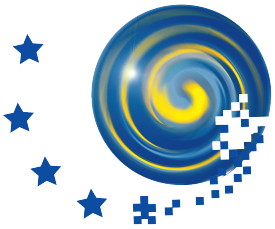
Rapport annuel
2005



CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

Adresse postale: rue Wiertz 60 — B-1047 Bruxelles
Bureau: rue Montoyer 63 — Bruxelles
E-mail: edps@edps.eu.int — Internet: www.edps.eu.int
Tél. (32-2) 283 19 00 — Fax (32-2) 283 19 50

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 bibliographique figure à la fin de l'ouvrage.

Luxembourg: Office des publications officielles des Communautés européennes, 2006

ISBN 92-95030-01-X

Printed in Luxembourg

IMPRIMÉ SUR PAPIER BLANCHI SANS CHLORE

Table des matières

Guide de l'utilisateur

Le lecteur trouvera à la suite de ce guide l'avant-propos de M. Peter Hustinx, le Contrôleur européen de la protection des données (CEPD), précédé de l'énoncé de ses missions.

Le chapitre 1 **«Bilan et perspectives»** présente une vue générale des activités du CEPD et décrit de façon détaillée le cadre juridique dans lequel elles s'inscrivent. Il met en lumière les résultats obtenus en 2005 et expose les objectifs retenus pour 2006.

Le chapitre 2 **«Contrôle»** décrit de façon complète les travaux menés pour vérifier que les institutions et organes de l'Union européenne (UE) s'acquittent de leurs obligations en matière de protection des données. La présentation générale est suivie d'une analyse du rôle des délégués à la protection des données (DPD) dans les administrations de l'UE. Ce chapitre comprend une analyse des contrôles préalables, plaintes et enquêtes traités en 2005 et résume les principales conclusions d'un document sur la transparence et l'accès du public aux documents qui a été publié en juillet 2005. Il comprend aussi une partie consacrée au contrôle des communications électroniques et une autre qui fait le point en ce qui concerne l'unité centrale d'Eurodac.

Le chapitre 3 **«Conseil»** traite du rôle consultatif du CEPD. Il est axé sur un document stratégique publié en mars et sur les avis relatifs à des propositions législatives et documents connexes, ainsi que sur leurs incidences. Ce chapitre comporte aussi une analyse des thèmes horizontaux et présente certaines nouveautés technologiques, telles que l'utilisation de la biométrie et l'identification par fréquence radio.

Le chapitre 4 **«Coopération»** décrit le travail effectué dans des forums importants tels que le Groupe de l'article 29, dans le cadre des autorités de contrôle communes relevant du troisième pilier et lors de la conférence européenne et de la conférence internationale des commissaires à la protection des données. Un compte rendu sur le séminaire organisé pour les organisations internationales clôt le chapitre.

Le chapitre 5 **«Communication»** présente la stratégie d'information et l'utilisation de différents outils de communication, tels que site internet, newsletters, service de presse et discours.

Le chapitre 6 **«Administration, budget et personnel»** décrit comment le bureau du CEPD a été consolidé durant sa deuxième année d'activité. Il passe en revue les aspects budgétaires, la question des ressources humaines et les accords de nature administrative.

Le rapport est complété d'**annexes,** dans lesquelles figurent des extraits du règlement (CE) n° 45/2001, une liste des abréviations, des statistiques concernant les contrôles préalables, la liste des délégués à la protection des données dans les institutions et organes, un descriptif de la composition du secrétariat, etc.

Une **synthèse** des principaux faits concernant l'année 2005 a été publiée séparément.

Pour de plus amples informations sur le CEPD, nous vous invitons à consulter notre site internet, qui reste notre premier outil de communication (www.edps.eu.int).

Il est possible de commander des exemplaires gratuits du rapport annuel ainsi que de la synthèse à l'adresse indiquée sur notre site internet.

Missions

Le Contrôleur européen de la protection des données a pour mission de veiller à ce que les institutions et organes communautaires, lorsqu'ils traitent des données à caractère personnel, respectent les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée. Le CEPD est chargé:

— de surveiller et d'assurer le respect des dispositions du règlement (CE) nº 45/2001 ainsi que d'autres actes communautaires concernant la protection des libertés et droits fondamentaux lorsque les institutions ou organes communautaires traitent des données à caractère personnel (contrôle);

— de conseiller les institutions et organes communautaires pour toutes les questions concernant le traitement de données à caractère personnel, y compris en réponse à une consultation dans le cadre de l'élaboration de dispositions législatives, et de surveiller les faits nouveaux ayant une incidence sur la protection des données à caractère personnel (conseil);

— de coopérer avec les autorités nationales de contrôle et avec les organes de contrôle relevant du troisième pilier de l'Union européenne, en vue d'améliorer la cohérence en ce qui concerne la 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 communautaires, en contribuant 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 communautaire, le cas échéant;

— d'améliorer la qualité des politiques de l'UE, chaque fois que la protection effective des données est une condition essentielle du succès de ces politiques.

Avant-propos

J'ai l'honneur de présenter au Parlement européen, au Conseil et à la Commission européenne le second rapport annuel sur mes activités en qualité de Contrôleur européen de la protection des données, conformément au règlement (CE) nº 45/2001 du Parlement européen et du Conseil et en application de l'article 286 du traité CE.

Le présent rapport couvre l'année 2005, qui est la première année complète d'activité depuis l'institution du Contrôleur européen de la protection des données en tant que nouvelle autorité de contrôle indépendante, dont la mission est de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, à l'égard du traitement des données à caractère personnel soient respectés par les institutions et organes communautaires.

La décision du Parlement européen et du Conseil me nommant Contrôleur européen de la protection des données et désignant M. Joaquín Bayo Delgado en qualité de Contrôleur adjoint a pris effet le 17 janvier 2004. La majeure partie de l'année 2004 a donc été consacrée à effectuer les premiers pas cruciaux pour mettre en place une nouvelle institution et à élaborer les rôles stratégiques qu'elle est appelée à jouer au niveau communautaire, afin de surveiller et d'assurer la mise en œuvre des garanties juridiques pour la protection des données à caractère personnel relatives aux citoyens de l'Union européenne.

Nous sommes très heureux de constater que l'un des principaux messages du premier rapport annuel — à savoir que la protection des données à caractère personnel, en tant que valeur fondamentale qui sous-tend les politiques de l'UE, devrait être considérée comme une condition du succès de ces politiques — a été bien reçu et surtout qu'il a été suivi par les différentes parties prenantes. Toute l'urgence qu'il y avait à agir dans ce domaine s'est également imposée comme une évidence, car l'UE ne saurait se permettre de ne pas être à la hauteur quant à l'application de règles qu'elle a fixées pour elle-même et pour ses États membres.

C'est sans aucun doute pour cela que nous avons été en mesure de réaliser en 2005 de réels progrès pour continuer à développer nos rôles stratégiques et à consolider la position du CEPD en tant que nouvel acteur officiel de premier plan dans un domaine de cette importance. Le présent rapport annuel expose plus en détail ces différents rôles et met en lumière leur impact croissant.

Je profite donc de l'occasion qui m'est offerte, à nouveau, pour remercier ceux qui, au sein du Parlement européen, du Conseil et de la Commission, ont activement contribué au succès de nos premiers pas et qui continuent à soutenir notre travail, ainsi que les membres des divers organes et institutions avec qui nous collaborons étroitement et qui sont le plus souvent directement responsables de la façon dont la protection des données est mise en pratique.

Je tiens à remercier tout particulièrement les membres de notre personnel, qui participent à l'accomplissement de notre mission et qui continuent à faire toute la différence dans les résultats obtenus. Le niveau de qualité et d'engagement dont le personnel a fait preuve a été exceptionnel et a contribué au premier chef à accroître notre efficacité. L'augmentation limitée de la taille de notre équipe a aussi été essentielle et bienvenue, et il en sera de même à l'avenir.

Peter Hustinx
Contrôleur européen de la protection des données

1. Bilan et perspectives

1.1. Vue générale sur 2005

Le cadre juridique dans lequel opère le Contrôleur européen de la protection des données (voir point 1.2) définit un certain nombre de tâches et de compétences, qui permettent de distinguer trois fonctions principales. Ces fonctions stratégiques ont été prises comme points de départ pour mettre en place la nouvelle autorité et demeureront des références pour les prochaines années:

— une fonction de **contrôle,** qui consiste à exercer une surveillance à l'égard des institutions et organes communautaires afin que ceux-ci respectent les garanties juridiques existantes chaque fois qu'ils traitent des données à caractère personnel;

— une fonction de **conseil,** qui consiste à conseiller les institutions et organes communautaires sur toutes les questions pertinentes, et particulièrement sur les propositions législatives ayant une incidence sur la protection des données à caractère personnel;

— une fonction de **coopération,** qui consiste à travailler avec les autorités nationales de contrôle et les organes de contrôle relevant du troisième pilier de l'UE (coopération policière et judiciaire en matière pénale), en vue d'améliorer la cohérence dans la protection des données à caractère personnel.

Ces fonctions sont exposées en détail dans les chapitres 2, 3 et 4 de ce rapport annuel, avec une présentation des principales activités du CEPD et des avancées réalisées en 2005. L'importance cruciale de l'information et de la communication en ce qui concerne ces activités nous a amenés à mettre séparément l'accent sur la **communication** dans le chapitre 5. La plupart de ces activités reposent sur une gestion efficace des **ressources** financières, humaines et autres, qui font l'objet du chapitre 6. Les principales fonctions du CEPD sont présentées dans la rubrique liminaire sur le mandat.

Il importe, à ce stade, de souligner à nouveau qu'**un nombre croissant de politiques de l'Union européenne requiert une utilisation licite des données personnelles.** En effet, de nos jours, de nombreuses activités, publiques ou privées, exercées dans notre société moderne sont à l'origine de données à caractère personnel ou s'en servent. Cela s'applique évidemment aussi aux institutions et organes européens dans l'exécution de leurs tâches administratives ou dans l'élaboration des politiques, ainsi que dans la mise en œuvre de leurs programmes politiques. Cela signifie que la **protection effective des données à caractère personnel,** en tant que valeur fondamentale qui sous-tend les politiques de l'UE, devrait être considérée comme une **condition du succès de ces politiques.** C'est cet esprit général qui continuera d'animer le CEPD, lequel attendra une réponse positive en retour.

1.1.1. Contrôle

En premier lieu, l'accent a été mis sur le développement du réseau des **délégués à la protection des données** (DPD) des institutions et organes communautaires. En novembre 2005 a été publié un document de référence sur le rôle joué par les délégués à la protection des données pour garantir le respect effectif du règlement (CE) n° 45/2001. Ce document de référence, qui a été envoyé aux responsables des ad-

ministrations de l'Union, souligne le rôle des DPD en tant que partenaires stratégiques des institutions et organes pour assurer le respect du règlement. Un des messages essentiels de ce document est qu'il est d'abord absolument indispensable que tous les organes désignent un délégué à la protection des données pour pouvoir s'acquitter de leurs obligations au titre du règlement. Un deuxième message fondamental est qu'il y a lieu d'améliorer la notification aux DPD des traitements de données à caractère personnel effectués au sein de leur institution ou organe et que les DPD doivent notifier au CEPD les traitements présentant des risques particuliers pour les personnes concernées et devant donc faire l'objet de contrôles préalables. La relation avec les DPD est examinée plus en détail au point 2.2 du présent rapport.

Deuxièmement, un accent majeur a été mis sur le **contrôle préalable** des traitements qui sont susceptibles de présenter des risques particuliers pour les personnes concernées, au sens de l'article 27 du règlement. Le principe de base est de contrôler les traitements nouveaux, mais, jusqu'à présent, la plupart des contrôles préalables ont été effectués a posteriori, car nombre des systèmes existants auraient fait l'objet d'un contrôle préalable si le CEPD avait été en fonction au moment de leur mise en place. En 2005, 34 avis ont été émis dans le cadre de contrôles préalables, dont 30 portaient sur des systèmes existants de divers organes et institutions. Pour le reste, il s'agissait de consultations quant à la nécessité de procéder à un contrôle préalable ou de cas qui, sans justifier la réalisation d'un contrôle préalable, appelaient néanmoins des observations. Le CEPD a défini un certain nombre de thèmes prioritaires de référence en ce qui concerne les contrôles préalables, à savoir les dossiers médicaux, l'évaluation professionnelle, les procédures disciplinaires, les dossiers des services sociaux et le suivi électronique. À la fin de 2005, 29 notifications étaient en cours d'examen et de nombreuses autres sont attendues dans un avenir proche. Il a été demandé aux institutions et organes de présenter leurs notifications en vue d'un contrôle préalable pour le printemps 2007 au plus tard. Une analyse plus détaillée des critères applicables, des aspects de procédure, des institutions et des questions qui se posent ainsi que du suivi des avis et des consultations sur les contrôles préalables figure au point 2.3 du présent rapport.

En troisième lieu, l'accent a été mis sur le traitement des **plaintes.** Toutefois, en 2005, seules 5 plaintes sur les 27 reçues par le CEPD ont été déclarées recevables et donc examinées. En fait, une grande majorité des plaintes reçues ne relèvent pas du domaine de compétence du CEPD. Dans ce cas, l'auteur de la plainte reçoit une réponse générale et, si possible, des conseils sur une voie de recours plus adaptée. En ce qui concerne le traitement des plaintes relevant de sa compétence, le CEPD a eu des contacts avec le Médiateur européen afin d'examiner les possibilités de collaboration dans un avenir proche. On trouvera plus d'informations sur ce sujet au point 2.4 du présent rapport.

Des moyens importants ont aussi été consacrés à l'élaboration d'un document de référence sur **l'accès du public aux documents et la protection des données,** qui a été présenté en juillet 2005 (voir point 2.6), à la préparation d'un document de référence sur l'utilisation des **communications électroniques** (voir point 2.7) et à la préparation de diverses activités liées au contrôle du système **Eurodac** (voir point 2.8).

1.1.2. Conseil

Une première priorité dans ce domaine a été de définir la **politique que le CEPD devrait suivre dans son rôle de conseiller** des institutions communautaires à l'égard des propositions législatives et documents connexes. Un document stratégique, publié en mars 2005, souligne que la fonction consultative du CEPD a une portée étendue et concerne toutes les propositions législatives ayant une incidence sur la protection des données à caractère personnel. Cette interprétation a été confirmée par la Cour de justice. Ce document stratégique présente aussi la façon dont le CEPD entend aborder, sur le fond, les propositions législatives, ainsi que son rôle procédural au cours des différentes phases du processus législatif. La Commission européenne utilise souvent la possibilité qui lui est donnée de faire appel au CEPD pour obtenir des observations informelles sur un projet de proposition législative avant que celui-ci ne soit soumis à la consultation formelle. Les avis formels sont toujours publiés et sont souvent présentés à la commission concernée du Parlement européen et/ou au groupe compétent du Conseil et ils sont suivis de façon systématique tout au long du processus législatif. La politique à suivre est expliquée plus en détail au point 3.2 du présent rapport.

En 2005, le CEPD a rendu six avis formels, sur des sujets qui cadrent parfaitement avec les préoccupations politiques de la Commission, du Parlement

et du Conseil. Des avis importants ont porté sur l'échange de données à caractère personnel dans le cadre du troisième pilier, le développement de systèmes d'information à grande échelle tels que le système d'information sur les visas (VIS), la seconde génération du système d'information Schengen (SIS II) et la question extrêmement controversée de la conservation obligatoire des données relatives aux communications électroniques pour que les services répressifs puissent y avoir accès. Une analyse de ces avis et de quelques thèmes horizontaux est présentée au point 3.3 du présent rapport.

Le CEPD a aussi, pour la première fois, fait usage de la possibilité d'**intervenir devant la Cour de justice** dans des affaires qui soulèvent des questions importantes quant à la protection des données. La Cour a accédé à la demande du CEPD de pouvoir intervenir dans deux affaires dont elle a été saisie et qui concernent le transfert à l'administration américaine des données des dossiers passagers (PNR), à l'appui des conclusions du Parlement. Le CEPD a présenté à la fois des observations écrites et orales, et attend maintenant la décision de la Cour dans ces deux affaires (voir point 3.4.2).

Au cours de l'année 2005, le CEPD a aussi exercé son rôle consultatif en ce qui concerne les **mesures administratives,** et plus particulièrement les règles d'application adoptées par les institutions et organes dans le domaine de la protection des données. Ce faisant, il est largement en mesure d'influer de manière plus structurelle sur la façon dont les dispositions en matière de protection des données sont mises en œuvre. Dans ce contexte, le CEPD a mis au point une approche pour les règles d'application spécifiques concernant le rôle des DPD (voir points 2.2 et 3.4.3).

Une tâche spéciale du CEPD consiste à **surveiller les faits nouveaux** qui ont une incidence sur la protection des données à caractère personnel. Le rapport présente par conséquent aussi une première évaluation de certaines nouveautés technologiques importantes ainsi que les faits nouveaux dans les domaines politique et législatif, qui feront l'objet d'un suivi systématique en 2006 et au-delà (voir point 3.5).

1.1.3. Coopération

La coopération avec les autorités nationales de contrôle s'inscrit dans le cadre du **Groupe de travail de l'article 29,** institué par l'article 29 de la directive 95/46/CE pour conseiller la Commission et contribuer à la mise en œuvre homogène des dispositions relatives à la protection des données, et dont le CEPD est membre à part entière. Un certain nombre de propositions législatives importantes ont été traitées par le CEPD et par le groupe dans des avis séparés. En l'occurrence, le CEPD a pu se féliciter du concours que les collègues au niveau national lui ont apporté ainsi que de leurs observations complémentaires qui peuvent contribuer à améliorer la protection des données. D'autre part, le CEPD a également consacré des moyens importants à l'élaboration de positions communes qui peuvent contribuer à assurer une plus grande cohérence et une application plus homogène des dispositions relatives à la protection des données au sein de l'Union européenne (voir point 4.1).

La coopération avec les **organes de contrôle institués en vertu du troisième pilier** (tels que les organes de contrôle de Schengen, du système d'information douanier, d'Europol et d'Eurojust) a été axée, dans une large mesure, sur l'élaboration de positions communes en vue de mettre au point un cadre général pour la protection des données dans le troisième pilier de l'UE. Des discussions ont été menées, plus spécifiquement, sur un nouveau système de contrôle relatif au SIS II, qui reposera sur une étroite coopération entre les autorités nationales de contrôle et le CEPD (voir point 4.2). Chacun des organes relevant du troisième pilier a été institué par un instrument différent et est généralement composé de représentants des autorités nationales de contrôle.

Le CEPD a également coopéré activement dans le cadre plus large de la **conférence internationale** et de la **conférence européenne** des commissaires à la protection des données (points 4.3 et 4.4). En septembre 2005, le CEPD a organisé, conjointement avec le Conseil de l'Europe et l'Organisation de coopération et de développement économiques (OCDE), un séminaire sur la protection des données dans les **organisations internationales** (voir point 4.5).

1.1.4. Communication

En 2005, le CEPD a accordé une attention toute particulière à la mise au point d'une **stratégie d'information** susceptible d'appuyer au mieux l'accomplissement des fonctions stratégiques du CEPD. Il est essentiel de mieux faire connaître la question de la protection des données en général et les fonctions et

activités du CEPD en particulier pour remplir avec efficacité les missions de contrôle, de conseil et de coopération. Cette stratégie d'information distingue différents groupes cibles et différents messages pour chacune de ces missions (voir point 5.2).

Le CEPD s'est également employé à développer des **outils d'information et de communication.** Une campagne générale d'information a été menée dans l'ensemble des institutions et organes de l'UE ainsi que dans tous les États membres. Elle a été suivie en 2005 par le lancement d'un service de presse et d'une newsletter régulière et par la création d'un nouveau logo et d'une charte graphique, et elle sera bientôt complétée par le lancement d'un nouveau site internet, qui sera l'outil de communication le plus important du CEPD. Entre-temps, le CEPD a continué de diffuser des informations utiles, en réponse à des demandes spécifiques ou de façon générale dans des avis, documents et discours qui figurent sur le site internet actuel (voir points 5.3 et suivants).

1.1.5. Ressources

Le CEPD a noté avec satisfaction que les autorités budgétaires ont prévu les **ressources budgétaires** nécessaires à la consolidation et à une croissance limitée de l'organisation, compte tenu de la nécessité de réaliser certaines tâches urgentes de contrôle et de conseil en matière de protection des données dans la plupart des institutions et organes. Le CEPD est conscient que bonne gestion financière et rigueur budgétaire sont des conditions essentielles pour maintenir la confiance sur ces sujets (voir point 6.2).

