de traitement liées à la procédure d´attestation des fonctionnaires de l´OEDT (dossier 2010-0407)

Procédures relatives à l'«outil 360° de retour d'informations sur les compétences en leadership» - BEI

Avis du 20 juillet 2010 sur la notification d'un contrôle préalable au sujet des procédures relatives à l'«outil 360° de retour d'informations sur les compétences en leadership» (dossier 2009-0215)

Procédure de promotion des fonctionnaires et des agents - CESE

Avis du 19 juillet 2010 sur la notification d'un contrôle préalable à propos de la «procédure de promotion des fonctionnaires et des agents» (dossier 2008-474)

Sélection et le recrutement de personnel non permanent - BEI

Lettre du 14 juillet 2010 sur la notification d'un contrôle préalable concernant la sélection et le recrutement de personnel non permanent à la Banque européenne d'investissement (dossier 2009-678)

Consultation et mise à jour de la base de données centrale des exclusions - Comité des Régions

Avis du 4 juin 2010 sur la notification d'un contrôle préalable à propos du dossier «procédures à appliquer pour la consultation et la mise à jour de la base de données centrale des exclusions» (dossier 2010-248)

Procédure de traitement des cas d'insuffisance professionnelle - Conseil

Avis du 4 juin 2010 sur la notification d'un contrôle préalable à propos du dossier «procédure de traitement des cas d'insuffisance professionnelle au Secrétariat Général du Conseil» (dossier 2010-237

Gestion et évaluation par la DG TRAD des traductions externes - Parlement

Avis du 4 juin 2010 sur la notification d'un contrôle préalable concernant «La gestion et l'évaluation par la DG TRAD des traductions externes» (dossier 2009-0827)

Procédure de sélection des intérimaires - Commission

Avis du 4 juin 2010 sur la notification d'un contrôle préalable concernant la procédure de sélection des intérimaires (dossier 2008-704)

Inscription d'une personne concernée dans la base de données centrale des exclusions - Commission

Avis du 26 mai 2010 sur la notification d'un contrôle préalable à propos du traitement de données à caractère personnel eu égard à l'«inscription d'une personne concernée dans la base de données centrale des exclusions» (dossier 2009-0681)

Procédure de nomination des directeurs généraux/directeurs/chefs d'unité - Parlement européen

Avis du 20 mai 2010 sur une notification en vue d'un contrôle préalable concernant la procédure de nomination des directeurs généraux/directeurs/chefs d'unité (dossier 2010-0270)

Recrutement d'experts nationaux détachés (END) et de stagiaires - Centre européen de prévention et de contrôle des maladies (ECDC)

Lettre du 19 mai 2010 relative à la notification d'un contrôle préalable concernant le recrutement d'experts nationaux détachés (END) et de stagiaires (dossier 2009-0453)

Recrutement d'agents temporaires et contractuels - Agence Européenne pour l'Environnement (AEE)

Lettre du 19 mai 2010 relative à la notification d'un contrôle préalable concernant le recrutement d'agents temporaires et contractuels (dossier 2009-0467)

Aides psycho-sociales et financières - Centre Commun de Recherche (CCR)

Avis du 10 mai 2010 sur la notification d'un contrôle préalable à propos des aides psycho-sociales et financières au Centre Commun de Recherche (CCR ITU) à Karlsruhe (dossier 2008-713)

Collecte de noms et de certaines données pertinentes des rapatriés pour des opérations de retour conjointes - FRONTEX

Avis du 26 avril 2010 sur la notification d'un contrôle préalable à propos du traitement de la «Collecte de noms et de certaines données pertinentes des rapatriés pour des opérations de retour conjointes (ORC)» (dossier 2009-0681)

Système d'alerte précoce et de réaction («SAPR») - Commission européenne

Avis du 26 avril 2010 sur une notification de contrôle préalable sur le système d'alerte précoce et de réaction («SAPR») (dossier 2009-0137)

Promotion interne des fonctionnaires et reclassement des agents temporaires - EMCDDA

Avis du 22 avril 2010 sur la notification de contrôle préalable relatif à «la promotion interne des fonctionnaires et le reclassement des agents temporaires» (dossier 2009-0839)