Le renforcement des **ressources humaines** a fait l'objet d'une grande attention. Des résultats significatifs ont été obtenus, tant sur le plan général du recrutement que du point de vue des programmes spéciaux de formation et du détachement d'experts nationaux. Le recours à des profils différents a permis une plus grande flexibilité et a représenté un défi constant pour le personnel (voir point 6.3).

On ne saurait insister assez sur l'importance de l'**accord de coopération administrative** conclu en 2004 avec la Commission, le Parlement et le Conseil, et qui a permis au CEPD de bénéficier d'un soutien extérieur dans les cas qui s'y prêtaient et de consacrer la majeure partie de ses ressources à l'exercice de ses activités fondamentales. La poursuite de cet accord au-delà des trois ans prévus est par conséquent essentielle. La coopération interinstitutionnelle à d'autres niveaux joue un rôle tout aussi important pour une autorité comme le CEPD dont la taille et la diversité interne restent limitées (voir point 6.4).

L'augmentation des effectifs, encore limitée pour l'instant mais appelée à s'accélérer dans un avenir proche, donne la mesure de l'importance qu'il y a à disposer d'une **infrastructure** et de locaux adéquats (voir point 6.5).

L'environnement administratif s'est également développé de façon satisfaisante en 2005. L'adoption d'un **règlement intérieur** marquera une étape clé et aura des conséquences importantes, tant sur le plan interne que sur le plan externe; la plus grande attention est donc accordée à son élaboration (voir point 6.6).

1.2. Cadre juridique

L'article 286 du traité CE, adopté en 1997 dans le cadre du traité d'Amsterdam, dispose que les actes communautaires relatifs à la protection de personnes physiques à l'égard du traitement des données à caractère personnel et à 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 une phase intermédiaire dans l'évolution du cadre juridique dans ce domaine, selon le mouvement entamé au début des années 70 au sein du Conseil de l'Europe.

1.2.1. Contexte

L'article 8 de la convention européenne des droits de l'homme 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, il a été considéré comme nécessaire d'adopter une convention distincte en matière de protection des données, afin de développer une approche po-

sitive et structurelle de la protection des libertés et droits fondamentaux, qui peut être affectée par le traitement des données à caractère personnel dans une société moderne. Cette convention, également appelée «convention 108», a été ratifiée par 35 États 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 qu'il faudrait prévoir pour les institutions et organes communautaires des garanties juridiques similaires, pour leur permettre de participer à la libre circulation des données à caractère personnel moyennant des règles de protection équivalentes. Mais, jusqu'à l'adoption de l'article 286 du traité CE, il n'existait pas de base juridique pour un tel instrument.

Les dispositions utiles visées à l'article 286 du traité CE ont été reprises dans le règlement (CE) nº 45/2001 du Parlement européen et du Conseil 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, qui est entré en vigueur en 2001 ([1]). Ce règlement a également institué, comme le prévoyait le traité, une autorité de contrôle indépendante, nommée le «Contrôleur européen de la protection des données», auquel un certain nombre de tâches et de compétences ont été assignées.

Le traité établissant une Constitution pour l'Europe, signé en octobre 2004, accorde une attention particulière à la protection des droits fondamentaux. Le respect de la vie privée et familiale et la protection des données à caractère personnel sont traités comme des droits fondamentaux distincts dans les articles II-67 et II-68 de la Constitution. La protection des données est aussi mentionnée à l'article I-51 de la Constitution, dans la partie I, titre VI, intitulé «La vie démocratique de l'Union». Il est ainsi manifeste que la protection des données est désormais considérée comme un élément fondamental d'une bonne gestion des affaires publiques. Le contrôle indépendant est un élément essentiel de cette protection.

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

1.2.2. Règlement (CE) nº 45/2001

En regardant de plus près le règlement, il convient de noter, dans un premier temps, qu'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». Cela signifie que seules les activités qui sont totalement en dehors du premier pilier ne relèvent pas des tâches et des compétences de contrôle du CEPD.

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) nº 45/2001 constitue la mise en œuvre de cette directive au niveau européen. Le règlement traite des principes généraux tels que le traitement loyal et licite, la proportionnalité et la compatibilité d'utilisation, les catégories particulières des 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 communautaires de désigner au moins une personne comme 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 de traitement. Des délégués sont désormais en place dans toutes les institutions communautaires et dans un certain nombre d'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).

1.2.3. 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 A), 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 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 communautaires. 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 plaintes, effectuer des enquêtes, informer les responsables du traitement et les personnes concernées, effectuer des contrôles préalables lorsque les traitements présentent des risques particuliers, etc. Le règlement habilite le CEPD à obtenir accès à toutes les informations utiles et aux locaux concernés lorsque cela est nécessaire à 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 de nouvelles dispositions législatives — énoncée 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 législative relative à la protection des données à caractère personnel — concerne aussi les projets de directive et 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 le troisième pilier. Surveiller les faits nouveaux qui présentent un intérêt et qui pourraient avoir une incidence sur la protection des données à caractère personnel constitue une autre tâche très importante. 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 la coopération avec les organes de contrôle relevant du troisième pilier sont de même nature. En tant que membre du Groupe de l'article 29 qui a été institué pour conseiller la Commission et pour développer des politiques harmonisées, le CEPD apporte une contribution précieuse. La coopération avec les organes de contrôle relevant du 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 dans le chapitre 4 du présent rapport.

1.3. Résultats obtenus en 2005

Le rapport annuel 2004 exposait les principaux objectifs figurant ci-après, qui avaient été retenus pour 2005. La plupart de ces objectifs ont été atteints.

- **Extension du réseau des délégués à la protection des données**

Le CEPD a contribué à élargir le réseau des DPD. Un document de référence sur le rôle joué par les DPD pour garantir le respect effectif du règlement (CE) n° 45/2001 a été publié en novembre 2005, et les institutions et organes ont été vivement encouragés à en tirer largement parti.

- **Brochures, site internet et newsletter**

Le CEPD a assuré une large diffusion de brochures publiées dans toutes les langues officielles et destinées à mieux faire connaître les droits des personnes concernées ainsi que son propre rôle en vertu du règlement. Une newsletter a été lancée pour fournir des informations sur les faits nouveaux. Un site internet entièrement nouveau sera mis en place prochainement.

- **Notifications et contrôles préalables**

Toutes les institutions et tous les organes ont été invités à notifier les traitements en cours, au plus tard pour le printemps 2007. Le CEPD a consacré beaucoup de temps et d'efforts pour réaliser le contrôle préalable des traitements susceptibles de présenter des risques particuliers. La plupart des avis relatifs à des contrôles préalables ont été publiés sur le site internet.

- **Lignes directrices pour le traitement des plaintes et pour les enquêtes**

L'élaboration de procédures normalisées pour le traitement des plaintes, des enquêtes et autres types de cas a pris plus de temps que prévu. Les grands principes seront intégrés au règlement intérieur que le CEPD prévoit d'adopter et qui sera publié sur le site internet au printemps 2006. Des lignes directrices plus détaillées suivront en temps utile.

- **Vérifications et enquêtes**

Le CEPD a effectué les préparatifs nécessaires en vue d'un audit sur la sécurité qui sera réalisé prochainement sur l'unité centrale du système Eurodac, afin de vérifier le respect des règles applicables et de mettre au point une méthode qui pourra être appliquée plus largement. Le CEPD a aussi lancé des enquêtes sur le terrain, là où cela s'est avéré nécessaire pour des cas précis.

- **Vie privée et transparence**

Le CEPD a publié en juillet 2005 un document de référence sur l'accès du public aux documents et la protection des données, qui contient des orientations visant à encourager les bonnes pratiques dans ces deux domaines et à aider les institutions et organes à se prononcer en cas de conflit entre ces deux droits fondamentaux.

- **Contrôle des communications électroniques et des données relatives au trafic**

Le CEPD a élaboré un projet de document définissant des lignes directrices concernant le traitement des données relatives au trafic et des données relatives à la facturation des différents types de communications (téléphone, courrier électronique, téléphone mobile, internet, etc.) dans les institutions et organes, en vue de clarifier et de renforcer les garanties actuellement applicables à ce type de traitements. La version finale de ce document sera publiée en 2006.

- **Avis sur des propositions législatives**

Le CEPD a publié un document stratégique sur son rôle en tant que conseiller des institutions communautaires à l'égard des propositions législatives et documents connexes. Ce document a permis d'harmoniser les pratiques concernant les consultations formelles et informelles de la Commission et d'assurer un suivi systématique au Parlement et au Conseil. Six avis formels sur différents sujets ont été adoptés en 2005.

- **Protection des données dans le cadre du troisième pilier**

Le CEPD a accordé une attention particulière à la mise en place d'un cadre général pour la protection des données à caractère personnel dans le cadre du troisième pilier. Un avis important a été publié en décembre 2005 sur la proposition de la Commission concernant un projet de décision-cadre sur ce thème. Un certain nombre de questions connexes ont été traitées dans d'autres avis.

- **Développement des ressources**

Une grande attention a été accordée en 2005 à une gestion efficace des ressources financières, humaines et autres. La consolidation de l'organisation, assortie d'une croissance limitée, a permis au CEPD de développer progressivement ses missions, afin de faire face aux besoins urgents en matière de contrôle et de conseil dans la plupart des institutions et organes.

1.4. Objectifs pour 2006

Les principaux objectifs énumérés ci-après ont été retenus pour 2006. Les résultats qui auront été obtenus seront analysés dans le prochain rapport annuel.

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

Le CEPD apportera un soutien important au réseau des délégués à la protection des données, en mettant l'accent en particulier sur la prise de fonction et la formation des délégués récemment nommés. Un calendrier sera établi pour effectuer des évaluations bilatérales des progrès accomplis en ce qui concerne les notifications, afin que la notification des traitements existants soit terminée au plus tard pour le printemps 2007.

- **Poursuite des contrôles préalables**

Le CEPD a l'intention de terminer les contrôles préalables portant sur des traitements existants dans les domaines de la santé, de l'évaluation professionnelle, des dossiers disciplinaires, du contrôle des communications électroniques et des dossiers des services sociaux. Un document stratégique comprenant une mise à jour sur les pratiques pertinentes et les conclusions relatives aux contrôles préalables sera publié à l'automne 2006.

- **Contrôle des communications électroniques et des données relatives au trafic**

Le CEPD publiera une version finale du document définissant des lignes directrices en ce qui concerne le traitement des données à caractère personnel dans le cadre des réseaux de communications électroniques, et mettra en place des procédures pour l'évaluation au cas par cas et l'approbation éventuelle des listes des données à conserver qui seront soumises par les institutions et organes communautaires.

- **Lignes directrices pour le traitement des dossiers personnels**

Le CEPD va élaborer et publier des lignes directrices sur le contenu et la durée de conservation des dossiers personnels relatifs aux membres du personnel des institutions et organes. Ces lignes directrices seront basées sur les conclusions des contrôles préalables et tiendront dûment compte des dispositions du statut et des exigences relatives à la protection des données.

- **Transferts vers les pays tiers**

Le CEPD fera l'inventaire des transferts de données à caractère personnel par les institutions et organes communautaires vers les pays tiers, les organisations internationales et les organes européens qui ne relèvent pas du champ d'application du règlement (CE) n° 45/2001 et de la directive 95/46/CE. Il publiera les lignes directrices nécessaires, après avoir entendu les commentaires des institutions et organes communautaires concernés.

- **Contrôle du système Eurodac**

Le CEPD va effectuer un audit approfondi de la sécurité des bases de données de l'unité centrale du système Eurodac et continuer à développer une étroite coopération avec les autorités nationales en charge de la protection des données sur un système de contrôle conjoint, en vue d'acquérir et de partager une expérience utilisable pour d'autres bases de données européennes à grande échelle.

- **Rôle consultatif sur les propositions législatives**

Le CEPD va consolider et poursuivre le développement de son rôle de conseiller sur les propositions législatives, en continuant à rendre des avis sur divers sujets, avec efficacité et en temps utile, et en s'attachant à faire en sorte que son rôle soit formellement reconnu dans les instruments juridiques en question.

- **Interventions dans des affaires dont la Cour de justice est saisie**

Le CEPD envisagera des interventions devant le Tribunal de la fonction publique, le Tribunal de première instance et la Cour de justice dans des cas qui soulèvent des questions liées à l'interprétation des principes de la protection des données, afin de contribuer à un développement cohérent de la législation en la matière au niveau européen.

- **Deuxième version du site internet**

Un site internet complètement remodelé sera lancé vers la mi-2006, avec un accès en ligne au registre des notifications de contrôle préalable, aux avis et au suivi. Le site internet sera structuré selon les principaux rôles du CEPD et offrira aux utilisateurs un meilleur accès aux informations pertinentes concernant les différentes activités.

- **Développement des ressources**

Le CEPD continuera à développer les ressources et l'infrastructure nécessaires pour assurer l'accomplissement efficace de ses fonctions. Il cherchera à obtenir la prolongation de l'accord de coopération administrative actuellement en vigueur avec la Commission, le Parlement et le Conseil, et à pouvoir disposer d'un plus grand nombre de bureaux afin d'être en mesure de répondre aux besoins actuels et à l'augmentation des effectifs qui est prévue.

2. Contrôle

2.1. Généralités

La mission du Contrôleur européen de la protection des données consiste à surveiller, de manière indépendante, les traitements effectués par des institutions ou organes communautaires, relevant en tout ou en partie du champ d'application du droit communautaire (à l'exclusion de la Cour de justice des Communautés européennes dans l'exercice de ses fonctions juridictionnelles). Le règlement (CE) n° 45/2001 définit et confère un certain nombre de fonctions et de compétences qui permettent au CEPD de s'acquitter de sa tâche de contrôle.

Comme en 2004, les activités de contrôle ont essentiellement porté, durant l'année 2005, sur le contrôle préalable. Cette tâche implique l'examen des activités exercées par les institutions et organes dans les domaines qui sont le plus susceptibles de présenter des risques spécifiques pour les personnes concernées, au sens de l'article 27 du règlement (CE) nº 45/2001. Les avis du CEPD permettent aux responsables du traitement d'adapter leurs traitements en fonction des orientations données par le CEPD, en particulier lorsque le non-respect des règles relatives à la protection des données risque de nuire gravement aux droits des personnes. Le contrôle préalable est le principal outil de contrôle dans la mesure où il permet une approche systématique. Le CEPD dispose d'autres instruments tels que le traitement des plaintes.

Pour ce qui est des compétences qui lui sont conférées, le CEPD n'a ordonné aucune mesure et n'a émis aucun avertissement ni interdiction à ce jour. Jusqu'à présent, il a suffi au CEPD de formuler ses avis (dans le cas tant des contrôles préalables que des plaintes) sous la forme de recommandations. Les responsables du traitement ont mis en application ces recommandations ou ont exprimé l'intention de le faire et prennent les mesures nécessaires. La rapidité des réactions varie selon les cas. Les services du CEPD ont donné des orientations en vue du suivi des recommandations.

2.2. Délégués à la protection des données

Le règlement prévoit que les institutions et organes communautaires doivent désigner, chacun, au moins une personne comme délégué à la protection des données (article 24, paragraphe 1). Certaines institutions ont associé au délégué à la protection des données un assistant ou un délégué adjoint à la protection des données. La Commission a également désigné un «coordinateur de la protection des données» dans chaque direction générale (DG) pour coordonner tous les aspects de la protection des données au sein de la DG.

Depuis plusieurs années, les délégués à la protection des données se rencontrent à intervalles réguliers afin d'échanger leurs expériences et d'examiner des questions horizontales. Ce réseau informel a fait la preuve de son efficacité en termes de collaboration et a abouti à l'adoption d'un certain nombre de documents de référence internes.

Le CEPD a participé à chacune des réunions organisées entre les délégués à la protection des données en mars (bureau du CEPD, Bruxelles), juillet (Cour des comptes, Luxembourg) et octobre (Médiateur européen, Strasbourg). Ces rencontres ont constitué pour le CEPD une bonne occasion de tenir les délégués

à la protection des données informés de son travail et d'examiner des questions d'intérêt commun. Le CEPD a profité de ces réunions pour expliquer et analyser la procédure de contrôle préalable et certaines des principales notions du règlement à prendre en compte dans le cadre de la procédure de contrôle préalable (par exemple le responsable du traitement, les traitements). Ces réunions ont aussi donné au CEPD l'opportunité de souligner les progrès réalisés en matière de traitement des dossiers devant faire l'objet d'un contrôle préalable et de fournir des informations détaillées sur certaines conclusions tirées de cette activité de contrôle préalable (voir point 2.3). Cette collaboration entre le CEPD et les délégués à la protection des données s'est donc poursuivie de manière très positive.

Le CEPD a présenté son document de référence intitulé «Accès du public aux documents et protection des données», question à laquelle les délégués à la protection des données sont souvent confrontés dans le cadre de leur travail.

Enfin, lors des réunions, les discussions ont porté en grande partie sur le document élaboré par les délégués à la protection des données et intitulé «Profile of DPO and good practice manual» (Profil du délégué à la protection des données et manuel de bonnes pratiques) et sur celui du CEPD intitulé «Document de référence sur le rôle joué par les délégués à la protection des données pour garantir le respect effectif du règlement (CE) n° 45/2001». Ces documents ont été élaborés en réponse aux inquiétudes des délégués à la protection des données sur la garantie d'indépendance attachée à leur fonction. Les délégués ont rédigé un document qui vise à:

— définir le profil «idéal» du délégué à la protection des données au sein des institutions ou organes communautaires;

— établir des règles minimales concernant leur position au sein des institutions ou organes communautaires;

— préciser les bonnes pratiques à appliquer dans l'exercice de leurs fonctions et établir des critères potentiels d'évaluation de leur travail.

Le CEPD s'est largement inspiré de ce document dans son document de référence.

Dans ce document, transmis aux responsables de l'administration de l'UE, le CEPD souligne le rôle clé joué par le délégué à la protection des données en tant que partenaire stratégique pour garantir le respect du règlement. Le CEPD:

— explique comment le respect des principes relatifs à la protection des données au sein des institutions et organes doit être garanti à différents niveaux pour lesquels le délégué à la protection des données, l'institution ou l'organe et le CEPD ont tous un rôle à jouer;

— donne des orientations sur la façon dont les délégués à la protection des données peuvent s'acquitter au mieux de leur mission, en toute indépendance;

— examine les principales fonctions des délégués à la protection des données, qui comprennent le contrôle du respect du règlement, la réception des notifications, la tenue d'un registre accessible au public, le conseil et la sensibilisation à la protection des données au sein même de l'institution ou de l'organe, et la notification au CEPD de certains traitements en vue d'un contrôle préalable.

Le message clé transmis par ce document n'était pas uniquement que tous les organes de l'UE doivent désigner un délégué à la protection des données, mais également que cette désignation n'implique pas en soi le respect automatique du règlement. Les délégués à la protection des données doivent être informés de manière plus appropriée des traitements de données à caractère personnel effectués au sein de leur institution ou organe et, le cas échéant, informer le CEPD de tout traitement susceptible de présenter des risques spécifiques pour les personnes concernées et devant donc, par conséquent, être soumis à un contrôle préalable.

2.3. Contrôle préalable

2.3.1. Base juridique

Principe général: article 27, paragraphe 1

L'article 27, paragraphe 1, du règlement (CE) n° 45/2001 dispose 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 leurs finalités» doivent être soumis au contrôle préalable du CEPD.

L'article 27, paragraphe 2, énumère les traitements susceptibles de présenter de tels risques. Cette liste n'est pas exhaustive. En effet, d'autres cas, qui ne figurent pas dans la liste, pourraient présenter des risques particuliers au regard des droits et libertés des personnes concernées et, par conséquent, justifier un contrôle préalable du CEPD. Par exemple, tout traitement de données à caractère personnel qui touche au principe de confidentialité visé à l'article 36 implique des risques spécifiques qui justifient un contrôle préalable du CEPD.

Cas énumérés à l'article 27, paragraphe 2

L'article 27, paragraphe 2, énumère un certain nombre de traitements susceptibles de présenter des risques particuliers au regard des droits et des libertés des personnes concernées, à savoir:

a) *les traitements de données relatives à la santé et les traitements de données relatives à des suspicions, infractions, condamnations pénales ou mesures de sûreté.* Ces catégories revêtent un caractère sensible et exigent une attention accrue étant donné qu'elles relèvent des catégories particulières de données visées à l'article 10 du règlement. Le CEPD a précisé ce critère en indiquant que, si les données relatives à la santé ou à des suspicions, etc., sont le résultat d'un traitement effectué avant leur enregistrement dans un fichier, c'est l'opération antérieure et non le fichier lui-même qui fait l'objet du contrôle préalable. Tel est le cas pour les dossiers personnels dans les institutions et les organes. Une autre distinction doit être faite: les «mesures de sûreté» ne sont pas des mesures relatives à la sûreté des bâtiments, par exemple, mais des mesures adoptées dans le cadre de procédures judiciaires;

b) *les traitements destinés à évaluer les aspects de la personnalité des personnes concernées, tels que leurs compétences, leur rendement ou leur comportement.* Ce critère est basé sur la finalité du traitement et non sur le simple recueil de données d'évaluation, si aucune évaluation ultérieure de la personne n'est prévue (là aussi, le traitement préalable de l'évaluation est en soi soumis à un contrôle préalable);

c) *les traitements permettant des interconnexions non prévues en vertu de la législation nationale ou communautaire entre des données traitées pour des finalités différentes.* Cette disposition vise à empêcher que des liens ne soient établis entre des données recueillies à des fins différentes. Le risque serait de pouvoir déduire de nouvelles informations à partir du lien établi entre des données n'ayant pas cette information pour finalité, ce qui détournerait ces données de la finalité pour laquelle elles avaient été initialement recueillies. L'utilisation d'un identifiant personnel peut être un indice, mais ne présente pas en soi un risque spécifique. L'utilisation de bases de données électroniques offrant la possibilité d'une interrogation par des outils logiciels peut être un autre élément à prendre en considération;

d) *les traitements visant à exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat.* Ce critère s'applique généralement aux listes noires et peut aussi concerner, dans une certaine mesure, les systèmes d'évaluation.

2.3.2. Procédure

Notification/consultation

Les contrôles préalables doivent être effectués par le CEPD après réception de la notification du délégué à la protection des données.

En cas de doute quant à la nécessité d'un contrôle préalable, le délégué à la protection des données peut aussi consulter le CEPD sur le cas en question (article 27, paragraphe 3). Cette procédure de consultation a constitué un outil fondamental pour l'élaboration des critères d'interprétation de l'article 27, paragraphes 1 et 2, précités. Dans certains cas, le délégué à la protection des données a envoyé une notification en vue d'un contrôle préalable, considérant qu'il y avait «nécessité» au sens juridique du terme, mais le CEPD a conclu que ce n'était pas le cas (voir au point 2.3.3 la partie consacrée aux avis sur les contrôles préalables rendus en 2005). Quoi qu'il en soit, ces cas, de même que les consultations, ont largement contribué à la clarification des critères applicables au contrôle préalable.

Délai, suspension et prolongation

Le CEPD doit rendre son avis dans les deux mois qui suivent la réception de la notification. Lorsque le CEPD demande des informations complémentaires, le délai de deux mois est généralement suspendu jusqu'à ce que les informations en question aient été communiquées.

Lorsque la complexité du dossier l'exige, le délai de deux mois peut également être prolongé pour une nouvelle période de deux mois sur décision du CEPD, qui doit être notifiée au responsable du traitement avant l'expiration du délai initial de deux mois. Si, au terme de deux mois, éventuellement prolongés, aucune décision n'a été rendue, l'avis du CEPD est réputé favorable.

Registre

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 doit pouvoir être accessible au public pour consultation.

Ce registre a pour base le formulaire de notification élaboré en 2004. En 2005, le formulaire de notification relatif au contrôle préalable qui doit être rempli par les délégués à la protection des données et transmis au CEPD, a été amélioré à la fois en termes de contenu, par l'ajout de nouveaux éléments pertinents, et de format, ce qui permet une meilleure articulation avec les formulaires internes de notification envoyés aux délégués, notamment ceux de la Commission et des autres institutions et organes qui suivent le même modèle.

L'expérience a montré qu'il est nécessaire de disposer de plus d'informations que celles prévues à l'article 27, paragraphe 5, en référence à l'article 25, afin d'avoir une bonne base juridique et factuelle permettant d'analyser les traitements. C'est pourquoi de nouveaux champs d'information ont été ajoutés au formulaire. Le besoin de demander des informations complémentaires est ainsi réduit au minimum.

Par souci de transparence, toutes les informations sont consignées dans le registre public, à l'exception des mesures de sécurité, qui ne doivent pas être mentionnées dans le registre accessible au public. Cette restriction est conforme à l'article 26 du règlement, qui prévoit que le registre des traitements tenu par chaque délégué à la protection des données contient les informations communiquées dans le formulaire de notification, à l'exception des mesures de sécurité.

Lorsque le CEPD a rendu son avis, celui-ci est mentionné dans le registre, ainsi que le numéro du dossier traité et les éventuelles mesures de suivi qui doivent être prises (les restrictions susmentionnées étant également applicables). Par la suite, les modifications apportées par le responsable du traitement à la lumière de l'avis du CEPD sont aussi indiquées sous une forme synthétique. Deux objectifs sont ainsi réalisés: d'une part, les informations relatives à un traitement donné sont tenues à jour, d'autre part, le principe de transparence est respecté.

Le registre sera accessible en ligne à l'issue de la deuxième phase de développement du site internet et permettra alors la consultation tant des notifications que des avis rendus. En attendant, la plupart des avis peuvent être consultés sur le site internet, y compris les notes qui sont ajoutées lorsque les recommandations sont mises en œuvre par les responsables du traitement.

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.

Les avis sont structurés de la façon suivante: description de la procédure, résumé des faits, analyse juridique, conclusions.

L'analyse juridique consiste, en premier lieu, à déterminer si le cas remplit bien les conditions requises pour pouvoir faire l'objet d'un contrôle préalable. Comme cela est précisé plus haut, si le cas ne relève pas des cas énumérés à l'article 27, paragraphe 2, le CEPD examinera les risques qui en découlent pour les droits et libertés de la personne concernée. Lorsque le cas remplit les conditions requises pour pouvoir faire l'objet d'un contrôle préalable, l'analyse juridique consiste principalement à déterminer si le traitement est conforme aux dispositions pertinentes du règlement. Si nécessaire, des recommandations sont formulées en vue de garantir le respect du règlement. Dans ses conclusions, le CEPD a jusqu'à présent déclaré que le traitement en question ne paraissait pas entraîner de violation d'une disposition quelconque du règlement, pour autant qu'il soit tenu compte des recommandations émises.

Afin de garantir, comme dans d'autres domaines, que l'ensemble du personnel travaille dans des conditions identiques et que les avis du CEPD sont adoptés à l'issue d'une analyse complète de toutes les informations

pertinentes, un manuel est en cours d'élaboration. Il présente la structure des avis, se fonde sur une somme d'expériences pratiques et fait l'objet d'une mise à jour permanente. Il comporte aussi une liste de contrôle.

Un système de gestion des tâches a été mis en place pour s'assurer que toutes les recommandations relatives à un cas donné sont mises en œuvre et, le cas échéant, que toutes les décisions sont respectées (voir point 2.3.7).

2.3.3. Analyse quantitative

Distinction entre les cas examinés a posteriori et les cas de contrôle préalable proprement dit

Le règlement est entré en vigueur le 1er février 2001. L'article 50 prévoit que les institutions et les organes communautaires doivent prendre les mesures nécessaires pour que les traitements déjà en cours à la date d'entrée en vigueur du règlement soient mis en conformité avec celui-ci dans un délai d'un an à compter de ladite date (soit le 1er février 2002). Or la nomination du CEPD et du Contrôleur adjoint a pris effet le 17 janvier 2004.

Les contrôles préalables concernent non seulement les traitements qui ne sont pas encore en cours (contrôles préalables «proprement dits»), mais aussi ceux qui ont débuté avant le 17 janvier 2004 ou avant l'entrée en vigueur du règlement (cas examinés «a posteriori»). Dans de tels cas, un contrôle au titre de l'article 27 ne pourrait être «préalable» au sens strict du terme, il doit donc être réalisé a posteriori. En adoptant cette approche pragmatique, le CEPD permet de garantir le respect de l'article 50 du règlement pour ce qui est des traitements qui présentent des risques particuliers.

Afin de résorber l'arriéré des cas susceptibles de faire l'objet d'un contrôle préalable, le CEPD a demandé aux délégués à la protection des données d'analyser la situation dans leurs institutions respectives en ce qui concerne les traitements relevant du champ d'application de l'article 27. Après avoir reçu les contributions de tous les délégués à la protection des données, le CEPD a, en 2004, dressé une liste des cas qui étaient susceptibles de faire l'objet d'un contrôle préalable. Cette liste a été précisée en 2005.

À l'issue de l'inventaire, certaines catégories de traitements ont été recensées dans la plupart des institutions et organes; on a donc estimé que ces catégories se prêtaient à un contrôle plus systématique. Afin de permettre une utilisation plus efficace des ressources humaines disponibles, le CEPD a établi un ordre de priorité des travaux relatifs aux cas examinés a posteriori. En septembre 2004, après examen de l'inventaire des cas qui doivent être soumis au CEPD par les institutions et organes, trois grandes priorités ont été fixées:

1) les dossiers médicaux;
2) l'évaluation du personnel;
3) les procédures disciplinaires.

Le CEPD a ajouté deux nouvelles priorités dans le cadre d'une demande de mise à jour de l'inventaire adressée aux institutions et organes en novembre 2005, à savoir:

4) les services sociaux;
5) le contrôle des communications électroniques.

Ces critères de priorité s'appliquent seulement aux cas examinés a posteriori, car les cas de contrôle préalable proprement dit doivent être traités avant que le traitement ne soit mis en œuvre, suivant le calendrier de l'institution ou de l'organe concerné.

Avis rendus en 2005 sur des cas de contrôle préalable

En 2005, c'est-à-dire pendant la première année complète d'activité du CEPD, 34 avis ont été rendus sur des cas de contrôle préalable.

Cour des comptes	5 cas de contrôle préalable
Commission européenne	4 cas de contrôle préalable
Comité des régions	3 cas de contrôle préalable
Conseil	4 cas de contrôle préalable
Banque centrale européenne	3 cas de contrôle préalable
Cour de justice des Communautés européennes	6 cas de contrôle préalable
Comité économique et social européen	1 cas de contrôle préalable
Banque européenne d'investissement	4 cas de contrôle préalable
Parlement européen	2 cas de contrôle préalable
OHMI [2]	2 cas de contrôle préalable

Sur les 34 cas de contrôle préalable, quatre seulement étaient des cas de contrôle préalable proprement dit, c'est-à-dire que les institutions et organes concernés (la Cour des comptes pour trois d'entre eux et la Banque centrale européenne pour le quatrième) ont suivi la procédure relative au contrôle préalable avant la mise en

[2] Office de l'harmonisation dans le marché intérieur (marques, dessins et modèles).

œuvre du traitement. Trois de ces quatre cas portaient sur des procédures disciplinaires et le quatrième était lié à une évaluation du personnel. Les 30 autres cas ont fait l'objet d'un contrôle préalable a posteriori.

Outre ces 34 cas de contrôle préalable sur lesquels un avis a été rendu, le CEPD a traité huit cas qui ont été considérés comme ne devant pas faire l'objet d'un contrôle préalable: deux notifications en provenance de la Cour de justice, deux de la Banque européenne d'investissement, deux du Médiateur européen, une du Comité des régions et une de la Commission. Sur ces huit cas, cinq concernaient les dossiers personnels des agents. Bien que les dossiers personnels ne soient pas soumis au contrôle préalable, ils existent dans toutes les institutions et tous les organes et soulèvent d'importantes questions relatives à la protection des données. Ce sujet spécifique sera donc traité dans un document destiné à donner des lignes directrices visant à ce que les droits des personnes puissent être dûment respectés.

Analyse par institution et organe

La plupart des institutions et organes ont notifié les traitements susceptibles de présenter des risques spécifiques. Lors de la mise à jour de leur inventaire des cas de contrôle préalable (en novembre 2005), les institutions et organes ont eu l'occasion de déterminer les domaines dans lesquels le nombre de notifications a sensiblement augmenté et ceux dans lesquels les notifications font défaut.

Seule une agence (l'OHMI) a notifié quelques cas. Le CEPD suppose que de nombreuses autres agences notifieront très prochainement des traitements, dans la mesure où certaines d'entre elles sont actuellement bien avancées dans la réalisation de leur propre inventaire.

Analyse par catégorie

Les cas de contrôle préalable traités se répartissent comme suit, par catégorie prioritaire:

Première catégorie (dossiers médicaux)	9 cas de contrôle préalable
Deuxième catégorie (évaluation du personnel)	19 cas de contrôle préalable
Troisième catégorie (procédures disciplinaires)	6 cas de contrôle préalable
Quatrième catégorie (services sociaux)	néant
Cinquième catégorie (contrôle des communications électroniques)	néant

La première catégorie comprend le dossier médical proprement dit (un cas de contrôle préalable) et toutes les procédures liées aux indemnités ou aux régimes d'assurance maladie (huit cas de contrôle préalable).

La catégorie la plus représentée reste la deuxième, relative à l'évaluation du personnel (56 % des cas; 19 dossiers sur 34). L'évaluation concerne tous les membres du personnel des institutions et organes communautaires, y compris les fonctionnaires, les agents temporaires et les agents contractuels.

La finalité de l'évaluation est pertinente au sens large en ce qu'elle porte non seulement sur l'évaluation proprement dite [voir par exemple le dossier 2005-218 concernant le rapport d'évolution de carrière (REC)], mais aussi sur tous les traitements de données qui ont contribué à l'évaluation de la personne concernée dans un cadre spécifique (telle que l'évaluation des prestataires extérieurs free-lance).

En ce qui concerne la troisième catégorie (les procédures disciplinaires), seuls six dossiers ont été traités. Ces traitements ont cependant été très bien documentés. Il est important de souligner que 75 % des cas de contrôle préalable proprement dit portent sur des procédures disciplinaires.

Étant donné que les quatrième et cinquième domaines prioritaires n'ont été introduits qu'en novembre 2005, il est logique qu'aucun avis n'ait été rendu à ce jour dans ces deux catégories, même si des notifications ont été reçues dans chacune d'elles.

Travail du CEPD et des institutions et organes

Les deux graphiques de l'annexe D illustrent le travail du CEPD et celui des institutions et organes. Ils fournissent des informations détaillées sur le nombre de jours de travail du CEPD, le nombre de jours de prolongation requis par le CEPD et le nombre de jours de suspension (temps nécessaire à la réception des informations de la part des institutions et organes).

Notifications en vue d'un contrôle préalable reçues en 2005, sur lesquelles des avis doivent être rendus en 2006

Il est probable que 2006 sera une année durant laquelle de nombreux cas de contrôle préalable seront analysés. À la fin de janvier, **33 cas de contrôle préalable** étaient déjà en cours de traitement: 29 notifications ont été transmises en 2005 (8 en décembre) et

4 en janvier 2006. Aucun de ces cas ne constitue un cas de contrôle préalable proprement dit. Un seul cas est considéré comme ne devant pas faire l'objet d'un contrôle préalable.

Commission européenne	3 cas de contrôle préalable
Conseil de l'Union européenne	8 cas de contrôle préalable
Banque centrale européenne	4 cas de contrôle préalable
Cour de justice des Communautés européennes	2 cas de contrôle préalable
Banque européenne d'investissement	3 cas de contrôle préalable
Office européen de sélection du personnel ([3])	3 cas de contrôle préalable
EUMC ([4])	1 cas de contrôle préalable
OHMI ([5])	1 cas de contrôle préalable
CdT ([6])	4 cas de contrôle préalable

Analyse par institution et organe

Les institutions et organes continuent de notifier au CEPD les traitements susceptibles de présenter des risques spécifiques. Après le lancement de la mise à jour de l'inventaire (en novembre 2005), on peut observer que certaines institutions ont envoyé de nombreuses notifications, alors que d'autres en ont envoyé relativement peu ou n'en ont pas envoyé du tout.

Outre l'OHMI, deux autres agences (l'EUMC et le CdT) sont désormais actives dans le domaine de la protection des données. Davantage d'agences devraient, dans un avenir proche, prendre en charge la question de la protection des données.

Analyse par catégorie

Les cas de contrôle préalable notifiés se répartissent comme suit, par catégorie prioritaire:

Première catégorie (dossiers médicaux)	9 cas de contrôle préalable
Deuxième catégorie (évaluation du personnel)	13 cas de contrôle préalable
Troisième catégorie (procédures disciplinaires)	1 cas de contrôle préalable
Quatrième catégorie (services sociaux)	2 cas de contrôle préalable
Cinquième catégorie (contrôle des communications électroniques)	3 cas de contrôle préalable
Autres domaines	1 cas de contrôle préalable ([7])

Dans la première catégorie (dossiers médicaux), le processus de notification s'est fait de manière continue et cela devrait encore être le cas en 2006, puisque de nombreuses procédures portent sur des dossiers médicaux.

La deuxième catégorie prioritaire (évaluation du personnel) regroupe toujours la majorité des cas — 13 dossiers sur 29 (45 %). C'est dans ce domaine qu'ont été notifiés des cas de première importance portant par exemple sur le recrutement des fonctionnaires, des agents temporaires et des agents contractuels (dossier «Office européen de sélection du personnel»), qui concernent l'ensemble des institutions et des organes.

En ce qui concerne la troisième catégorie (procédures disciplinaires), le CEPD attend des notifications de la part des institutions.

Dans la quatrième catégorie (services sociaux), des notifications ont déjà été reçues (une du Conseil et une de la Commission).

La cinquième catégorie (contrôle des communications électroniques) revêt une importance particulière. Le CEPD élabore actuellement un document relatif au contrôle préalable des systèmes de contrôle des communications électroniques qui servira de base pour le contrôle préalable dans ce domaine (voir point 2.7).

2.3.4. Principales questions soulevées par les cas examinés a posteriori

Les données médicales et autres données relatives à la santé sont traitées par les institutions et organes. Toute donnée liée à la connaissance directe ou indirecte de l'état de santé d'une personne relève de cette catégorie. Ainsi, la «double allocation» pour enfant handicapé, l'enregistrement des absences, etc., sont soumis au contrôle préalable.

Dans ce domaine, tant la nécessité du contrôle préalable que les conditions spécifiques relatives au traitement de données sensibles s'appliquent (article 10 du règlement). La base juridique et la stricte nécessité du traitement de ces données ont été examinées avec

([3]) L'Office européen de sélection du personnel dépend du délégué à la protection des données de la Commission.
([4]) Observatoire européen des phénomènes racistes et xénophobes.
([5]) Office de l'harmonisation dans le marché intérieur (marques, dessins et modèles).
([6]) Centre de traduction des organes de l'Union européenne.
([7]) Lié aux irrégularités financières.

attention. La confidentialité est aussi une question cruciale.

Dans certains cas, l'externalisation des services médicaux fait que le traitement se situe hors du champ d'application du règlement (mais la législation nationale transposant la directive 95/46/CE est alors applicable).

L'*évaluation du personnel* est, pour des raisons évidentes, un traitement commun à tous les organes et institutions. Des cas très divers ont été analysés, allant de la sélection de nouveaux membres du personnel à l'évaluation annuelle, concernant à la fois le personnel permanent et le personnel temporaire, de même que les stagiaires. En dehors des questions ordinaires de conservation des données, d'information, etc., l'accent a été mis sur la limitation des finalités: aucune donnée collectée à des fins d'évaluation ne peut être utilisée pour une finalité incompatible. La conservation des données dans les dossiers personnels est aussi à prendre en considération dans le cadre de ces opérations. Dans un cas portant sur la surveillance des appels téléphoniques, des données relatives au trafic faisaient partie du système, et l'article 37 était donc aussi applicable.

Enquêtes administratives et mesures disciplinaires: trois cas de contrôle préalable a posteriori ont été traités dans ce domaine. Comme dans les cas de contrôle préalable proprement dit (voir point 2.3.5), il était primordial de distinguer les dossiers personnels des dossiers disciplinaires ou concernant des enquêtes administratives afin de garantir le respect des délais de conservation des données. Un des principaux problèmes rencontrés est qu'il semble y avoir une contradiction entre le principe de conservation limitée des données, auquel s'ajoute le principe de prescription des sanctions, et l'interprétation actuelle de l'article 10, point i), de l'annexe IX du statut. Les recommandations du CEPD et les travaux en cours tendent à réconcilier le principe de protection des données avec la nécessité de prendre en compte les antécédents dans les cas de nouveau manquement passible d'une sanction disciplinaire.

2.3.5. Principales questions soulevées par les cas de contrôle préalable proprement dit

Normalement, le CEPD devrait rendre son avis avant qu'un traitement ne soit entrepris, de sorte que les droits et les libertés des personnes concernées soient garantis dès le départ. Tel est l'objet de l'article 27. Parallèlement au traitement des cas de contrôle préalable a posteriori, quatre cas de contrôle préalable proprement dit ([8]) ont été notifiés au CEPD en 2005. La conclusion générale tirée de l'examen de tous ces cas est que l'information est souvent moins concrète dans le cadre du contrôle préalable proprement dit que dans le cadre du contrôle préalable a posteriori, pour ce qui a trait au traitement des données. Dans les cas de contrôle préalable proprement dit, les règles de procédure constituent un aspect essentiel de la notification.