Traitements de données dans le cadre de la gestion des appels d'offres - ETF

Avis du 22 avril 2010 sur une notification de contrôle préalable concernant les traitements de données dans le cadre de la gestion des appels d'offre (dossier 2009-0037)

Traitement de l'insuffisance professionnelle - Cour de Justice

Avis du 21 avril 2010 sur la notification d'un contrôle préalable à propos du dossier «traitement de l'insuffisance professionnelle» (dossier 2009-860)

Enquêtes administratives et procédures disciplinaires - EMA

Avis du 21 avril 2010 sur une notification de contrôle préalable relative au traitement de données personnelles lors d'enquêtes administratives et de procédures disciplinaires (dossier 2010-0047)

Procédures de passation des marchés et appels à manifestation d'intérêt pour la sélection d'experts - Commission

Avis du 15 avril 2010 sur le modèle de notification de contrôle préalable concernant le dossier «Procédures de passation des marchés et appels à manifestation d'intérêt pour la sélection d'experts» (dossier 2009-570)

Efficacité du leadership - Commission

Avis du 7 avril 2010 sur une notification de contrôle préalable relatif à l'«efficacité du leadership» (dossier 2010-0002)

Procédures de sélection du personnel par des panels - BEI

Avis du 26 mars 2010 sur la notification d'un contrôle préalable à propos du dossier «procédures relatives à la sélection du personnel par des panels» (dossier 2009-679)

Gestion des congés - Parlement

Avis du 25 mars 2010 sur la notification d'un contrôle préalable concernant la gestion des congés (dossier 2009-595)

Fichier manuel de documents relatifs aux handicaps des visiteurs - Parlement européen

Avis du 16 mars 2010 sur la notification en vue d'un contrôle préalable concernant le «fichier manuel de documents relatifs aux handicaps des visiteurs» (dossier 2009-564)

Mobilité interne - OHMI

Avis du 15 mars 2010 sur la notification en vue d'un contrôle préalable, reçue de l'Office pour l'harmonisation du marché intérieur, concernant la mobilité interne (dossier 2008-426)

EEA - Inventaire d'auto-perception BELBIN - Commission européenne

Avis du 15 mars 2010 sur une notification en vue d'un contrôle préalable reçue du délégué à la protection des données de la Commission européenne concernant l'«inventaire d'auto-perception BELBIN - EEA» (dossier 2009-377)

Évaluation des performances - EMCDDA

Avis reflété dans une lettre du 8 mars 2010 sur la notification en vue d'un contrôle préalable concernant l'évaluation des performances (dossier 2009-838)

Gestion des absences et des congés de maladie - CESE

Avis du 5 mars 2010 sur une notification de contrôle préalable relatif à la gestion des absences et des congés de maladie à l'aide de la base de données «Centurio» (dossiers 2009-0702 et 2009-0703)

Sélection de conseillers confidentiels - FRA

Avis du 10 février 2010 sur une notification de contrôle préalable concernant les procédures de sélection pour la sélection de conseillers confidentiels (dossier 2009-857)

Nomination de membres d'encadrement intermédiaire - Office communautaire des variétés végétales (OCVV)

Avis du 28 janvier 2010 sur la notification d'un contrôle préalable concernant la nomination de membres d'encadrement intermédiaire (dossier 2009-666)

e-Probation - Banque européenne d'investissement

Avis du 21 janvier 2010 sur la notification de contrôle préalable concernant le traitement de données à caractère personnel dans la gestion des périodes probatoires (e-probation) (dossier 2009-718)

Réclamations des affiliés - Comité de Gestion de l'Assurance maladie

Avis du 18 janvier 2010 sur la notification de contrôle préalable reçue du Comité de Gestion de l'Assurance maladie à propos du dossier «Réclamations des affiliés» (dossier 2009-070)

Accès au disque/courrier électronique privé - Cour des comptes

Avis du 18 janvier 2010 sur une notification en vue d'un contrôle préalable concernant la «procédure d'accès au disque/courrier électronique privé» (dossier 2009-620)

Annexe F — Liste des avis sur des propositions législatives

Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)

Avis du 20 décembre 2010 sur la proposition de règlement du Parlement européen et du Conseil concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)

La stratégie de sécurité intérieure de l'UE en action: cinq étapes vers une Europe plus sûre

Avis du 17 décembre 2010 sur la communication de la Commission «Stratégie de sécurité intérieure de l'UE en action: Cinq étapes vers une Europe plus sûre»

EURODAC

Avis du 15 décembre 2010 sur la création du système Eurodac pour la comparaison des empreintes digitales

Proposition de règlement sur la commercialisation et l'utilisation de précurseurs d'explosifs

Avis du 15 décembre 2010 sur la proposition de règlement sur la commercialisation et l'utilisation de précurseurs d'explosifs

La politique antiterroriste de l'UE: principales réalisations et défis à venir

Avis du 24 novembre 2010 sur la communication de la Commission au Parlement européen et au Conseil - «La politique antiterroriste de l'UE: principales réalisations et défis à venir»

Démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers

Avis du 19 octobre 2010 sur démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers

Décision de protection européenne et décision d'enquête européenne en matière pénale

Avis du 5 octobre 2010 sur la décision de protection européenne et la décision d'enquête européenne en matière pénale

Gestion de l'information dans l'espace de liberté, de sécurité et de justice

Avis du 30 septembre 2010 sur la communication de la Commission au Parlement européen et au Conseil - «Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice»

Systèmes de garantie des dépôts

Avis du 9 septembre 2010 sur la proposition de directive du Parlement européen et du Conseil relative aux systèmes de garantie des dépôts (refonte)

Traitement et transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme (TPTP II)

Avis du 22 juin 2010 sur la proposition de décision du Conseil sur la conclusion de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme (TFTP II)

Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures (Frontex)

Avis du 17 mai 2010 sur la proposition de règlement du Parlement européen et du Conseil adaptant le règlement du Conseil (CE) N° 2007/2004 établissant une Agence européenne pour la coopération aux frontières extérieures des États membres de l'Union européenne (FRONTEX)

Abus sexuels d'enfants et pédopornographie

Avis du 10 mai 2010 sur la proposition de directive du Parlement européenne et du Conseil relative à l'exploitation et aux abus sexuels concernant des enfants et à la pédopornographie, abrogeant la décision-cadre 2004/68/JAI

Initiative citoyenne

Avis du 21 avril 2010 sur la proposition de Règlement du Parlement européen et du Conseil relatif à l'initiative citoyenne

Déchets d'équipements électriques et électroniques (DEEE)

Avis du 14 avril 2010 sur la proposition de directive du Parlement européen et du Conseil relative aux déchets d'équipements électriques et électroniques (DEEE)

Promotion de la confiance dans la société d'information

Avis du 18 mars 2010 sur la promotion de la confiance dans la société d'information par des mesures d'encouragement de la protection des données et de la vie privée

Coopération douanière UE-Japon

Avis du 12 mars 2010 sur la proposition de décision du Conseil relative à une position à prendre par l'Union au sein du comité mixte de coopération douanière UE-Japon concernant la reconnaissance mutuelle des programmes relatifs aux opérateurs économiques agréés dans l'Union européenne et au Japon

Accord commercial anti-contrefaçon (ACAC)

Avis du 22 février 2010 sur les négociations en cours au sein de l'Union européenne pour un accord commercial anti-contrefaçon (ACAC)

Accidents et incidents dans l'aviation civile

Avis du 4 février 2010 sur la proposition de règlement du Parlement européen et du Conseil sur les enquêtes et la prévention des accidents et des incidents dans l'aviation civile

Coopération dans le domaine fiscal

Avis du 6 janvier 2010 sur la proposition de directive du Conseil relative à la coopération administrative dans le domaine fiscal

Annexe G — Discours du contrôleur et du contrôleur adjoint

Tout au long de l'année, le contrôleur et le contrôleur adjoint ont continué de consacrer beaucoup de temps et d'efforts à l'explication de leur mission et à la sensibilisation à la protection des données en général, ainsi qu'à un certain nombre de questions particulières, à l'occasion de discours et de contributions similaires devant différentes institutions et dans divers États membres.