Le dossier «Compass» de la Cour des comptes concernait la nouvelle procédure d'évaluation du personnel. Les seules recommandations émises afin d'améliorer le système du point de vue de la protection des données étaient d'inclure les informations prévues à l'article 11, paragraphe 1, point f), et à l'article 12, paragraphe 1, point f), afin d'assurer la loyauté du traitement, d'adopter des mesures de sécurité dans les communications et de limiter l'accès aux données en cas d'appel.

Le dossier «Harcèlement» de la Cour des comptes portait sur un système destiné à faire face aux situations de harcèlement. Au départ, il a été déclaré que la phase «informelle» de la procédure établie par la Cour des comptes n'entrait pas dans le champ d'application du règlement dans la mesure où il n'y avait pas d'enregistrement des données personnelles collectées. Le CEPD a estimé qu'il était primordial que cette phase informelle soit couverte par le règlement afin que les garanties relatives au traitement des données à caractère personnel puissent être pleinement mises en œuvre. Compte tenu de la sensibilité de ces questions, des recommandations ont été émises dans de nombreux domaines (base juridique, information des personnes concernées, limitation des finalités, etc.).

Dans le dossier «Enquêtes administratives et procédures disciplinaires internes» de la Cour des comptes, le CEPD a notamment émis des recommandations concernant le traitement des données sensibles définies à l'article 10 et les droits d'accès et de rectification (qui revêtent un sens particulier dans ce contexte). La principale question était celle de la distinction entre les dossiers disciplinaires et les dos-

([8]) C'est-à-dire portant sur des opérations de traitement dont la mise en œuvre n'a pas encore débuté.

siers personnels et des différentes règles applicables en matière de conservation des données.

Les mêmes questions se posaient dans le dossier «Enquêtes administratives internes» de la Banque centrale européenne. Ces enquêtes peuvent à terme entraîner l'ouverture de procédures disciplinaires. En l'espèce, la possibilité d'intercepter des communications téléphoniques a été analysée, et une approche restrictive a été considérée comme acceptable. Le CEPD est parvenu à une interprétation logique de la limitation de la conservation des données relatives au trafic des communications en interprétant conjointement les articles 37 et 20 du règlement.

2.3.6. Consultations

En cas de doute quant à la nécessité d'un contrôle préalable, le délégué à la protection des données doit consulter le CEPD sur le dossier (article 27, paragraphe 3). En 2005, les délégués à la protection des données ont consulté le CEPD sur plusieurs sujets.

Le CEPD a précisé que doivent être soumis à un contrôle préalable:

— le contrôle des données de trafic relatives aux communications électroniques dans les institutions et organes (la cinquième catégorie prioritaire en ce qui concerne les cas de contrôle préalable a posteriori), dans la mesure où il porte sur l'évaluation du comportement des personnes;

— les systèmes visant à faire face au problème du harcèlement sur le lieu de travail, pour les mêmes motifs;

— les traitements destinés à une réorientation professionnelle du personnel, effectués par un groupe composé notamment d'un médecin, d'une assistante sociale, etc.;

— les nouvelles procédures de promotion.

Dans d'autres cas, le contrôle préalable n'a pas été jugé nécessaire:

— une procédure d'examen visant à accorder ou non le bénéfice d'un droit, d'une prestation ou d'un contrat, parce que l'article 27, paragraphe 2, point d), fait seulement référence à l'exclusion. Cependant, si une évaluation a lieu, le cas entre dans le champ d'application de l'article 27, paragraphe 2, point b);

— la gestion des structures administratives, telles que les descriptifs de postes, parce qu'ils n'impliquent pas d'évaluation et qu'il n'existait aucun autre risque;

— le télétravail, sauf si des mécanismes d'évaluation sont introduits dans le système;

— l'externalisation des missions des équipes de secours d'urgence (dans la mesure où la sélection des membres des équipes est sous l'entière responsabilité d'une entité privée).

Le traitement des données à caractère médical est un domaine complexe:

— le traitement, par les services administratifs d'une institution ou d'un organe, de données relatives à la santé est soumis au contrôle préalable, conformément à l'article 27, paragraphe 2, point a);

— lorsque les services médicaux sont gérés en externe par une autre institution ou organe communautaire, ils doivent faire l'objet d'un contrôle préalable au niveau de ce dernier et non au niveau de l'organe qui a externalisé ses services;

— si les services sont assurés par une société privée, le règlement ne s'applique pas et la législation nationale transposant la directive 95/46/CE est applicable. En conséquence, il ne devrait pas y avoir de contrôle préalable de la part du CEPD;

— un cas de figure limite a été analysé, dans lequel les services médicaux étaient assurés par un médecin et une infirmière dans les locaux de l'institution. Dans la mesure où il a été conclu que l'institution exerçait le rôle et les compétences d'un responsable du traitement, le contrôle préalable a été jugé nécessaire;

— les données relatives à la santé ont aussi constitué un critère déterminant pour considérer qu'un traitement visant à prendre en compte les handicaps de certains membres du personnel en cas d'urgence et à leur assurer des places de stationnement spéciales entrait dans le champ d'application du contrôle préalable.

Par ailleurs, pour être fonctionnels, les systèmes «généraux» à plusieurs composantes ne font pas l'objet d'un contrôle préalable, même s'ils comportent des sous-systèmes entrant dans le champ d'application de l'article 27. Dans ces cas, la notification du système général a été utilisée comme information générale de

base pour le contrôle du sous-système. Un exemple clair est celui du système Sysper 2 de la Commission, qui comprend des traitements tels que le REC (rapport d'évolution de carrière du personnel), évidemment soumis au contrôle préalable.

2.3.7. Suivi des avis et consultations relatifs au contrôle préalable

Lorsque le CEPD rend un avis sur un cas qui lui est soumis en vue d'un contrôle préalable, ou lorsqu'il analyse un cas pour décider de la nécessité d'un contrôle préalable et que certains aspects critiques semblent nécessiter des mesures de correction, l'avis émis par le CEPD peut être assorti d'une série de recommandations qui doivent être prises en considération afin de rendre le traitement conforme au règlement. 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. Il peut en particulier saisir l'institution ou l'organe communautaire concerné.

En outre, le CEPD peut 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), ou adresser un avertissement ou une admonestation au responsable du traitement. Il peut aussi ordonner la rectification, le verrouillage, l'effacement ou la destruction de toutes les données, ou interdire temporairement ou définitivement un traitement. Dans le cas où les décisions du CEPD ne seraient pas respectées, celui-ci a le droit de saisir la Cour de justice des Communautés européennes dans les conditions prévues par le traité CE.

Tous les cas de contrôle préalable ont abouti à des recommandations. Comme expliqué plus haut (aux points 2.3.4 et 2.3.5), la plupart des recommandations concernent l'information des personnes concernées, les délais de conservation des données, la limitation des finalités et les droits d'accès et de rectification. Les institutions et organes sont disposés à suivre ces recommandations et, à ce jour, il n'a pas été nécessaire de prendre des décisions d'exécution. Le temps nécessaire à la mise en œuvre de ces mesures diffère selon les cas. En 2005, six dossiers ont été clos, car toutes les recommandations avaient été mises en œuvre ([9]). Dans un dossier ([10]), une mesure reste en suspens.

En ce qui concerne le suivi des consultations sur la nécessité d'un contrôle préalable a posteriori, si la réponse a été positive et que le cas relève d'une catégorie prioritaire (sept cas en 2005), la réception de la notification fait l'objet d'un suivi, et, si nécessaire, un rappel est adressé. Lorsque le cas ne relève pas d'une catégorie prioritaire, le suivi consiste à demander qu'une notification soit envoyée en temps utile. Dans les cas de contrôle préalable proprement dit, la notification est demandée immédiatement. Dans les autres cas, il n'a pas été conclu à l'existence de risques spécifiques au sens de l'article 27, mais il convenait néanmoins de modifier certains aspects; un dossier a été clos, car les modifications requises avaient été effectuées, et les deux autres sont encore pendants.

2.3.8. Conclusions et perspectives

L'année 2005 a été une année d'intense activité dans le domaine du contrôle préalable. Les résultats sont assez satisfaisants, mais plusieurs institutions et organes n'ont pas envoyé de notifications en vue d'un contrôle préalable a posteriori dans les domaines prioritaires recensés. L'année 2006 est une année décisive pour l'obtention de ces informations et la réalisation de l'analyse des traitements dans tous les organes et institutions, pour ce qui concerne ces domaines. Ce processus devrait s'achever au plus tard au printemps 2007. Le CEPD mettra tout en œuvre pour atteindre cet objectif. Les nouveaux organes, mais aussi les institutions qui existent depuis plus longtemps, doivent examiner leurs traitements de données dans tous les domaines, mais plus particulièrement dans les domaines prioritaires, afin de veiller à respecter ce délai.

Une attention particulière sera portée en 2006 aux communications électroniques. Le CEPD prépare actuellement un document sur le sujet (voir point 2.7). Étant donné que le contrôle des communications électroniques à des fins de gestion du trafic et du budget, y compris la vérification de l'usage autorisé, tel qu'il est décidé par chaque institution et or-

([9]) Conseil de l'Union européenne, dossier 2004-319; Parlement européen, dossiers 2004-13 et 2004-126; Commission européenne, dossiers 2004-95 et 2004-96; OHMI, dossier 2004-174.

([10]) Commission européenne, dossier 2004-196.

gane, est soumis au contrôle préalable conformément à l'article 27, paragraphe 2, point b), les délégués à la protection des données devront envoyer les notifications pertinentes relatives aux systèmes existants dès que le CEPD aura publié son document sur le sujet, lequel comportera la liste visée à l'article 37, paragraphe 2.

Il faut également sensibiliser les institutions et organes à l'éventuelle nécessité d'un contrôle préalable lors de la phase de conception de nouveaux systèmes. Le calendrier de mise en œuvre des nouveaux projets doit tenir compte du délai nécessaire à l'institution ou à l'organe pour permettre au délégué à la protection des données d'adresser une notification au CEPD et du délai nécessaire au CEPD pour rendre son avis, afin que l'institution ou l'organe puisse mettre en œuvre les recommandations du CEPD avant de lancer le traitement.

En ce qui concerne la procédure, il serait souhaitable, quand des informations complémentaires sont demandées par le CEPD, de les lui fournir dans un délai plus court. En fait, si les formulaires de notification sont parfaitement remplis et que des documents d'appui exhaustifs sont fournis, les demandes d'informations complémentaires devraient devenir l'exception et non plus la règle, comme c'est le cas aujourd'hui encore.

Il convient d'apporter un soutien aux délégués à la protection des données récemment nommés et d'élaborer un calendrier des évaluations bilatérales organisées avec tous les délégués quant à l'avancement du processus de notification, en vue d'atteindre les objectifs précités. Il sera fort utile, dans ce contexte, de pouvoir disposer d'un document stratégique présentant une mise à jour des pratiques et des conclusions relatives au contrôle préalable.

2.4. Plaintes

2.4.1. Introduction

Conformément à l'article 32, paragraphe 2, à l'article 33 et à l'article 46, point a), du règlement, toute personne physique peut présenter une plainte au CEPD indépendamment de sa nationalité ou de son lieu de résidence ([11]). Les plaintes ne sont recevables que si elles émanent d'une personne physique et concernent la violation du règlement par une institution ou un organe de l'Union européenne lors du traitement de données à caractère personnel dans le cadre de l'exercice d'activités qui relèvent en tout ou en partie du champ d'application de la législation communautaire. Comme on le verra ci-après, un certain nombre de plaintes présentées au CEPD ont été déclarées irrecevables car le CEPD n'était pas compétent.

Lorsque le CEPD reçoit une plainte, il transmet un accusé de réception à l'auteur de la plainte, sans se prononcer sur la recevabilité, sauf dans le cas où la plainte est manifestement irrecevable sans qu'il soit nécessaire de procéder à un examen complémentaire. Le CEPD demande aussi à l'auteur de la plainte de l'informer d'éventuelles autres actions engagées devant une juridiction nationale, la Cour de justice des Communautés européennes ou auprès du Médiateur européen (pendantes ou non).

Si la plainte est recevable, le CEPD procède à une enquête, notamment en contactant l'institution ou l'organe concerné ou en demandant des renseignements complémentaires à l'auteur de la plainte. Le CEPD est habilité à obtenir du responsable du traitement ou de l'institution ou organe concerné l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires pour les besoins de l'enquête ainsi que l'accès à tous les locaux dans lesquels un responsable du traitement ou une institution ou un organe exerce ses activités.

Le CEPD a reçu 27 plaintes en 2005, dont 5 seulement ont été déclarées recevables et ont été examinées de manière approfondie par le CEPD. De plus, 4 décisions ont été adoptées par le CEPD concernant

([11]) Selon l'article 32, paragraphe 2, «[…] toute personne concernée peut présenter une réclamation au Contrôleur européen de la protection des données si elle estime que les droits qui lui sont reconnus à l'article 286 du traité ont été violés à la suite du traitement de données à caractère personnel la concernant, effectué par une institution ou un organe communautaire».
En vertu de l'article 33, «Toute personne employée par une institution ou un organe communautaire peut présenter une réclamation au Contrôleur européen de la protection des données pour une violation alléguée des dispositions du présent règlement régissant le traitement des données à caractère personnel, sans passer par les voies officielles».
Conformément à l'article 46, point a), le CEPD «entend et examine les réclamations et informe la personne concernée des résultats de son examen dans un délai raisonnable».

des plaintes présentées en 2004. Ces dossiers seront également rapidement évoqués ci-après.

2.4.2. Plaintes déclarées recevables

Dossiers 2004 en suspens

Comme on l'a mentionné ci-dessus, bien que certains dossiers aient été déposés en 2004, le CEPD n'a rendu de décision qu'en 2005.

Une plainte reçue par le CEPD en 2004 (dossier 2004-111) concernait la divulgation de données à caractère personnel concernant des personnes impliquées dans une affaire relative au droit de la concurrence. La Commission peut décider que certaines données à caractère personnel recueillies dans le cadre d'une affaire relative à la concurrence (ne) sont (pas) confidentielles. L'auteur de la plainte a contesté la décision prise à son égard. Bien que l'auteur de la plainte ait soulevé des questions intéressantes, il n'a pas fourni au CEPD les informations requises pour qu'il puisse poursuivre l'examen du dossier. Par conséquent, le CEPD n'a pas été en mesure de rendre une décision.

Une autre plainte, en suspens depuis 2004 (dossier 2004-329), portait sur la collecte de données nécessaires pour le remboursement de frais de voyage à un expert ayant participé à une réunion organisée par la Commission européenne (qualité des données: article 4 du règlement). Le CEPD a interrogé la Commission à ce titre et a finalement conclu que la collecte de données à caractère personnel était pertinente, adéquate et non excessive.

Enfin, une plainte reçue en 2004 (dossier 2004-7) concernait l'accès illicite à des informations contenues dans le système Sysper 2 (système d'information de la Commission européenne) et la diffusion illicite de celles-ci en violation de l'article 22 du règlement (sécurité). À l'issue d'un échange d'informations sur ce dossier, la Commission a informé le CEPD qu'une enquête serait ouverte dans le cadre de l'Office d'investigation et de discipline.

Dossiers 2005

Une plainte a été présentée contre le Parlement européen en raison de la publication des noms de pétitionnaires (dossier 2005-40). Il s'agissait de savoir si le traitement était licite (article 5) et si le niveau d'information fourni était suffisant pour que le consentement de la personne concernée constitue un motif valable justifiant le traitement/la divulgation (article 2). Le CEPD a principalement conclu que le traitement était licite parce qu'il était fondé non pas sur un consentement indubitable mais sur l'article 5, points a) et b), à savoir l'exécution d'«une mission effectuée dans l'intérêt public» et le «respect d'une obligation légale». L'information fournie aux personnes concernées était cependant insuffisante et le CEPD a donc suggéré que le secrétariat de la commission des pétitions modifie les formulaires utilisés pour déposer une pétition afin de mieux attirer l'attention sur les conséquences de cet acte. Le CEPD a aussi suggéré que l'on introduise la possibilité de refuser la divulgation des données pour des raisons impérieuses et légitimes.

Une plainte a été présentée contre la Commission européenne en ce qui concerne le «profil» d'une personne en ligne (dossier 2005-112). Un des participants à une conférence de trois jours organisée par la Commission européenne voulait que le profil qu'il avait communiqué avant la conférence et qui apparaissait dans une partie spécifique du site internet Europa soit retiré du site. La personne concernée a contacté le CEPD pour s'opposer (article 18) à la divulgation de son curriculum vitae. Le CEPD a transmis la demande au fonctionnaire responsable du site internet en question, en lui demandant de se pencher sur le fond du dossier. Le responsable a ultérieurement décidé de retirer le profil de la personne concernée du site internet.

Une autre plainte portait sur le droit d'accès (article 13) à des données à caractère personnel dans le cadre d'un concours interne de l'OHMI (dossier 2005-144). Cette plainte soulevait des questions intéressantes quant au droit d'accès aux données dans le cadre des procédures de sélection organisées par l'Office européen de sélection du personnel. Ce dossier a donné lieu à une enquête sur place réalisée par le CEPD. À la suite de cette enquête, le CEPD a considéré que l'accès aux données devrait être accordé, droit dont l'auteur de la plainte a bénéficié par la suite.

Une autre plainte a été présentée dans le cadre d'une procédure de sélection au sein du Parlement européen (dossier 2005-182). L'auteur de la plainte (un candidat à un poste) demandait la rectification de ses données à caractère personnel dans la base de données du Parlement européen (article 14). Le CEPD a

décidé que le personnel devait être informé du droit d'accès et de rectification concernant certaines bases de données. Cependant, pour ce qui est de la rectification même des données, le CEPD a indiqué qu'il n'est habilité à intervenir qu'en ce qui concerne les données factuelles mais que les données d'évaluation ne relèvent pas de sa compétence.

Une plainte a été présentée par un journaliste qui contestait la divulgation — non explicite — de son nom par un communiqué de presse de l'OLAF dans le cadre d'une affaire de corruption (dossier 2005-190). Il invoquait le traitement loyal des données (article 4) et le droit à la rectification (article 14). L'auteur de la plainte avait déjà présenté une plainte au Médiateur. Le CEPD a clos le dossier dans la mesure où il ne pouvait rien ajouter aux conclusions du Médiateur dans cette affaire.

Une plainte a été transmise au CEPD (dossier 2005-377) concernant certaines informations publiées dans la presse au sujet d'une procédure disciplinaire à l'encontre de deux fonctionnaires de l'UE. Le but de la plainte était d'établir comment ces informations avaient pu être diffusées en dehors de la Commission européenne. Le CEPD a décidé de ne pas ouvrir d'enquête, en l'absence de preuves suffisantes.

2.4.3. Plaintes déclarées irrecevables: principaux motifs d'irrecevabilité

Sur les 27 plaintes reçues en 2005, 22 ont été déclarées irrecevables parce qu'elles ne relevaient pas de la compétence du CEPD. En effet, les dossiers ne concernaient pas le traitement de données à caractère personnel par des institutions et organes communautaires: ce sont donc les autorités nationales chargées de la protection des données qui auraient dû être saisies. Dans un cas, la plainte concernait une information diffusée sur le site internet du Conseil de l'Europe qui n'a pas le statut d'institution ou d'organe communautaire. Le CEPD a donc renvoyé l'auteur de la plainte devant le Conseil de l'Europe.

2.4.4. Collaboration avec le Médiateur européen

Conformément à l'article 195 du traité CE, le Médiateur est habilité à recevoir les plaintes relatives à des cas de mauvaise administration dans l'action des institutions ou organes communautaires. Le Médiateur européen et le CEPD ont des compétences qui se chevauchent dans le cadre du traitement des plaintes dans la mesure où les cas de mauvaise administration peuvent concerner le traitement des données à caractère personnel. Par conséquent, les plaintes dont le Médiateur est saisi peuvent porter sur des questions liées à la protection des données. De même, les plaintes présentées au CEPD peuvent concerner des plaintes qui ont déjà, en tout ou en partie, fait l'objet d'une décision du Médiateur.

Afin d'éviter les doubles emplois inutiles et d'assurer, dans toute la mesure du possible, une approche cohérente des questions liées à la protection des données, tant générales que spécifiques, que soulèvent les plaintes, les deux institutions procèdent à un échange d'informations concernant l'introduction de plaintes qui présentent un intérêt pour l'autre institution, ainsi que la suite réservée aux plaintes.

Des travaux complémentaires sont réalisés afin de déterminer les différentes formes que pourrait prendre la collaboration entre le Médiateur européen et le CEPD pour devenir plus structurelle dans un avenir proche.

2.4.5. Travaux complémentaires dans le domaine des plaintes

Le CEPD a travaillé à la rédaction d'un manuel interne pour le traitement des plaintes par les services du CEPD.

Deux membres des services du CEPD ont aussi participé à un atelier de traitement des plaintes auprès des autorités nationales chargées de la protection des données à Paris, en novembre 2005. Durant cet atelier de deux jours, les membres des services du CEPD ont présenté un aperçu des plaintes traitées par le CEPD et des éléments de la stratégie de communication. L'atelier a constitué une occasion intéressante de partager des expériences dans ce domaine et de tirer des enseignements du traitement des plaintes au niveau national.

2.5. Enquêtes

Le Contrôleur adjoint et un membre de son équipe ont mené la première enquête du CEPD sur les lieux en vertu de l'article 47 du règlement dans le cadre

En ce qui concerne le dossier 2005-0190, voyez les corrections dans le rapport annuel 2007, paragraphe 2.4.2 "Présentation d'un dossier dans le rapport annuel 2005".

d'une plainte relative au droit d'accès aux données. Les données concernaient les résultats d'un examen oral lors d'une procédure de sélection interne au sein d'une agence de l'UE. La visite a permis au Contrôleur de déterminer la portée exacte des données qui faisaient l'objet de la demande d'accès. Le Contrôleur a aussi mis la visite à profit pour rencontrer différents services de l'agence et expliquer les principales fonctions et activités du CEPD.

2.6. Accès du public aux documents et protection des données

Comme il l'avait annoncé dans le rapport annuel 2004, le CEPD a déployé des efforts importants pour élaborer un document de référence — qui a été présenté en juillet — portant sur la relation entre le règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et le règlement relatif à l'accès du public aux documents ([12]). Ces deux droits fondamentaux, dont aucun n'a la primauté sur l'autre, sont des éléments essentiels de la vie démocratique au sein de l'Union européenne. Ils constituent aussi un élément important de la notion de bonne gestion des affaires publiques. De nombreux documents détenus par les institutions et les organes de l'UE contiennent des données à caractère personnel. Ce sont les raisons pour lesquelles il est de la plus haute importance d'aborder la possibilité de divulguer un document public contenant des données à caractère personnel de manière appropriée et bien réfléchie.

Le document comporte une description ainsi qu'une analyse de la relation entre les deux droits fondamentaux et fournit des exemples pratiques ainsi qu'une liste des points à vérifier afin de guider les fonctionnaires et les services responsables de l'administration de l'UE. Le document a été bien perçu de manière générale, et certaines institutions et organes s'en servent quotidiennement dans leur travail.

Le document a pour ligne directrice le principe suivant: l'accès aux documents détenus par l'administration de l'UE ne peut être refusé systématiquement au seul motif que ces documents contiennent des données à caractère personnel. L'exception de l'article 4, paragraphe 1, point b), du règlement relatif à l'accès du public ([13]) prévoit qu'il doit y avoir atteinte à la vie privée d'une personne pour empêcher la divulgation. Tout en préconisant d'examiner chaque cas de manière concrète et à titre individuel, le document replace dans son contexte l'exception dont le libellé a été soigneusement choisi, en faisant valoir que les critères figurant ci-après doivent être satisfaits pour qu'un document public ne soit pas divulgué:

1) la vie privée de la personne concernée doit être en jeu;
2) l'accès du public doit affecter sérieusement la personne concernée;
3) l'accès du public n'est pas autorisé par la législation relative à la protection des données.

Le document interprète le troisième critère de la façon suivante: il convient d'évaluer au cas par cas si la divulgation d'un document qui a trait à la vie privée d'une personne est conforme aux dispositions des articles 4, 5 et 10 du règlement relatif à la protection des données. Si la divulgation est conforme aux principes relatifs à la qualité et au traitement licite des données, le CEPD estime qu'il est proportionné de rendre le document public, tant que celui-ci ne contient pas de données sensibles.

Enfin, le document énonce deux notions importantes qui doivent être prises en considération:

1) les personnes exerçant des fonctions publiques suscitent un plus grand intérêt de la part du public. Dans ces circonstances, il peut être nécessaire de divulguer leurs données à caractère personnel;
2) une approche proactive est toujours souhaitable. Par conséquent, l'institution ou l'organe informe la personne concernée de ses obligations en matière de transparence et de ce que certaines données à caractère personnel sont, par analogie, susceptibles d'être rendues publiques.

2.7. Contrôle des communications électroniques

L'utilisation des outils de communication électronique au sein des institutions et organes communautaires génère de plus en plus de données à caractère

([12]) Règlement (CE) nº 1049/2001.

([13]) «Les institutions refusent l'accès à un document dans le cas où sa divulgation porterait atteinte à la protection […] de la vie privée et de l'intégrité de l'individu, notamment en conformité avec la législation communautaire relative à la protection des données à caractère personnel.»

personnel dont le traitement entraîne l'application des dispositions du règlement. À la fin de 2004, le CEPD a entamé des travaux concernant le traitement des données générées par l'utilisation des communications électroniques (téléphone, courrier électronique, téléphone mobile, internet, etc.) dans les institutions et organes communautaires. Ce projet était partiellement fondé sur des informations générales, fournies par les délégués à la protection des données, sur les pratiques de leur institution dans ce domaine. Il s'est aussi inspiré des conclusions rendues dans le cadre de l'examen de dossiers présentés au CEPD en vue d'un contrôle préalable. Un projet de document a été soumis aux DPD et devrait faire l'objet de nouvelles discussions avec les parties prenantes avant sa publication finale en juin 2006.

2.8. Eurodac

En janvier 2004, l'autorité de contrôle commune d'Eurodac a été remplacée par le CEPD, conformément à l'article 20, paragraphe 11, du règlement Eurodac ([14]). Depuis lors, le CEPD a été chargé de contrôler l'unité centrale d'Eurodac. Toutefois, le contrôle d'Eurodac dans son ensemble est essentiellement caractérisé par la coopération entre les autorités nationales de contrôle et le CEPD afin d'examiner les problèmes de mise en œuvre liés au fonctionnement d'Eurodac, de se pencher sur les difficultés qui peuvent éventuellement surgir lors des vérifications effectuées par les autorités nationales de contrôle et de formuler des recommandations en vue de trouver des solutions communes aux problèmes existants.

Contrôle de l'unité centrale

En tant qu'autorité de contrôle de l'unité centrale, le CEPD a lancé une inspection de grande ampleur en deux étapes:

— une première inspection des locaux de l'unité centrale et de l'infrastructure du réseau qui a abouti à un rapport final au début de 2006;

— un audit approfondi de la sécurité des bases de données de l'unité centrale et de ses locaux afin d'évaluer si les mesures de sécurité mises en place sont conformes aux exigences définies par le règlement Eurodac (qui devrait être mené à bien dans le courant de 2006).

Dans le cadre de la première inspection, le Contrôleur a effectué une visite des locaux d'Eurodac en mai 2005, a étudié de manière approfondie les documents relatifs au fonctionnement d'Eurodac et a rencontré à plusieurs reprises les différents fonctionnaires chargés de la sécurité et de la gestion du système. Ces premières mesures ont conduit à la rédaction d'un questionnaire détaillé qui a été transmis à la Commission. Ce questionnaire portait sur les points suivants: gestion des risques et des incidents, documents concernant la sécurité, contrôle de l'accès physique et électronique, sécurité des communications, éducation et formation à la sécurité de l'information, statistiques, accès direct et transmission directe des données provenant des États membres. Sur la base de l'analyse des réponses au questionnaire et de l'évaluation effectuée lors des visites, un projet de rapport a été préparé et transmis à la Commission en décembre 2005. Un rapport final, qui tenait compte des observations formulées par la Commission, a été établi en février 2006.

Parallèlement, le CEPD a pris les mesures nécessaires pour procéder à un audit de sécurité complet de l'unité centrale. À cette fin, un accord a été élaboré avec l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) en vue d'aider le CEPD à s'acquitter de cette tâche.

Coopération avec les autorités nationales chargées de la protection des données

Dans son rapport annuel 2004, le CEPD a présenté la façon dont il concevait le contrôle d'Eurodac ([15]). Dès lors, le CEPD a aussi élargi son rôle en créant une plate-forme de coopération en matière de contrôle et d'échange d'expériences avec les autorités nationales chargées de la protection des données. En tenant compte du cadre réglementaire applicable ainsi que

([14]) Règlement (CE) nº 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système «Eurodac» pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin.

([15]) Rapport annuel 2004, p. 34: «Le CEPD est l'autorité de contrôle pour l'unité centrale d'Eurodac et contrôle en outre la licéité de la transmission des données à caractère personnel par l'unité centrale aux États membres. Les autorités compétentes des États membres, pour leur part, contrôlent la licéité du traitement des données à caractère personnel, y compris de leur transmission à l'unité centrale, effectuée par l'État membre en question. En d'autres termes, le contrôle doit être exercé à ces deux niveaux, en étroite coopération.»

des rapports annuels publiés par la Commission sur le fonctionnement d'Eurodac ([16]), une liste de thèmes à débattre dans le cadre d'une réunion avec les autorités nationales chargées la protection des données a été élaborée, et un suivi au niveau national sur la base d'une méthodologie commune a été envisagé. Cette approche s'est révélée très utile dans le cadre du contrôle d'autres systèmes d'information à grande échelle, tels que le système d'information Schengen.

Une première réunion de coordination avec les autorités nationales chargées de la protection des données s'est tenue le 28 septembre 2005. Elle a donné lieu à un échange d'informations très positif et a été une occasion très utile de discuter d'une approche commune du contrôle. Les participants ont sélectionné, à partir d'une liste établie par le CEPD, quelques thèmes méritant une analyse plus approfondie et ont marqué leur accord sur trois points principaux: les recherches spéciales, la possibilité d'utiliser Eurodac à d'autres fins que celles prévues dans le règlement Eurodac, et la qualité technique des données. Ces questions seront examinées au niveau national et les résultats de cet examen seront compilés par le CEPD pour être ensuite discutés lors d'une deuxième réunion à la fin du printemps 2006. Le CEPD attend avec intérêt les résultats de cette première approche coordonnée.

([16]) Le deuxième rapport annuel a été publié le 20 juin 2005 sous la référence SEC(2005) 839.

3. Conseil

3.1. Introduction

La première année complète durant laquelle le CEPD a pleinement exercé ses fonctions consultatives a été importante pour deux raisons. En premier lieu, le CEPD a défini la politique à suivre dans le cadre de son rôle de conseiller des institutions communautaires concernant les propositions législatives (et les documents connexes). En second lieu, le CEPD a rendu des avis sur un certain nombre de propositions législatives importantes.

Le CEPD a défini sa politique dans un document stratégique dans lequel il faisait part de son ambition de devenir un conseiller faisant autorité, auquel serait conféré un vaste mandat couvrant toutes les questions liées au traitement des données à caractère personnel. L'interprétation large de ce mandat résulte de la description de la mission figurant à l'article 41 du règlement (CE) nº 45/2001 et a été confirmée par la Cour de justice. La Cour a souligné que cette mission consultative ne vise pas uniquement les traitements de données à caractère personnel effectués par les institutions ou les organes communautaires ([17]). Le mandat porte également sur les propositions législatives relevant du troisième pilier du traité UE (coopération policière et judiciaire en matière pénale).

Des propositions importantes ont été présentées par la Commission en 2005 pour mettre en œuvre le programme de La Haye approuvé par le Conseil européen en novembre 2004. Ce programme a renforcé le caractère prioritaire de l'action de l'UE dans le cadre de l'espace de liberté, de sécurité et de justice en mettant l'accent sur l'aspect répressif et en créant la possibilité d'accroître les échanges de données entre les autorités des États membres. Dans ce contexte, le programme reconnaît la nécessité de se doter de règles appropriées pour la protection des données à caractère personnel. Les avancées les plus importantes en matière de protection des données ont été les suivantes:

— un troisième élément central de la législation relative à la protection des données au niveau européen a été élaboré: la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale a pour objectif d'assurer la protection des données dans un domaine où de nombreuses données sensibles sont traitées et où le niveau de protection prévu sur le plan européen peut être considéré comme insuffisant, dans la mesure où la directive 95/46/CE ne s'applique pas;

— les propositions législatives concernant le système d'information Schengen de deuxième génération (SIS II) et le système d'information sur les visas (VIS) ont contribué au développement de systèmes d'information à grande échelle. Par exemple, le VIS est conçu pour traiter 20 millions d'entrées par an concernant les personnes qui demandent un visa de court séjour;

— pour la première fois, des acteurs privés seront tenus en vertu de la législation communautaire de conserver des données à caractère personnel et donc de mettre en place des bases de données à la seule fin de lutter contre des formes graves de criminalité. Cette obligation est la conséquence de la directive sur la conservation des données.

Le CEPD exerce son mandat consultatif non seulement en rendant des avis sur les propositions législa-

([17]) Ordonnances du 17 mars 2005 dans deux affaires concernant le traitement des données «PNR» (voir point 3.4.2).

tives mais aussi de plusieurs autres façons. Le CEPD est intervenu pour la première fois dans des affaires portées devant la Cour de justice, en particulier dans les affaires «PNR» et a fait valoir son point de vue sur des questions importantes relatives à la protection des données auprès de la Cour. De plus, le CEPD a exposé sa position à plusieurs reprises notamment lors de conférences et de séminaires publics et dans le cadre de réunions de la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen.

Enfin, le mandat du CEPD en tant qu'organe consultatif n'est pas strictement lié aux propositions législatives. L'article 28, paragraphe 1, du règlement lui confère un mandat dans le cadre des mesures administratives relatives au traitement des données à caractère personnel impliquant une ou plusieurs institutions ou organes communautaires. L'article 46, point d), définit ce mandat de manière plus détaillée pour ce qui est des règles d'application.

La présente partie du rapport annuel se propose non seulement de présenter un panorama des principales activités réalisées en 2005 et — dans la mesure du possible — de leurs effets, mais également d'envisager les défis auxquels le Contrôleur sera confronté dans les années à venir. Il convient ainsi d'analyser les conséquences des nouveaux progrès technologiques ainsi que de l'évolution dans les domaines politique et législatif.

3.2. Politique suivie par le CEPD

Document stratégique intitulé «Le CEPD en tant que conseiller des institutions communautaires à l'égard des propositions de législation et documents connexes» (mars 2005)

Par ce document stratégique, le CEPD entend se définir comme un conseiller faisant autorité, fiable et cohérent de la Commission, du Parlement européen et du Conseil dans le cadre du processus législatif. En d'autres mots, le CEPD envisage de devenir un partenaire incontournable dans le cadre de ce processus. Ce document précise les trois éléments fondamentaux de son rôle consultatif.

Le premier élément concerne la portée de sa fonction, à savoir les questions pour lesquelles la consultation du CEPD est requise. Comme on l'a précisé précédemment, la fonction est large dans la mesure où les propositions législatives portent sur de nombreux thèmes qui peuvent avoir une incidence sur la protection des données à caractère personnel.

Le deuxième élément a trait à la teneur des interventions. Les interventions du CEPD sont fondées sur le postulat général selon lequel il convient de contribuer au processus législatif non seulement de manière critique mais également constructive:

— il est essentiel de mettre en lumière l'importance que revêt une proposition législative à l'égard de la protection des données à caractère personnel;

— l'article 6 du traité UE préconise de veiller au respect des droits fondamentaux tels qu'ils sont garantis par la convention européenne des droits de l'homme (CEDH), en particulier par la jurisprudence relative à l'article 8 de la CEDH. Des instruments juridiques ne devraient pas priver une personne privée de l'essentiel de la protection à laquelle elle a droit;

— le CEPD ne jouera pas seulement le rôle de «gendarme» de la vie privée, mais il prendra en considération le fait que la bonne gestion des affaires publiques requiert aussi le respect d'autres intérêts publics justifiés;

— les propositions ne devraient pas être simplement rejetées: le CEPD proposera des solutions de remplacement.

Le troisième élément est lié au rôle que le CEPD envisage de jouer dans le cadre institutionnel. Afin d'exercer, de manière efficace, sa fonction de conseiller auprès des trois acteurs fondamentaux du processus législatif, il est de la plus haute importance de choisir le bon moment pour intervenir. Le document stratégique prévoit différents moments. Avant que la proposition de la Commission ne soit adoptée, le service responsable de cette institution peut procéder à une consultation informelle. Il est désormais d'usage que cette consultation informelle ait lieu parallèlement à la consultation interne interservice au sein de la Commission. Ensuite a lieu la consultation officielle et publique sur la base de la proposition de la Commission. Le CEPD s'efforce de présenter ses avis à un stade précoce de la procédure au sein du Parlement européen et du Conseil. Une troisième étape facultative est devenue une pratique courante dans les dossiers les plus importants: une nouvelle consultation informelle par le Parlement européen et le Conseil. Le CEPD a non seulement présenté son

avis formel oralement à plusieurs reprises dans le cadre de la commission LIBE du Parlement européen et dans le cadre des groupes de travail compétents du Conseil, mais a aussi accepté d'être consulté à nouveau — très souvent à la demande de l'une de ces institutions — à un stade ultérieur.

Enfin, le rôle du CEPD et les fonctions consultatives du Groupe de l'article 29 se recouvrent largement. Le document stratégique souligne que ces deux organes ne devraient pas se faire concurrence. En pratique, ils exercent un rôle complémentaire, dans l'intérêt de la protection des données à caractère personnel. Le fait que deux organes présentent des avis sur les propositions importantes ne fait que renforcer l'intérêt qui est accordé à la protection des données au cours du processus législatif, à condition, bien sûr, que les messages émanant de ces deux organes ne soient pas contradictoires. Aucune contradiction n'a encore été constatée et il ne devrait pas y en avoir à l'avenir, non seulement parce que le CEPD est membre du Groupe de l'article 29, mais aussi parce que les deux organes défendent les mêmes intérêts essentiels.

Lorsqu'une proposition est fondée sur le titre VI du traité UE (troisième pilier), cas dans lequel le Groupe de l'article 29 n'a pas de rôle consultatif officiel, il y a chevauchement entre les avis du CEPD et les avis d'autres groupes — informels — des autorités nationales chargées de la protection des données. Le CEPD a mis en place une approche pratique fondée sur la coopération qui fonctionne de manière satisfaisante.

Mise en œuvre du document stratégique

Plusieurs thèmes relevant de l'espace de liberté, de sécurité et de justice ont été au centre des activités du CEPD pendant l'année 2005. Le CEPD a pris en compte les éléments suivants:

— établissement du principe de proportionnalité, afin de déterminer si une proposition concilie la nécessité de maintenir l'ordre de manière adéquate et la protection des données à caractère personnel;

— approfondissement des questions liées aux systèmes d'information à grande échelle tels que le VIS et le SIS II, en particulier en ce qui concerne la sécurité de ces systèmes et l'accès à ceux-ci;

— soutien apporté à une avancée importante de la protection des données réalisée par la proposition de décision-cadre du Conseil relative à la protection des données dans le cadre du troisième pilier;

— au sein de la Commission, la DG Justice, liberté et sécurité devient de plus en plus la contrepartie naturelle du CEPD: elle est chargée des droits fondamentaux, coordonne la protection des données au sein de la Commission et traite la plupart des dossiers importants. Dans sa communication du 10 mai 2005 sur le programme de La Haye, la Commission a fixé dix priorités dans le programme de travail de la DG Justice, liberté et sécurité. La Commission met l'accent sur l'équilibre entre le principe de disponibilité — au centre de l'approche de la Commission — et la protection des droits fondamentaux;

— la deuxième DG qui traite de dossiers très importants pour la protection des données est la DG Société de l'information et médias. En 2005, les dossiers traités par cette dernière ne représentaient pas une partie importante du travail consultatif du CEPD, mais cela devrait changer en 2006.

En ce qui concerne la façon de procéder, le CEPD a mis au point une méthode de travail. Il a fondé ses priorités sur le programme de travail de la Commission pour 2005 ainsi que sur d'autres instruments de planification pertinents des institutions. Quelques dossiers ont été ajoutés sur l'initiative du CEPD. Les dossiers ont été classés soit «hautement prioritaires», lorsqu'ils requéraient une intervention proactive précoce du CEPD, et en tout état de cause son avis officiel, soit «faiblement prioritaires» lorsqu'ils ne requéraient pas une intervention proactive du CEPD (et n'aboutissaient pas nécessairement à un avis officiel).

Le CEPD envisage d'établir ses priorités de la même façon dans les années à venir et d'informer la Commission de ses premières conclusions.