Parlement européen – Commissions

27 janvier	Contrôleur adjoint, commission LIBE, politiques antiterroristes (Bruxelles)24*
4 mars	Contrôleur, commission LIBE, PNR et respect transatlantique de la vie privée (Bruxelles)*
21 juin	Contrôleur, commission LIBE, Charte des droits fondamentaux (Bruxelles)*
23 juin	Contrôleur, commission LIBE, accord TFTP II (Bruxelles)*
28 septembre	Contrôleur adjoint, commission LIBE, lutte contre les abus sexuels (Bruxelles)*
9 novembre	Contrôleur, commission PETI, accès du public aux documents (Bruxelles)*
15 novembre	Contrôleur et Contrôleur adjoint, commission LIBE, rapport annuel 2009 (Bruxelles)

Parlement européen - autres

28 janvier	Contrôleur, Journée de la protection des données (Bruxelles)
9 février	Contrôleur, Journée pour un internet plus sûr (Bruxelles)
16 mars	Contrôleur, députés européens, ACAC (Bruxelles)
24 mars	Contrôleur adjoint, Plate-forme de la vie privée: liberté sur l'internet (Bruxelles)
8 avril	Contrôleur, députés européens, PNR (Bruxelles)
1er décembre	Contrôleur, Plate-forme de la vie privée: examen de la protection des données (Bruxelles)

Conseil

19 janvier	Contrôleur adjoint, conférence sur l'ECRIS (Bruxelles)*
25 janvier	Contrôleur, représentation polonaise, Journée de la protection des données (Bruxelles)
11 février	Contrôleur, conférence sur la confiance dans les TIC (Leon)*
24 mars	Contrôleur, Groupe de travail sur la protection des données (Bruxelles)

Commission

28 janvier	Contrôleur, Journée de la protection des données, mini-symposium (Bruxelles)
28 janvier	Contrôleur, Journée de la protection des données, discours du déjeuner (Bruxelles)

* Texte disponible sur le site internet du CEPD

22 juin	Contrôleur, conférence sur les systèmes de transport intelligents (Bruxelles)*
29 juin	Contrôleur et Contrôleur adjoint, audience sur l'examen de la protection des données (Bruxelles)
22 septembre	Contrôleur, députés européens, groupe de travail sur les services de réseaux sociaux (Bruxelles)
5 octobre	Contrôleur, table ronde sur l'avenir de la protection des données à caractère personnel (Bruxelles)
18 novembre	Contrôleur, conférence de l'OLAF (Paris)*
3 décembre	Contrôleur, conférence sur la directive relative à la conservation des données (Bruxelles)*

Autres institutions et organes de l'Union européenne

27 janvier	Contrôleur adjoint, Journée de la protection des données à l'EMEA (Bruxelles)*
7 mai	Contrôleur, Agence des droits fondamentaux (Vienne)
27-28 mai	Contrôleur et Contrôleur adjoint, atelier sur les organisations internationales (Florence)
31 mai	Contrôleur, Protection des données et application de la loi (Trèves)*
7 juin	Contrôleur adjoint, CESE sur le harcèlement en ligne (Bratislava)25*
15-16 juin	Contrôleur et Contrôleur adjoint, Protection des données dans les procédures pénales (Madrid)
13 septembre	Contrôleur, université d'été ENISA-FORTH (Héraklion)
15 novembre	Contrôleur et Contrôleur adjoint, conférence de presse sur le rapport annuel 2009 (Bruxelles)*

Conférences internationales

30 janvier	Contrôleur, Ordinateurs, vie privée et protection des données (Bruxelles)
10 mars	Contrôleur, table ronde sur 30 ans de respect de la vie privée dans l'OCDE (Bruxelles)*
20 avril	Contrôleur, sommet mondial sur la vie privée de l'IAPP (Washington DC)26**
29 avril	Contrôleur et Contrôleur adjoint, Autorités européennes de protection des données (Prague)*
6 juillet	Contrôleur, Privacy Laws & Business (Cambridge)
25 octobre	Contrôleur adjoint, Voix publique de la société civile (Jérusalem)*
26 octobre	Contrôleur, 30 ans de lignes directrices de l'OCDE sur le respect de la vie privée (Jérusalem)
27 octobre	Contrôleur, vie privée et commissaires à la protection des données (Jérusalem)
28 octobre	Contrôleur adjoint, vie privée et commissaires à la protection des données (Jérusalem)*