3.3. Propositions législatives

3.3.1. Les avis du CEPD en 2005 [18]

Avis du 13 janvier 2005 concernant la proposition de décision du Conseil relative à l'échange d'informations extraites du casier judiciaire

La proposition de la Commission a été introduite comme une mesure ayant un horizon temporel limité, destinée à répondre à un besoin urgent de disposi-

[18] Voir annexe F.

tions relatives à l'échange d'informations extraites du casier judiciaire, jusqu'à ce qu'un instrument juridique plus définitif ait été mis en place. La nécessité de présenter cette proposition s'est fait sentir à la suite de l'affaire Fourniret, affaire qui a fait grand bruit dans l'opinion publique et qui concernait un ressortissant français qui avait déménagé en Belgique. Les autorités belges ne disposaient pas d'informations sur ses condamnations antérieures liées à des actes de pédophilie. La proposition contient deux nouvelles dispositions relatives à l'échange d'informations sur les condamnations.

La relative brièveté de l'avis du CEPD s'explique par l'urgence de la situation et le caractère temporaire de la mesure. Le CEPD a recommandé de limiter le champ d'application de la proposition à l'échange d'informations sur les condamnations liées à certaines infractions graves. Il a également suggéré qu'il conviendrait de préciser les garanties qui existent pour la personne concernée.

Avis du 23 mars 2005 sur la proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour

Cette proposition de la Commission vise à améliorer la mise en œuvre de la politique commune en matière de visas en facilitant l'échange de données entre les États membres. Le système VIS reposera sur une architecture centralisée comprenant une base de données dans laquelle les dossiers de demande de visa seront stockés dénommée «système central d'information sur les visas» (CS-VIS), ainsi qu'une interface nationale (NI-VIS) située dans les États membres. Le règlement envisage d'enregistrer les données biométriques (photographies et empreintes digitales) pendant la procédure de demande de visa et de les stocker dans la base de données centrale. Le système VIS contiendra (et permettra l'échange) des données biométriques d'un volume sans précédent (20 millions d'entrées par an relatives à des demandes de visa) qui pourrait atteindre 100 millions d'entrées à l'issue de la période de conservation maximale de cinq ans.

Le CEPD reconnaît que le développement d'une politique commune en matière de visa nécessite un échange efficace des données pertinentes. Le VIS constitue l'un des mécanismes susceptibles de garantir la fluidité des échanges d'informations. Néanmoins, ce nouvel instrument devrait se limiter à la collecte et à l'échange de données dans la mesure où ceux-ci sont nécessaires à la mise en place d'une politique commune en matière de visa et proportionnés à cet objectif. En particulier, un accès systématique des services répressifs ne serait pas conforme à cette finalité.

Tout en reconnaissant les avantages que présente l'utilisation des données biométriques dans le système VIS, le CEPD en souligne l'incidence majeure et suggère de l'assortir de garanties strictes. En outre, en raison des imperfections techniques du recours aux empreintes digitales, il y a lieu d'élaborer des procédures de secours et de les inclure dans la proposition, pour éviter des conséquences inacceptables pour un grand nombre de personnes.

Pour ce qui concerne le contrôle des visas aux frontières extérieures, le CEPD a considéré qu'il suffirait que les autorités compétentes contrôlant les visas n'aient accès qu'à la puce sécurisée, ce qui éviterait l'accès à la base de données centrale.

Avis du 15 juin 2005 sur la proposition de décision du Conseil relative à la conclusion d'un accord entre la Communauté européenne et le gouvernement du Canada sur le traitement des données relatives aux informations anticipées sur les voyageurs (API)/ dossiers passagers (PNR)

L'accord avec le Canada est le deuxième accord de ce type conclu avec des pays tiers sur ce sujet. Le premier accord conclu avec les États-Unis d'Amérique a été attaqué devant la Cour de justice par le Parlement européen, et le CEPD a soutenu les conclusions déposées par le Parlement (voir point 3.4.2). Le CEPD a axé son avis sur les différences principales qui existent entre l'accord conclu avec le Canada et celui conclu avec les États-Unis:

— la proposition prévoit un système de type «push» qui permet aux compagnies aériennes opérant dans la Communauté européenne de contrôler les transferts de données aux autorités canadiennes, contrairement au système «pull»;

— les engagements pris par les autorités canadiennes sont contraignants;

— la liste des données PNR à transférer est plus limitée et exclut le transfert d'informations sensibles;

— le système législatif de protection des données est beaucoup plus développé au Canada qu'aux États-Unis.

Le CEPD a approuvé les principaux éléments de la proposition. Cependant, il a conclu que l'accord requiert une modification de la directive 95/46/CE, raison pour laquelle l'avis conforme du Parlement européen aurait dû être obtenu avant de conclure l'accord.

Avis du 26 septembre 2005 sur la proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE

La proposition concernée a été présentée dans un contexte où les craintes suscitées par les attentats terroristes avaient pris de l'ampleur, et elle était étroitement liée à la lutte contre le terrorisme (et les autres formes graves de criminalité) au lendemain des attentats de Londres de juillet 2005.

Selon le CEPD, la proposition revêt la plus haute importance:

— pour la première fois, un instrument de droit européen oblige les personnes privées à conserver des données aux fins du maintien de l'ordre. Ce principe de base est contraire aux obligations actuellement édictées par le droit communautaire qui prévoit que les fournisseurs de services de télécommunications sont uniquement autorisés à collecter et à stocker des données relatives au trafic pour des raisons directement liées à la communication elle-même, y compris à des fins de facturation. Les données doivent ensuite être effacées (sauf exceptions);

— il s'agit d'une obligation qui concerne directement tous les citoyens de l'UE.

Le CEPD est conscient du fait que la disponibilité suffisante de certaines données relatives au trafic et de données de localisation peut constituer un instrument précieux pour les services répressifs et contribuer à la sécurité physique des personnes. Toutefois, dans son avis, le CEPD indique que les nouveaux instruments prévus dans la proposition en question n'en deviennent pas automatiquement nécessaires pour autant. Selon le CEPD, la nécessité de cette nouvelle obligation de conserver des données — dans son intégralité — n'a pas été démontrée de manière satisfaisante.

Néanmoins, tout en reconnaissant qu'un instrument juridique concernant la conservation des données pourrait bien être adopté quoi qu'il en soit, le CEPD s'est principalement penché sur la proportionnalité des mesures proposées. Il a souligné que la seule conservation des données relatives au trafic et des données de localisation n'est pas en soi une réponse pertinente ni efficace. Des mesures supplémentaires s'imposent pour permettre aux autorités d'avoir un accès ciblé et rapide aux données dont elles ont besoin dans un cas précis. De plus, la proposition devrait limiter les durées de conservation et la quantité de données à stocker et prévoir des mesures de sécurité satisfaisantes.

Le CEPD a demandé que la proposition soit modifiée en y introduisant:

— des dispositions portant spécifiquement sur l'accès aux données relatives au trafic et aux données de localisation par les autorités compétentes et sur l'utilisation ultérieure de ces données,

— des garanties supplémentaires pour la protection des données et de nouvelles dispositions incitant les fournisseurs à investir dans une infrastructure technique suffisante, en particulier l'indemnisation des frais supplémentaires.

Enfin, le CEPD s'est inscrit en faux contre l'argument juridique selon lequel une proposition relevant du premier pilier ne pourrait pas comporter de règles relatives à l'accès de la police et des autorités judiciaires à des données.

Avis du 19 octobre 2005 sur trois propositions concernant le système d'information Schengen de deuxième génération (SIS II)

Le système d'information Schengen (SIS) est un système informatique européen à grande échelle créé en 1995 pour compenser la suppression des contrôles aux frontières intérieures de l'espace Schengen. Un nouveau système d'information Schengen «de deuxième génération» (SIS II) remplacera le système actuel et permettra d'élargir l'espace Schengen aux nouveaux États membres de l'UE. Ce système présentera en outre de nouvelles caractéristiques telles qu'un accès élargi au SIS (par Europol, Eurojust, les

magistrats nationaux et les services chargés de l'immatriculation des véhicules), la mise en relation des signalements et l'ajout de nouvelles catégories de données, y compris les données biométriques (empreintes digitales et photographies). Les dispositions Schengen, élaborées sous la forme d'un cadre intergouvernemental, seront entièrement transformées en instruments juridiques européens, ce dont le CEPD se félicite.

Les propositions en vue de l'établissement du SIS II sont principalement les suivantes: une proposition de règlement qui réglementera les aspects du SIS II relevant du premier pilier (immigration) et une proposition de décision qui réglementera l'utilisation du SIS à des fins relevant du troisième pilier ([19]). En vertu du traité UE, il est nécessaire de réglementer ce système unique en recourant à deux instruments principaux. Le résultat est cependant extrêmement complexe et a nécessité une étude minutieuse de l'ensemble de l'environnement juridique. Le CEPD a souligné que, malgré sa complexité, le nouveau régime juridique devrait assurer un niveau élevé de protection des données, être fiable tant pour les citoyens que pour les autorités partageant leurs données et être cohérent dans son application à différents cadres (premier ou troisième pilier).

Le CEPD a recensé plusieurs points positifs qui constituent une amélioration par rapport à la situation actuelle, mais aussi certains sujets de préoccupation: l'ajout dans le SIS II de nouveaux éléments accroissant son éventuelle incidence sur la vie des personnes devrait être accompagné de précautions plus restrictives, décrites dans l'avis. Par exemple:

— l'accès aux données du SIS II ne peut être accordé à de nouvelles autorités sans que cela soit absolument justifié. Il convient également de le restreindre autant que possible, tant en ce qui concerne les données accessibles que les personnes autorisées à y accéder;

— la mise en relation des signalements ne peut jamais conduire, même indirectement, à une modification des droits d'accès;

— il semble que les incidences de l'introduction des données biométriques dans le système n'aient pas été analysées de manière assez approfondie et que la fiabilité de ces données ait été surestimée. Le CEPD reconnaît toutefois que l'introduction de ces données peut améliorer les prestations du système et aider les victimes d'une usurpation d'identité;

— le contrôle du système doit être assuré de façon cohérente et complète à la fois au niveau européen et au niveau national.

Avis du 19 décembre 2005 sur la proposition de décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale

Ladite proposition de la Commission a pour objet d'établir des normes communes pour la protection des données dans le cadre du troisième pilier, domaine actuellement régi par des législations nationales non harmonisées. Cette proposition qui vient à point nommé sera aussi importante que la directive 95/46/CE relative à la protection des données et la convention 108 du Conseil de l'Europe. Dans son avis, le CEPD s'est félicité de la proposition qui vise à garantir le droit fondamental à la protection des données à caractère personnel eu égard également à l'augmentation des échanges de données à caractère personnel entre les autorités répressives et les autorités judiciaires des États membres de l'UE.

Une protection efficace des données à caractère personnel est non seulement importante pour les personnes concernées, mais elle contribue aussi au succès de la coopération policière et judiciaire à proprement parler. Le CEPD a souligné qu'il importait de garantir la cohérence du texte avec la législation en vigueur en matière de protection des données (en particulier la directive 95/46/CE et la convention 108) en prévoyant un ensemble complémentaire de règles qui tiennent compte de la nature spécifique du domaine répressif. Il est essentiel que les principales règles de protection des données s'appliquent à toutes les données policières et judiciaires — pas seulement à celles échangées entre les États membres, mais aussi aux données utilisées dans un pays.

De l'avis du CEPD, les données à caractère personnel devraient être collectées et traitées pour des finalités déterminées et explicites (une infraction spécifique, une enquête précise, etc.), et leur utilisation ultérieure ne pourrait être autorisée que selon des conditions très strictes. De plus, il est impératif de trai-

([19]) Il existe même une troisième proposition: une proposition de règlement fondé sur le titre V (transports) concernant spécifiquement l'accès des services chargés de l'immatriculation des véhicules aux données du SIS.

ter les données concernant différentes catégories de personnes — les personnes suspectes, les personnes condamnées, les victimes, les témoins, les personnes pouvant fournir des renseignements — selon des conditions et des mesures de protection appropriées différentes, de prévoir des garanties spécifiques sur les décisions individuelles automatisées et d'assurer une protection adéquate aux échanges de données à caractère personnel avec des pays tiers.

3.3.2. Thèmes horizontaux

La nécessité de prévenir la criminalité et de faire face à la menace terroriste ainsi que le développement progressif des volets internes et externes de l'espace de liberté, de sécurité et de justice ont fortement orienté le programme de travail des institutions communautaires et, en conséquence, celui du CEPD. Ainsi, en 2005, le CEPD a évolué dans un environnement institutionnel et juridique plus complexe, recouvrant un large éventail d'initiatives qui concernaient non seulement les politiques liées à la libre circulation des personnes (relevant du premier pilier) mais aussi les dispositions relatives à la coopération policière et judiciaire en matière pénale (troisième pilier).

Le CEPD se félicite de ce que son rôle consultatif dans le cadre des propositions législatives relevant du troisième pilier a influencé la pratique de la Commission consistant à procéder à des consultations tant formelles qu'informelles pour ses propositions relevant du troisième pilier. Il est à espérer que, dans une prochaine étape, le public ait encore davantage connaissance de la consultation du CEPD (dans le cadre du premier et du troisième pilier) s'il en est fait mention dans le préambule des propositions.

La structure à piliers du traité UE a fait naître de nouvelles questions et de nouveaux défis, découlant non seulement de la diversité des acteurs qui participent au processus décisionnel, mais aussi de chevauchements et interférences qui peuvent intervenir entre différentes bases juridiques et propositions législatives. On peut trouver des exemples éloquents de ce phénomène dans de nombreux avis du CEPD rendus en 2005. Dans les deux avis relatifs au traitement des PNR par le Canada et à la conservation des données concernant les télécommunications, le CEPD a analysé les garanties et les conditions à appliquer dans les cas où des données à caractère personnel collectées pour des finalités commerciales sont utilisées à des fins de prévention de la criminalité. Dans l'avis rendu sur la conservation des données, le CEPD devait examiner plusieurs propositions parallèles et se prononcer sur la base juridique la plus appropriée, alors que l'avis sur le SIS II portait sur un ensemble d'instruments juridiques concernant des aspects du système proposé relevant tant du premier que du troisième pilier.

Dans ce contexte, le CEPD s'est efforcé d'assurer, dans toute la mesure du possible, la cohérence des règles de protection des données dans l'ensemble de la législation européenne, en dépit de la structure à piliers et de la diversité des procédures décisionnelles et des acteurs institutionnels.

Dans le prolongement de son document stratégique, le CEPD a retenu le principe de proportionnalité comme l'un des principes directeurs essentiels de ses avis sur des propositions législatives: le traitement des données à caractère personnel n'est autorisé que dans la mesure où il est nécessaire et pour autant qu'aucun autre moyen portant moins atteinte à la vie privée n'ait la même efficacité. Cette appréciation s'est inscrite dans une perspective plus large, compte tenu de l'ensemble des différents intérêts publics en jeu, parfois contradictoires. Dans la mesure du possible, le CEPD a adopté une approche proactive, en proposant des solutions de substitution viables qui pourraient répondre aux besoins du maintien de l'ordre tout en assurant une meilleure défense du droit fondamental à la protection des données à caractère personnel. Dans son avis sur la décision-cadre relative à la protection des données dans le cadre du troisième pilier, le CEPD a montré comment, dans certains cas, une protection adéquate des données peut répondre à la fois aux besoins des personnes concernées et à ceux des autorités policières et judiciaires.

En ce qui concerne le moment de son intervention, le CEPD a, dans tous les dossiers, rendu des avis à un stade précoce du processus de décision, afin de permettre, tant aux citoyens qu'aux acteurs institutionnels concernés, de tenir dûment compte de la position qu'il exprimait. En outre, le CEPD a de plus en plus recouru à la possibilité de rendre un avis informel avant même que la proposition de la Commission ne soit adoptée.

3.4. Autres activités dans le cadre du conseil

3.4.1. Documents connexes

En 2005, le CEPD a aussi accordé plus d'attention aux documents qui précèdent les propositions formelles, tels que les communications de la Commission. Ce type de documents servant souvent de base à des choix politiques devant être pris dans le cadre de propositions législatives, le CEPD considère la possibilité d'y réagir comme une occasion importante d'exprimer ses vues sur les aspects à long terme des orientations en matière de protection des données.

Tel a été le cas avec la communication de la Commission sur la dimension externe de l'espace de liberté, de sécurité et de justice, qui établit une stratégie relative à la dimension extérieure des actions dans le domaine de la liberté, de la sécurité et de la justice. Le CEPD a défendu le point de vue selon lequel les aspects intérieurs et extérieurs sont intrinsèquement liés et a encouragé la Commission à prendre les devants pour promouvoir la protection des données à caractère personnel au niveau international en favorisant les approches bilatérales et multilatérales avec les pays tiers et la coopération avec d'autres organisations internationales.

3.4.2. Interventions devant la Cour de justice

En 2005, la Cour de justice a accordé pour la première fois au CEPD le droit d'intervenir dans deux affaires dont elle était saisie. Le Parlement demandait l'annulation de la décision du Conseil concernant la conclusion d'un accord entre la Communauté européenne et les États-Unis sur le traitement et le transfert des données des dossiers passagers (PNR) par des transporteurs aériens à l'administration américaine, ainsi que l'annulation de la décision de la Commission relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés à l'administration américaine.

Le CEPD est intervenu au soutien des conclusions du Parlement européen et a présenté des observations écrites à la Cour. Lors de l'audience de la Cour, il a défendu oralement son point de vue, dont voici les éléments essentiels:

— les décisions attaquées ne permettent pas aux compagnies aériennes européennes de respecter les obligations qui leur incombent en vertu de la directive 95/46/CE et modifient donc lesdites obligations (puisqu'un accord conclu avec un pays tiers l'emporte sur la législation interne de l'Union européenne);

— les décisions attaquées violent la protection des droits fondamentaux;

— la Commission outrepasse la marge d'appréciation prévue par l'article 25 de la directive.

Le 22 novembre 2005, l'avocat général a présenté ses conclusions, dans lesquelles il propose d'annuler les décisions — toutefois pour des motifs totalement différents de ceux que le CEPD avait exposés.

3.4.3. Mesures administratives

En 2005, le CEPD a exercé de la façon suivante sa compétence consultative en matière de mesures administratives, en particulier à propos de mesures d'application adoptées par les institutions et organes communautaires dans le domaine de la protection des données.

Le CEPD a mis au point, pour ce qui concerne en particulier les délégués à la protection des données, une approche pour les règles d'application prévues à l'article 24, paragraphe 8, du règlement. Selon lui, le champ d'application de ces règles devrait être aussi large que possible, de manière à couvrir les aspects qui touchent directement les personnes concernées, tels que le droit à l'information, l'accès, la rectification, les plaintes, etc. Le DPD d'une institution ou d'un organe doit jouer un rôle essentiel à cet égard.

Étant donné que le règlement confère au délégué à la protection des données des compétences pour examiner les faits (point 1 de l'annexe du règlement), celui-ci est bien placé pour traiter les plaintes à leur premier stade et essayer de résoudre le problème au niveau interne.

Le CEPD a eu l'occasion de donner des conseils sur les mesures d'application élaborées par la Cour des comptes, avec des résultats très satisfaisants.

Plusieurs autres questions ont été portées à son attention, lui donnant ainsi la possibilité d'exprimer son avis.

L'une d'elles portait sur l'évaluation du personnel militaire par le Conseil, bien qu'il ait été constaté que ce traitement n'entrait pas dans le champ d'application du règlement. Le CEPD a profité de l'occasion pour préciser le rôle du responsable du traitement et informer sur l'applicabilité des principes généraux en matière de protection des données.

Une autre question, reçue à la fin de l'année 2005, concernait la publication sur l'intranet de la Commission de photographies de fonctionnaires réalisées précédemment pour les badges de sécurité. Au début de janvier 2006, un avis négatif a été rendu, insistant sur la nécessité d'obtenir le consentement de la personne concernée.

Une autre question encore concernait le traitement de données à caractère personnel par la Cour des comptes dans le cadre de ses activités de vérification. Le CEPD a estimé qu'il s'agissait d'un traitement typique de données rentrant dans le champ d'application du règlement.

Quelques lignes directrices générales, dont la nécessité d'un contrôle préalable, ont été remises au délégué à la protection des données de l'OLAF à propos des mesures à prendre à l'égard de certains bénéficiaires d'opérations financées par la section «Garantie» du FEOGA ([20]).

D'autres recommandations ont été émises sous forme d'informations sur des sujets variés, tels que le traitement des données dans le contexte de visites de groupes à la Cour de justice et le droit d'accès en ce qui concerne l'évaluation des compétences de gestion au sein de la Banque centrale européenne.

Enfin, il y a lieu de noter, en ce qui concerne le rôle des DPD, que:

— à la demande du DPD de la Commission, le CEPD a conseillé qu'un DPD soit désigné dans chaque bureau interinstitutionnel. Cette idée figure dans le document de référence sur le DPD (voir point 2.2);

— plusieurs réunions bilatérales avec les DPD ont eu lieu afin de les conseiller sur diverses questions liées à leur rôle.

([20]) Fonds européen d'orientation et de garantie agricole.

3.5. Perspectives pour 2006 et au-delà

3.5.1. Nouveaux développements technologiques

La Commission européenne œuvre en faveur d'une société de l'information en Europe, fondée sur l'innovation, la créativité et l'inclusion, qui tablera sur trois grandes évolutions technologiques: une bande passante presque illimitée, une capacité de stockage infinie et un réseau de communications omniprésent. Le CEPD va décrire ici certains des nouveaux développements technologiques que ces tendances pourraient induire et qui devraient avoir une incidence majeure sur la protection des données.

La notion de données à caractère personnel et l'incidence des technologies nouvelles et émergentes

La directive 95/46/CE définit comme suit les données à caractère personnel:

«[...] toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale»

L'application de ce concept aux technologies émergentes risque de soulever de nouvelles questions du fait que la définition des données à caractère personnel comprend deux éléments importants dont le sens n'est plus évident, à savoir «concernant» et «identifiable». L'application de ces éléments est remise en question par les nouvelles formes de traitement des données, comme les services internet, et par une érosion des barrières technologiques traditionnelles (limitations de puissance, portée d'émission limitée, données isolées, etc.). En témoignent l'utilisation croissante des «marqueurs RFID» (marqueurs d'identification par radiofréquence) et le développe-

ment massif des réseaux de télécommunications, qui ont les répercussions suivantes:

— tous les objets marqués deviennent des collecteurs de données à caractère personnel;

— la «présence» de ces petits objets est, tout comme les individus qui les mettent en place, caractérisée par leur aspect «toujours connectés»;

— la cascade de données qui en résulte nourrit en permanence un énorme stock de données.

La RFID, une technologie prometteuse et contestée

En 2005, le CEPD a pris part aux travaux du Groupe de l'article 29 dans le domaine de la RFID et s'est félicité des mesures préparatoires prises par la Commission. Les marqueurs RFID nécessitent toutefois une analyse plus approfondie en raison de leur incidence préoccupante sur la protection des données à caractère personnel. Ces technologies ne sont pas seulement sensibles du fait de leur nouveau mode de collecte des données à caractère personnel, mais aussi parce que les marqueurs RFID vont constituer des éléments clés des environnements intelligents. Il importe donc que toutes les parties concernées tiennent des réunions de consultation.

L'émergence d'un environnement intelligent (intelligence ambiante)

Selon le rapport de l'Union internationale des télécommunications (UIT) ([21]), paru lors du sommet de l'ONU à Tunis, la société émergente de l'information repose sur l'«internet des objets», qui établit des ponts entre le monde numérique et le monde réel. Dans un tel environnement, le modèle de protection des données, qui suppose un responsable central du traitement, est clairement remis en cause par le développement d'une connectivité aux réseaux omniprésente.

Pendant la période de transition, alors que l'utilisateur navigue encore entre des îlots d'environnement intelligent, il est essentiel d'introduire des exigences en matière de protection de la vie privée et des données, qui feront partie intégrante de la conception de ces espaces d'intelligence ambiante. La domestication de ces technologies émergentes — et donc leur acceptation par le grand public — ne sera pas seulement fonction de l'attrait que présentent la commodité offerte par l'intelligence ambiante et les nouveaux services, mais aussi des avantages conférés par des systèmes de protection des données adaptés et cohérents qui devront être mis en place. Un des plus grands défis posés au monde de l'intelligence ambiante consistera à gérer dûment les données que ces environnements produiront en permanence.

Les systèmes de gestion des identités

Les systèmes de gestion des identités sont considérés comme des éléments clés des services émergents d'administration en ligne. Ces systèmes requerront une attention particulière dans le cadre de la protection des données. On peut y voir la conversion sous forme numérique de deux processus fondamentaux: celui de l'identification et celui de la construction d'identité. L'un et l'autre sont fondés sur l'utilisation de données à caractère personnel telles que les données biométriques. La mise en place de normes adéquates joue un rôle déterminant pour veiller à ce que ces processus respectent le cadre juridique de la protection des données, mais la définition de ces normes revêt aussi un caractère hautement stratégique dans la mesure où l'un des objectifs visés est une grande interopérabilité, qui aura des effets bénéfiques sur le principe de mobilité, un des objectifs de Lisbonne.

Les récentes initiatives des États-Unis, qui ont défini une nouvelle norme pour tous les employés et agents contractuels fédéraux, auront certainement une forte influence sur les normes internationales. L'UE doit renforcer les investissements déjà consentis dans ce domaine et lancer de nouvelles initiatives — bien sûr dans le respect des exigences en matière de protection des données. De plus, un cadre cohérent pour la protection des données a contribué à prévenir les risques de vol d'identité, menace importante pour les systèmes de gestion des identités mais maintenue jusqu'à présent à un niveau relativement faible.

L'ère de la biométrie

L'utilisation de données biométriques a fait l'objet de nombreuses propositions de la Commission européenne présentées en 2005. Ces premières initiatives vont faciliter l'adoption de la biométrie dans de nombreux autres aspects du quotidien des citoyens européens. Les institutions européennes sont donc investies d'une grande responsabilité quant à la manière dont ces technologies seront mises en place.

([21]) Rapport internet de l'UIT 2005, «The internet of things», novembre 2005, http://www.itu.int/osg/spu/publications/internetofthings

Dans son avis sur les propositions législatives concernant le système d'information Schengen de deuxième génération, le CEPD a proposé que soit établie une liste d'exigences communes et fondamentales tenant compte du caractère sensible par définition des données biométriques. Cette liste devrait pouvoir s'appliquer à tout système utilisant la biométrie, quelle que soit sa nature. Les exigences devraient être établies et définies par un groupe d'étude multidisciplinaire; il s'agirait d'aller au-delà de la définition de normes qui prévoient simplement des méthodes d'application respectant les droits des utilisateurs en matière de protection des données. À titre d'exemples, le CEPD a proposé les éléments suivants: procédure de secours, analyse d'impact ciblée, importance accordée à la procédure d'enrôlement et accent mis sur le niveau de précision.

3.5.2. Faits nouveaux dans les domaines politique et législatif

Avis et autres interventions

Au cours du dernier mois de l'année 2005, le CEPD a reçu de nouvelles demandes de conseil portant sur des propositions présentées par la Commission dans le domaine de la coopération policière et judiciaire. Il rendra ses avis au début de l'année 2006.

Une attention particulière doit être apportée à la proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité, adoptée par la Commission le 12 octobre 2005. Selon ce principe, présenté dans le programme de La Haye, les informations traitées par les autorités répressives d'un État membre dans le cadre de la lutte contre la criminalité devraient être disponibles aussi pour les autorités compétentes d'autres États membres de l'UE. Cette proposition est étroitement liée à celle qui porte sur la protection des données traitées dans le cadre du troisième pilier.

Par ailleurs, cette proposition doit être replacée dans la perspective de la tendance générale à l'augmentation des échanges de données entre les services répressifs des États membres de l'UE. En effet, des instruments juridiques parallèles ont été proposés dans des cadres différents: le traité de Prüm (appelé parfois aussi «Schengen III»), signé par sept États membres, n'en est qu'un exemple. Il est donc des plus souhaitable de disposer d'un cadre légal complet traitant de la protection des données à caractère personnel traitées dans le cadre du troisième pilier et ce, que la proposition relative au principe de disponibilité soit approuvée ou non, comme le CEPD l'a indiqué dans son avis sur la protection des données dans le cadre du troisième pilier.

Une autre tendance concerne les propositions visant à étendre les pouvoirs d'investigation des services répressifs (incluant souvent Europol), à savoir donner à ces derniers l'accès à des bases de données qui, au départ, n'ont pas été créées à des fins répressives. La Commission a adopté le 24 novembre 2005 une proposition de décision du Conseil concernant l'accès en consultation au système d'information sur les visas par les autorités compétentes en matière de sécurité intérieure et par Europol. Le CEPD a rendu un avis sur cette proposition le 24 janvier 2006. De plus, la communication de la Commission sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes propose explicitement de donner aux autorités responsables de la sécurité intérieure l'accès à d'autres grandes bases de données telles que SIS II (premier pilier) et Eurodac. Bien entendu, il s'agit d'un fait nouveau que le CEPD entend surveiller de très près, en prenant en considération la nécessité de trouver un équilibre entre les principes essentiels de la protection des données et les intérêts des autorités responsables de la sécurité intérieure.

En outre, la Commission a adopté une proposition de décision-cadre relative à l'échange d'informations extraites du casier judiciaire, destinée à établir des mesures organisationnelles régissant le stockage et l'échange entre les États membres des informations sur les personnes condamnées. La proposition devrait remplacer la «mesure d'urgence» sur laquelle le CEPD a rendu un avis le 13 janvier 2005 (voir ci-dessus).

À la fin de 2005, la DG Société de l'information et médias a entamé le réexamen du cadre réglementaire de l'UE pour les communications et les services électroniques, y compris le réexamen de la directive 2002/58/CE. Le CEPD suivra ces travaux de près et exposera ses idées sur une future réglementation dans ce domaine.

Domaines d'intérêt à moyen et à long terme

Il est clair que l'agenda du CEPD est déterminé en grande partie par le programme de travail de la Commission. Ses activités en 2006 et 2007 sont donc tributaires des changements dans les priorités établies par la Commission, qui peuvent entraîner des modifications de son propre programme de travail.

En 2005, le volet «conseil» des travaux du CEPD a été presque exclusivement centré sur l'espace de liberté, de sécurité et de justice. La plupart de ses interventions ont eu pour contexte la nécessité croissante d'échanger des informations de part et d'autre des frontières intérieures des États membres afin de lutter contre le terrorisme ou d'autres formes (graves) de criminalité ou dans le cadre de l'entrée de ressortissants de pays tiers sur le territoire de l'UE.

La communication de la Commission sur la stratégie politique annuelle pour 2006 et le programme législatif et de travail de la Commission pour 2006 fixent les priorités pour l'année 2006 et, dans une moindre mesure, pour les années suivantes. Pour le CEPD, les perspectives de prospérité et de sécurité sont les plus importantes. Dans le cadre de celles-ci, les orientations vont se modifier:

— en ce qui concerne la prospérité, le CEPD suivra de près les nouvelles initiatives liées à la mise en place de la société européenne de l'information. À court terme, c'est le réexamen du cadre réglementaire sur les communications électroniques qui retiendra son attention;

— en ce qui concerne la sécurité, d'autres priorités pourraient l'emporter au sein de l'espace de liberté, de sécurité et de justice en raison de développements technologiques comme la biométrie et des pressions grandissantes exercées sur les responsables publics et privés du traitement de données pour qu'ils accordent l'accès à celles-ci à des fins répressives. Dans ce contexte, la Commission a présenté comme une initiative essentielle le fait que les forces de police aient accès aux bases de données servant au contrôle des frontières extérieures.

D'une façon générale, d'autres domaines sont appelés à devenir de plus en plus importants, comme les communications électroniques et les données médicales.

4. Coopération

4.1. Groupe de l'article 29

Le Groupe de l'article 29, institué par l'article 29 de la directive 95/46/CE, est un organe consultatif indépendant sur la protection des données à caractère personnel agissant dans le cadre de ladite directive. Sa mission, décrite à l'article 30, peut être résumée comme suit:

— donner à la Commission européenne un avis autorisé au nom des autorités de protection des données des États membres sur les questions relatives à la protection des données;

— promouvoir l'application uniforme des principes généraux de la directive dans tous les États membres, au moyen de la coopération entre les autorités de contrôle compétentes en matière de protection des données;

— conseiller la Commission sur toute mesure communautaire ayant une incidence sur les droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel;

— émettre des recommandations destinées au grand public et, en particulier, aux institutions communautaires sur toute question concernant la protection des personnes à l'égard du traitement des données à caractère personnel dans la Communauté européenne.

Le groupe 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 organes communautaires et d'un représentant de la Commission. Cette dernière assure également son secrétariat.

Le CEPD est membre de plein droit du Groupe de l'article 29 depuis le début de 2004. Selon l'article 46, point g), du règlement (CE) n° 45/2001, il «participe aux activités du groupe». Le CEPD estime qu'il s'agit d'une enceinte très importante pour coopérer avec les autorités nationales de contrôle. Il va aussi de soi que le groupe joue un rôle central pour assurer la mise en œuvre homogène de la directive et l'interprétation de ses principes généraux: c'est une autre raison pour laquelle le CEPD participe activement à ses activités.

Conformément à l'article 46, point f), sous i), du règlement, le CEPD doit également coopérer avec les autorités nationales de contrôle dans la mesure nécessaire à l'accomplissement de leurs devoirs respectifs, notamment en échangeant toutes informations utiles et en demandant ou en donnant toute autre aide utile à l'exécution des tâches respectives. Cette coopération se met en place au cas par cas. Le CEPD participe aussi, à l'invitation de ses collègues nationaux, à des événements nationaux consacrés à des thèmes particuliers. La coopération directe avec les autorités nationales se révèle de plus en plus utile lorsqu'il est question de systèmes internationaux tels que Eurodac et le système proposé d'information sur les visas (VIS), qui nécessitent un contrôle commun effectif (voir point 2.8).

En 2005, le groupe a rendu un certain nombre d'avis sur des propositions législatives; celles-ci ont aussi fait l'objet d'un avis du CEPD, rendu sur la base de l'article 28, paragraphe 2, du règlement. Si cette dernière consultation est une étape obligatoire du processus législatif de l'UE, les avis du groupe sont bien sûr aussi extrêmement utiles, en particulier parce qu'ils peuvent attirer l'attention sur des points présentant de l'intérêt sur le plan national.

C'est pourquoi le CEPD se félicite des avis rendus par le Groupe de l'article 29, qui vont généralement

dans le même sens que les avis que lui-même a rendus peu de temps auparavant ([22]). On trouvera des exemples de cette synergie entre le Groupe de l'article 29 et le CEPD dans les avis suivants:

— avis sur la proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour [COM(2004) 835 final], adopté le 23 juin 2005 (WP 110) ([23]);

— avis sur la proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, modifiant la directive 2002/58/CE [COM(2005) 438 final], adopté le 21 octobre 2005 (WP 113);

— avis sur les propositions de règlement du Parlement européen et du Conseil [COM(2005) 236 final] et de décision du Conseil [COM(2005) 230 final] sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération, et sur une proposition de règlement du Parlement européen et du Conseil sur l'accès des services des États membres au système d'information Schengen de deuxième génération [COM(2005) 237 final], adopté le 25 novembre 2005 (WP 116).

Le CEPD a aussi contribué activement à la préparation de différents avis du groupe visant à encourager une meilleure mise en œuvre de la directive 95/46/CE ou une interprétation commune de ses dispositions essentielles. Le CEPD est convaincu que ces activités — dont on trouvera deux exemples ci-après — devraient continuer à jouer un rôle prépondérant dans le programme de travail annuel du Groupe de l'article 29:

— rapport sur l'obligation de notification aux autorités de contrôle, la meilleure utilisation des exceptions et la simplification, ainsi que sur le rôle des délégués à la protection des données à caractère personnel dans l'Union européenne, adopté le 18 janvier 2005 (WP 106);

— document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995, adopté le 25 novembre 2005 (WP 114).

Il convient de noter que les interprétations communes de la directive peuvent avoir, pour les institutions et organes communautaires, une influence directe sur l'application du règlement (CE) n° 45/2001, puisque les deux instruments sont étroitement liés: ainsi, l'article 26, paragraphe 1, de la directive et l'article 9, paragraphe 6, du règlement traitent en termes presque identiques la question des transferts vers un pays tiers. Le CEPD a donc l'intention d'utiliser ces interprétations comme plate-forme pour ses propres travaux.

Enfin, le CEPD a contribué activement à l'élaboration de documents relatifs à de nouveaux développements technologiques importants. Le document sur les questions de protection des données liées à la technologie RFID, adopté le 19 janvier 2005 (WP 105) en est un exemple illustratif. Le CEPD est aussi représenté au sein de la task-force «Internet» du groupe.

4.2. Troisième pilier

L'article 46, point f), sous ii), du règlement (CE) n° 45/2001 prévoit que le CEPD coopère avec les organes de contrôle de la protection des données institués en vertu du titre VI du traité UE (troisième pilier), en vue d'améliorer «la cohérence dans l'application des règles et procédures dont ils sont respectivement chargés d'assurer le respect». Ces organes de contrôle sont les autorités de contrôle communes (ACC) d'Europol, de Schengen, d'Eurojust et du système d'information douanier. La plupart de ces organes sont composés de représentants (en partie les mêmes) des autorités nationales de contrôle. En pratique, la coopération se fait donc avec les ACC concernées, avec l'aide du secrétariat commun à la protection des données travaillant au Conseil, et, plus généralement, avec les autorités nationales chargées de la protection des données.

La nécessité d'une coopération étroite entre les autorités nationales chargées de la protection des données et le CEPD s'est fait sentir ces dernières années, avec l'augmentation constante des initiatives prises au ni-

([22]) Voir les avis du CEPD rendus les 23 mars, 26 septembre et 19 octobre 2005.

([23]) Voir le site internet du Groupe de l'article 29: http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_fr.htm

veau européen pour lutter contre le terrorisme et la criminalité organisée, qui comprennent diverses propositions relatives à l'échange de données à caractère personnel.

En 2004, une approche structurée pour mettre au point des positions politiques sur les mesures répressives et les questions connexes a fait l'objet d'un accord. Un groupe de planification a été créé pour coordonner les activités des différents organes; le CEPD y était représenté. D'autre part, le groupe de travail «Police» a repris ses fonctions en tant qu'enceinte commune de la conférence européenne (voir aussi point 4.3). En juin 2004, les membres du groupe de planification sont convenus que le groupe «Police», au sein duquel toutes les autorités devaient être représentées, prépare:

— un document d'orientation devant être adopté à la conférence de printemps qui s'est tenue à Cracovie en 2005;

— un avis sur le futur instrument législatif sur la protection des données dans le cadre du troisième pilier;

— un avis sur la proposition suédoise de décision-cadre relative à la simplification des échanges d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne.

La réunion du groupe «Police», qui s'est tenue à La Haye le 28 janvier 2005, a produit trois documents:

— un projet de document d'orientation sur les services répressifs et l'échange d'informations dans l'UE, qui contient des propositions concrètes pour l'élaboration d'un instrument du troisième pilier relatif à la protection des données en assurant la cohérence avec les normes de protection des données figurant dans la directive 95/46/CE;

— un projet de «déclaration de Cracovie» prônant un système de protection des données traitées dans le cadre du troisième pilier qui respecte les normes de la directive et présentant le document d'orientation comme une contribution aux initiatives en cours;

— un projet d'avis sur la proposition suédoise.

Lors d'une audience publique de la commission LIBE du Parlement européen, le 31 janvier 2005, plusieurs intervenants, dont le CEPD, ont préconisé l'adoption de règles spécifiques pour le troisième pilier. Les autorités chargées de la protection des données se sont à nouveau réunies le 12 avril 2005 pour mettre au point les documents à soumettre à la conférence de printemps de Cracovie.

La conférence de printemps, qui s'est tenue du 24 au 26 avril 2005, a adopté les trois documents susmentionnés. Dans sa déclaration de Cracovie ([24]), la conférence a précisé que les «initiatives destinées à améliorer les services répressifs dans l'UE, comme le principe de disponibilité, ne devraient être introduites que sur la base d'un système approprié de protection des données, qui garantisse une norme de protection élevée et équivalente».

Le 21 juin 2005, une réunion du groupe «Police» s'est tenue à Bruxelles pour examiner les réactions reçues à la suite de la déclaration de Cracovie, du document d'orientation et de l'avis sur la proposition suédoise. De plus, les représentants de la Commission l'ont informé de l'état d'avancement des travaux sur la décision-cadre relative à la protection des données traitées dans le cadre du troisième pilier. La Commission a présenté un document de réflexion sur ce sujet. Le thème du droit d'accès à des données des services de police a aussi été abordé, à la suite des discussions qui ont eu lieu lors de la conférence de printemps ([25]).

Le 4 octobre 2005, la Commission a adopté une proposition de décision-cadre relative à la protection des données traitées dans le cadre du troisième pilier, au sujet de laquelle le CEPD a rendu un avis le 19 décembre 2005 (voir point 3.3.1).

Le groupe «Police» s'est à nouveau réuni à Bruxelles, le 18 novembre 2005, pour préparer un avis sur la proposition finale de la Commission. De l'avis général des participants, cette proposition représente un tournant important dans la protection des données et il ne faudrait pas laisser passer l'occasion d'instaurer une protection des données au sein du troisième pilier. La majeure partie de la discussion a été centrée sur le champ d'application et la base juridique de la proposition. Dans son avis sur la proposition,

([24]) Voir http://www.edps.eu.int/02_fr_legislation.htm#CECD (en anglais uniquement).