Autres événements

22 janvier	Contrôleur adjoint, 30ème anniversaire du CRID (Namur)*

* Texte disponible sur le site internet du CEPD

** Vidéo disponible sur le site internet du CEPD

2 février	Contrôleur, Congrès policier européen (Berlin)*
26 février	Contrôleur, Propriété intellectuelle et société de l'information (Barcelone)*
5 mars	Contrôleur, colloque PLN (Bruxelles)
9 mars	Contrôleur, Chambre du commerce britannique en Belgique (Bruxelles) *
12 mars	Contrôleur adjoint, Éthique médicale et droits des patients (San Remo)
23 mars	Contrôleur, rencontre parlementaire conjointe sur la sécurité (Paris)*
26 mars	Contrôleur, mobilité mondiale et sécurité (Bruxelles)*
13 avril	Contrôleur, Journée européenne de sensibilisation à la sécurité informatique (Bruxelles)*
23 avril	Contrôleur, Chambre du commerce américaine dans l'Union européenne (Bruxelles)*
28 avril	Contrôleur adjoint, Conseil judiciaire (Rome)
11 mai	Contrôleur adjoint, atelier sur l'informatique dématérialisée (Bruxelles)
20 mai	Contrôleur, Data Protection Intensive (Londres)
1er juin	Contrôleur, Confiance numérique (Bruxelles)
2 juin	Contrôleur, L'internet des objets (Bruxelles)
8 juin	Contrôleur adjoint, table ronde sur la sécurité (Bruxelles)
15 juin	Contrôleur adjoint, traité de Lisbonne (Londres)
17 juin	Contrôleur adjoint, Forum des responsables de sécurité européens (Bruxelles)
22 juin	Contrôleur, Chambre du commerce américaine dans l'Union européenne (Bruxelles) *
23 juin	Contrôleur, Union européenne numérique et IAPP (Bruxelles)
29 juin	Contrôleur adjoint, CEPS sur les frontières et la justice pénale (Bruxelles)
8 juillet	Contrôleur adjoint, Alma Graduate School (Bologne)
12 juillet	Contrôleur adjoint, Conseil judiciaire (Rome)
7 septembre	Contrôleur, Future Security (Berlin)
15 septembre	Contrôleur, Vie privée et sécurité (Bruxelles)
16 septembre	Contrôleur, Conseil de Lisbonne sur le marché numérique (Bruxelles)
20 septembre	Contrôleur, Lutte contre le terrorisme et protection des données (Bruxelles)
23 septembre	Contrôleur, atelier sur la révision en matière de protection des données (Bruxelles)
28 septembre	Contrôleur, Protection des données et liberté de l'information (Budapest)
29 septembre	Contrôleur, sécurité de l'information et respect de la vie privée (Budapest)
29 septembre	Contrôleur adjoint, sécurité des frontières de l'Union européenne (Bruxelles)*

13 octobre	Contrôleur, Respect de la vie privée dans un monde numérique (Bruxelles)
22 octobre	Contrôleur adjoint, Justice pénale en Europe (Luxembourg)*
5 novembre	Contrôleur adjoint, Respect des règles en matière de respect de la vie privée (Rome)
17 novembre	Contrôleur adjoint, Transports intelligents (Milan)
23 novembre	Contrôleur, Vie privée et recherche scientifique (Bruxelles)*
23 novembre	Contrôleur adjoint, Recherche médicale et respect de la vie privée (Bruxelles)*
24 novembre	Contrôleur adjoint, séminaire sur la protection des données - message vidéo (Buenos Aires)
29 novembre	Contrôleur, Amis de l'Europe sur la protection des données dans l'Union européenne (Bruxelles)
30 novembre	Contrôleur, Forum Europe sur la protection des données dans l'Union européenne (Bruxelles)
30 novembre	Contrôleur, Forum Internet européen (Bruxelles)
2 décembre	Contrôleur, Hogan & Lovells (Londres)
9 décembre	Contrôleur, Éthique et gouvernance en biométrie (Bruxelles)*
10 décembre	Contrôleur adjoint, Droits des passagers européens (Bruxelles)*
16 décembre	Contrôleur, Assemblée sur l'avenir de l'internet (Gand)*

Annexe H — Composition du secrétariat du CEPD

Le CEPD, le Contrôleur adjoint et la plupart de leurs collaborateurs

Directeur a.i., chef du Secrétariat

Christopher DOCKSEY

• Contrôle et mise en application

Sophie LOUVEAUX *Responsable Contrôle et mise en application*	John-Pierre LAMB *Expert national détaché*
Laurent BESLAY *Coordinateur Sécurité et technologie*	Xanthi KAPSOSIDERI *Conseiller juridique*
Jaroslaw LOTARSKI *Coordinateur pour les réclamations*	Luisa PALLA *Assistante Contrôle et mise en application*
Maria Verónica PEREZ ASINARI *Coordinateur pour les consultations*	Dario ROSSI *Assistant Contrôle et mise en application* *Correspondant Comptabilité* *Gestionnaire de l'entrepôt externe de données (EDWM)*
Isabelle CHATELIER *Conseiller juridique*	Tereza STRUNCOVA *Conseiller juridique*
Bart DE SCHUITENEER *Conseiller Technologies* *Local Security Officer/LISO*	Michaël VANFLETEREN *Conseiller juridique*
Delphine HAROU *Conseiller juridique*	

• Politique législative et consultation

Hielke HIJMANS *Responsable Politique législative et consultation*	Raffaele DI GIOVANNI BEZZI *Assistant Politique législative et consultation*
Bénédicte HAVELANGE *Coordinatrice Grands systèmes TI et politique des frontières*	Herke KRANENBORG *Conseiller juridique*
Anne-Christine LACOSTE *Coordinatrice pour la coopération avec les APD*	Roberto LATTANZI *Expert national détaché*
Rosa BARCELO *Conseiller juridique*	Alfonso SCIROCCO *Délégué à la protection des données* *Gestion de la qualité*
Zsuzsanna BELENYESSY *Conseiller juridique*	Luis VELASCO *Conseiller Technologies*
Katarzyna CUADRAT-GRZYBOWSKA *Conseiller juridique*	

• Registre et assistance opérationnelle

Andrea BEACH *Responsable Registre et assistance opérationnelle*	Kim Thien LÊ *Assistante administrative*
Christine HUC *Assistante administrative*	Ewa THOMSON *Assistante administrative*
Kim DAUPHIN *Assistante administrative*	

• Information et communication

Nathalie VANDELLE *Responsable Information et communication*	Agnieszka NYKA *Assistante Information et communication*
Olivier ROSSIGNOL *Assistant Information et communication*	

• Ressources humaines, budget et administration

Leonardo CERVERA NAVAS *Responsable Ressources humaines, budget et administration*	Aida PASCU *Assistante administrative* *Assistante LSO*
Isabelle DELATTRE *Assistante Questions financières et comptabilité*	Sylvie PICARD *Délégué adjoint à la protection des données* *COFO - ICO*
Anne LEVÊCQUE *Assistante Ressources humaines* *GECO*	Anne-Françoise REYNDERS *Assistante administrative*
Vittorio MASTROJENI *Conseiller Ressources humaines*	Marian SANCHEZ LOPEZ *Conseiller Questions financières et comptabilité*

Le Contrôleur Européen de la Protection des Données

Rapport Annuel 2010

Luxembourg: Office des publications de l'Union européenne

2011 — 124 p. — 21 x 29,7 cm

ISBN 978-92-95073-21-0
doi:10.2804/21446

COMMENT VOUS PROCURER LES PUBLICATIONS DE L'UNION EUROPÉENNE?

Publications gratuites:

- sur le site EU Bookshop (http://bookshop.europa.eu);
- auprès des représentations ou des délégations de l'Union européenne. Vous pouvez obtenir leurs coordonnées en consultant le site http://ec.europa.eu ou par télécopieur au numéro +352 2929-42758.

Publications payantes:

- sur le site EU Bookshop (http://bookshop.europa.eu).

Abonnements facturés (par exemple séries annuelles du *Journal officiel de l'Union européenne*, recueils de la jurisprudence de la Cour de justice de l'Union européenne):

- auprès des bureaux de vente de l'Office des publications de l'Union européenne (http://publications.europa.eu/others/agents/index_fr.htm).

QT-AA-11-001-FR-N

LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

Le gardien européen
de la protection des données personnelles

www.edps.europa.eu

Office des publications

ISBN 978-92-95073-21-0