([25]) Le groupe de travail a ensuite formulé des observations sur le document de réflexion de la Commission relatif au troisième pilier, qu'il a transmises en juillet 2005 au service concerné de la Commission.

le CEPD a adopté une position ferme sur ces deux questions.

Les travaux ont aussi porté sur le projet de décision-cadre traitant du principe de disponibilité, de même que sur les résultats d'un questionnaire relatif au droit d'accès. Ce dernier a mis en évidence les différences entre les États membres quant à l'octroi d'un droit d'accès aux données des services de police. Ses conclusions confirment la nécessité d'une harmonisation, compte tenu en particulier de l'intensification des échanges de données entre les États membres.

Lors d'une réunion spéciale qui s'est déroulée à Bruxelles le 24 janvier 2006, la conférence des autorités européennes chargées de la protection des données a adopté, à propos de la proposition de décision-cadre relative à la protection des données traitées dans le cadre du troisième pilier, un avis allant largement dans le même sens que celui adopté par le CEPD le 19 décembre 2005 (voir point 3.3.1). La nécessité de nouvelles actions sera vraisemblablement examinée lors de la prochaine conférence de printemps.

SIS II

Le CEPD a aussi coopéré avec l'autorité de contrôle commune de Schengen pour élaborer l'avis sur le système d'information Schengen de deuxième génération (SIS II). Des contacts informels réguliers ont permis de coordonner au maximum les approches. Le CEPD a été très sensible au fait d'avoir été invité en tant qu'observateur à la réunion de l'ACC du 27 septembre 2005; il en a profité pour préciser sa position sur certains points. Au début de 2006, les discussions avec l'ACC ont débouché sur une approche commune quant au contrôle du SIS II, qui mérite d'être prise en compte par le Parlement européen et le Conseil lorsqu'ils statueront sur les propositions relatives au SIS II.

4.3. Conférence européenne

Les autorités chargées de la protection des données des États membres de l'UE et du Conseil de l'Europe se rencontrent annuellement lors d'une conférence de printemps pour discuter de questions d'intérêt commun et pour échanger des informations et partager leur expérience sur différents sujets. Le CEPD et son adjoint ont participé, du 24 au 26 avril 2005, à la conférence de Cracovie organisée par l'inspecteur général polonais de la protection des données.

Le CEPD a apporté une contribution particulière à la session intitulée «La directive 95/46/CE: modification ou nouvelle interprétation». Parmi les autres sujets abordés durant la conférence, citons «L'incidence de la directive 95/46/CE sur la protection des données à caractère personnel dans l'UE et les pays tiers», «L'incidence de la jurisprudence de la Cour européenne de justice des Communautés européennes sur l'application de la directive 95/46/CE», «Le transfert des données à caractère personnel vers les pays tiers — Règles contraignantes applicables aux entreprises — Les nouveaux instruments législatifs — La loi applicable», «Les responsables de la protection des données à caractère personnel», «Le droit d'accès aux données exercé par les personnes concernées — Approche pratique», «Sensibilisation et éducation» et «La protection des données à caractère personnel traitées dans le cadre du troisième pilier». Dans ce contexte, ainsi que cela a été mentionné au point 4.2, plusieurs documents importants ont été adoptés.

La prochaine conférence européenne aura lieu à Budapest les 24 et 25 avril 2006 et traitera, entre autres, de la protection des données traitées dans le cadre du troisième pilier, de la protection des données dans le cadre de recherches historiques et scientifiques et de l'efficacité des autorités chargées de la protection des données. Le CEPD présidera la session sur la protection des données traitées dans le cadre du troisième pilier.

4.4. Conférence internationale

La conférence internationale des commissaires à la protection des données et à la vie privée, venant d'Europe et d'autres parties du monde, dont le Canada, l'Amérique latine, l'Australie, la Nouvelle-Zélande, Hong Kong, le Japon et d'autres territoires de la région Asie-Pacifique, se réunit tous les ans au mois de septembre depuis plusieurs années. La 27e conférence internationale s'est tenue à Montreux (en Suisse) du 14 au 16 septembre 2005.

Le thème général était «La protection des données à caractère personnel: dans un monde globalisé, un droit universel dans le respect des diversités». Le CEPD et

son adjoint ont tous les deux assistés à la conférence, à l'issue de laquelle les autorités participantes sont convenues de promouvoir la reconnaissance du caractère universel des principes de protection des données; elles ont aussi adopté la déclaration de Montreux ([26]), qui résume ces principes et invite les diverses parties prenantes à contribuer à leur reconnaissance universelle en termes tant politiques et juridiques que pratiques. La réalisation des objectifs figurant dans la déclaration sera évaluée régulièrement.

La conférence a aussi adopté deux résolutions sur l'utilisation de la biométrie dans les passeports, cartes d'identité et documents de voyage, et sur l'utilisation de données à caractère personnel pour la communication politique. L'une et l'autre traitent de questions qui donnent actuellement lieu à des discussions délicates dans de nombreuses enceintes ([27]).

La prochaine conférence internationale, qui devait avoir lieu à Buenos Aires du 1er au 3 novembre 2006, se tiendra probablement dans un autre endroit qui sera déterminé sous peu.

4.5. Séminaire pour les organisations internationales

Le CEPD a organisé à Genève, le 15 septembre 2005, un séminaire sur la protection des données dans les organisations internationales, conjointement avec le Conseil de l'Europe, l'OCDE et les autorités de protection des données d'Autriche et de Suisse. S'y sont réunis des représentants d'une vingtaine d'organisations, dont l'ONU, Interpol, l'OIM et l'OTAN. Intitulé «La protection des données dans le cadre de la bonne gouvernance des organisations internationales», le séminaire avait pour objectif de sensibiliser les participants aux principes universels de la protection des données et à leurs conséquences pour le travail des organisations internationales.

Alors que pratiquement toutes les organisations internationales traitent des données à caractère personnel et de nombreuses données sensibles, le plus souvent dans l'intérêt et au profit des personnes concernées, les garanties sont très souvent insuffisantes. La raison en est que les organisations internationales ne sont généralement pas soumises aux droits nationaux et ne sont donc pas juridiquement liées par le vaste éventail d'instruments de protection des données qui sont applicables aux institutions publiques et aux entreprises privées dans de nombreux pays à travers le monde. Le séminaire visait à mettre ce manque en évidence afin de le combler. Il a suscité un grand intérêt chez les participants, dont un grand nombre a demandé qu'il ait une suite. Cette demande sera bien sûr prise en considération, en concertation avec les organisations internationales capables et désireuses de coopérer et de partager leur expérience dans ce domaine.

([26]) Voir http://www.edps.eu.int/02_fr_legislation.htm#international
([27]) Ibid.

5. Communication

5.1. Introduction

Avec le développement de la stratégie d'information, 2005 a apporté des améliorations importantes en ce qui concerne les communications externes du CEPD. S'appuyant sur les méthodes mises en place durant la première année de fonctionnement, la stratégie vise à structurer les communications par rapport à un objectif global et par rapport à un objectif spécifique. Pour cela, elle définit les outils de communication disponibles et établit un rapport entre les groupes cibles et les principales activités de l'institution.

L'objectif global est double:

— mieux sensibiliser à la protection des données en général;

— mieux sensibiliser aux principales activités du CEPD et des institutions.

Une meilleure sensibilisation à la protection des données en général est importante durant les premières années de l'activité d'une institution, et le CEPD a pris particulièrement soin de faire apparaître l'institution sur la scène politique. Le CEPD et son adjoint ont donc représenté l'institution à de nombreuses conférences, séminaires et cours — non seulement aux sièges des institutions et organes de l'UE, mais aussi dans un certain nombre d'États membres, tels que l'Allemagne, Chypre, l'Espagne, la France, la Lituanie, la Pologne et le Royaume-Uni. Ils se sont également rendus dans ce contexte dans des États non membres comme les États-Unis et la Suisse — respectivement pour une table ronde à haut niveau sur la confidentialité des données et dans le cadre de la conférence internationale annuelle sur la vie privée et la protection des données à caractère personnel.

Au fur et à mesure que le travail sur les dossiers progressait (contrôles préalables et conseils sur les propositions législatives par exemple), l'objectif global s'est graduellement diffusé à travers un objectif spécifique. L'objectif spécifique est un peu plus lié à un cas particulier. On peut citer les exemples de la présentation au Conseil de l'avis sur la proposition de décision-cadre relative à la protection des données dans le cadre du troisième pilier et de la présentation au Parlement européen de l'avis sur la proposition de directive relative à la conservation des données des communications électroniques.

5.2. Principales activités et groupes cibles

Dans le cadre de l'élaboration de la stratégie d'information, différents groupes cibles ont été identifiés. En liaison avec les principales activités du CEPD, ces groupes sont les suivants:

1. Contrôle: s'assurer que les administrations européennes respectent leurs exigences en termes de protection des données

a) les particuliers; personnes concernées en général, en fonction du traitement mené, et personnel des institutions et organes de l'UE en particulier. Pour ce groupe cible, ce qui compte c'est la «perspective des droits»; le droit fondamental à la protection des données et les droits spécifiques des personnes concernées (définis notamment aux articles 13 à 19 du règlement);

b) le système institutionnel: les délégués à la protection des données et coordinateurs de la protec-

tion des données dans les institutions et organes de l'UE. Pour ce groupe, ce qui compte c'est la «perspective des obligations», comme les règles générales pour garantir la légalité du traitement, les critères pour en assurer la légitimité, mais aussi l'obligation de transmettre à la personne concernée des informations sur le traitement (comme le prévoient les articles 4 à 12 du règlement).

2. Conseil: promouvoir la protection des données dans le cadre des nouvelles mesures législatives et administratives

Jusqu'ici, le CEPD a rendu des avis relatifs aux propositions de nouveaux textes législatifs dont les groupes cibles sont les acteurs politiques de l'UE. Conformément aux procédures législatives de l'UE, l'avis du CEPD sur une proposition donnée est ainsi dans un premier temps transmis à la Commission européenne (en raison du grand nombre de propositions relevant du domaine de l'application de la loi présentées en 2005, la plupart des avis concernaient la DG Justice, liberté et sécurité, même si d'autres directions générales ont été aussi concernées). Dans un deuxième temps, quand le Conseil et le Parlement européen analysent en détail la proposition, l'avis du CEPD est transmis, par exemple, au comité de l'article 36 du Conseil et à la commission LIBE du Parlement.

3. Coopération

Le CEPD coopère avec d'autres acteurs concernés relevant de ce domaine, regroupés sous la désignation «collègues de la protection de données». On peut distinguer trois niveaux de coopération: les collègues au niveau de l'Union européenne, les collègues dans un contexte européen plus large (par exemple dans le cadre de la conférence européenne sur la protection des données qui comprend aussi des États non membres de l'UE mais membres du Conseil de l'Europe), ou au niveau international (par exemple dans le cadre de la conférence internationale sur la protection des données).

Au niveau de l'UE, la coopération peut être divisée entre les travaux relevant du premier pilier (le domaine du traité CE) et les travaux relevant du troisième pilier (coopération policière et judiciaire). L'enceinte la plus importante dans le cadre du premier pilier est le Groupe de l'article 29 (voir point 4.1).

En ce qui concerne le troisième pilier, le CEPD a participé en tant qu'observateur aux travaux d'un certain nombre d'autorités de contrôle communes (voir point 4.2). Lors de l'examen des propositions relatives au SIS II par l'autorité de contrôle commune de Schengen, le CEPD a participé à ces discussions et a aussi transmis son avis au président et au secrétariat.

5.3. Outils de communication

L'année 2005 a aussi vu se développer un ensemble d'outils de communication, tels que les documents de référence, les newsletters, les communiqués de presse, etc., qui sont habituels pour de nombreux services publics. Chacun de ces outils possède ses propres caractéristiques et son propre cycle de vie, et leur utilisation peut varier en fonction du groupe cible à qui il est destiné. Les éléments les plus importants sont décrits ci-après.

5.4. Campagne d'information du CEPD

Entre le mois de mars et le mois de juillet, le CEPD a distribué deux brochures descriptives qui ont été élaborées à la fin de l'année 2004 (l'une sur l'institution et ses fonctions et l'autre sur les droits des personnes concernées). Ces brochures ont été traduites dans les vingt langues officielles de l'UE et, au total, quelque 80 000 exemplaires ont été diffusés dans l'ensemble des États membres. Les groupes cibles les ont reçus soit directement, chaque membre du personnel de l'UE ayant reçu son propre exemplaire, soit indirectement, des exemplaires étant diffusés via les relais d'information d'Europe Direct et les autorités chargées de la protection des données dans les États membres.

5.5. Service de presse

Le service de presse du CEPD a été créé juste avant le lancement du document de référence sur l'accès du public aux documents et la protection des données. Le service est géré par un attaché de presse, qui est la personne à contacter par les journalistes et qui est chargé de s'occuper des demandes d'interview, de l'organisation des conférences de presse, de la publication des communiqués de presse, etc.

S'adressant naturellement aux journalistes, le service de presse a pour objectif de promouvoir un message précis, destiné à un ou plusieurs groupes cibles. En ce sens, les médias constituent un groupe cible et, en même temps, un relais qui peut permettre la transmission du message au(x) groupe(s) cible(s) en question.

Des conférences de presse ont été organisées pour la présentation du rapport annuel en mars ainsi que pour la présentation de l'avis du CEPD sur la conservation des données en septembre 2005. Dans les deux cas, de nombreux journalistes étaient présents et la couverture par les médias a donc été importante. Un déjeuner de presse a été organisé pour la présentation du document de référence sur l'accès du public aux documents et la protection des données (voir point 2.6) et pour la présentation générale des activités et des priorités du CEPD.

5.6. Site internet

Considéré comme le principal outil de communication du CEPD, le site internet est la source d'information la plus complète sur les activités de l'institution. Il offre aussi la possibilité de relier des informations et de fournir des explications complémentaires par le biais de références croisées.

Le site internet a été créé durant le premier semestre 2004 et s'est considérablement étoffé en 2005 avec l'introduction de nouvelles rubriques et de nouveaux types de documents. En l'absence d'outils statistiques sophistiqués, il est difficile de tirer des conclusions fiables sur la fréquentation du site internet. Cependant, les impressions générales sont les suivantes:

— le nombre de visites du site a connu un bond quantitatif après les vacances d'été en août, le trafic s'étant alors stabilisé à environ 1 000 visites par semaine, contre 700 en moyenne auparavant;

— on estime le nombre moyen de pages consultées à 2 par visite (3,3 si l'on exclut les visiteurs qui ne consultent qu'une page, par exemple en utilisant un lien direct vers un document électronique particulier), ce qui traduit une faible «tendance à naviguer»;

— chaque fois que le CEPD a présenté un nouvel avis, une newsletter, un communiqué de presse ou un document similaire, le site internet a connu une nette augmentation de sa fréquentation.

Les statistiques ont en outre incité le CEPD à affecter du personnel à un projet qui débouchera sur la création d'un site internet plus convivial, de seconde génération. Ce projet de refonte a commencé à l'automne 2005 et se terminera au printemps 2006 avec le lancement du nouveau site internet.

5.7. Discours

Le CEPD a continué de consacrer des efforts et un temps considérables à l'explication de sa 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 prononcés devant différentes institutions et dans divers États membres tout au long de l'année. Le CEPD a aussi accordé un certain nombre d'interviews aux médias concernés.

Le CEPD a fait de fréquentes apparitions au sein de la commission LIBE du Parlement européen. Le 31 janvier, il a présenté son point de vue sur les questions relevant du troisième pilier lors d'un séminaire public sur le thème «La protection des données et la sécurité des citoyens». Le 30 mars, il a présenté son avis sur la proposition de règlement concernant le système d'information sur les visas (VIS) lors du séminaire public sur les frontières. Le 12 juillet, il a donné des explications sur le document de référence concernant l'accès du public aux documents et la protection des données. Le 26 septembre, il a présenté son avis sur la proposition de directive relative à la conservation des données de communications, et, le 23 novembre, celui sur les propositions concernant la seconde génération du système d'information Schengen (SIS II).

Le 21 octobre, l'avis sur le SIS II a été présenté par le Contrôleur adjoint au groupe «Acquis de Schengen» du Conseil.

Le 18 octobre, le CEPD a prononcé un discours, lors d'un symposium de la Commission sur le thème de la sécurité électronique, concernant la mise en œuvre du règlement (CE) n° 45/2001. Le 9 novembre, il a donné une conférence au Conseil sur la nécessité de la protection des données, intitulée «Is Big Brother watching?» (Est-ce que Big Brother nous regarde?). Il

a donné une conférence similaire à la Commission le 15 décembre.

En mars, le CEPD a effectué une série de discours au Canada et aux États-Unis: le 5 mars à l'université d'Ottawa, le 7 mars à la faculté de droit de l'université du Michigan, à Ann Arbor (États-Unis), et le 10 mars, lors d'une conférence de l'International Association of Privacy Professionals (association internationale des professionnels de la protection de la vie privée), à Washington DC. Le 8 juin, le CEPD a participé à une réunion des commissaires à l'information et à la protection de la vie privée à Ottawa à l'invitation du commissaire à la protection de la vie privée du Canada.

Tout au long de l'année, le CEPD s'est également rendu dans un certain nombre d'États membres. Le 7 avril, il était à Berlin, à la European Academy for Freedom of Information and Data Protection. Le 11 avril, il était aux festivités de départ du commissaire à la protection des données de Saxe-Anhalt à Magdeburg, en Allemagne. Le 18 avril, il a donné une conférence à l'université de Leyde, aux Pays Bas. Le 25 avril, il s'est exprimé lors de la conférence européenne qui s'est tenue à Cracovie, en Pologne. Le 2 juin, il a participé à la conférence nordique de Trondheim dans le cadre de discussions avec ses collègues scandinaves. Le 23 juin, il a présenté un discours sur la protection des données et la sécurité dans l'Union européenne lors du quatorzième forum de la protection des données à Wiesbaden.

Le 13 octobre, le CEPD était à l'université de Tilburg, aux Pays Bas. Le 21 octobre, il était présent à la conférence «Biométrie 2005» à Londres. Le 2 novembre, il a fait un discours à Limassol, à Chypre. Le 8 novembre, il a participé à un séminaire au Sénat français à Paris. Le 14 novembre, il est intervenu dans le cadre d'une conférence sur le commerce électronique à Vilnius, en Lituanie. Le 29 novembre, il a participé à une conférence à Manchester, et, le 30 novembre, il était à un séminaire sur le thème «La directive 95/46/CE: dix ans après» au British Institute of International and Comparative Law à Londres.

Le Contrôleur adjoint a effectué des présentations similaires à Madrid et à Barcelone, entre autres pour le réseau judiciaire européen, sur le thème de la protection des données dans le cadre du troisième pilier.

5.8. Newsletter

Un premier numéro de la newsletter du CEPD a été envoyé à un certain nombre de personnes qui étaient considérées comme des destinataires pertinents, par exemple des journalistes et des personnes travaillant dans le domaine de la protection des données. La newsletter vise à attirer l'attention sur les activités récentes et à promouvoir les documents disponibles en ligne sur le site internet. Trois numéros ont été publiés au cours du second semestre de 2005 et au moins quatre numéros par an sont prévus.

La possibilité de s'abonner à la newsletter ([28]) a été créée à la fin du mois d'octobre et quelque 250 personnes l'ont fait dans les deux mois qui ont suivi, dont des membres du Parlement européen, du personnel de l'UE et des autorités nationales chargées de la protection des données.

5.9. Information

En 2005, le CEPD a reçu plus de 100 demandes par courrier électronique, transmises pour la plupart par des particuliers, mais aussi par des juristes, des étudiants, etc., sollicitant des informations et/ou des conseils relatifs à la protection des données en Europe. Considérant que ces demandes sont une bonne occasion de fournir un service, le CEPD a pour objectif de communiquer une réponse personnalisée dans un délai de quelques jours ouvrables — et il y parvient la plupart du temps. Ces demandes peuvent être divisées en deux catégories principales — les demandes de conseil et les demandes d'information, bien que certaines d'entre elles contiennent naturellement des éléments des deux catégories à la fois.

Plus de 30 demandes de conseil ont été traitées, allant de questions précises sur l'interprétation d'un article donné ou d'un élément particulier de la législation de l'UE sur la protection des données jusqu'aux questions sur les différences qui existent entre les principes généraux de la protection des données dans l'Union européenne et aux États-Unis, en passant par ce qu'il y a lieu de faire figurer dans une déclaration relative à la protection de la vie privée sur le site internet d'une institution de l'Union européenne.

([28]) http://www.edps.eu.int/publications/newsletter_fr.htm

Le CEPD a aussi traité près de 70 demandes d'information, une catégorie très vaste qui comprend, entre autres, des questions générales sur les politiques de l'UE, des questions relatives aux nouveaux textes législatifs et à la protection des données qui font l'objet d'un débat public et, enfin, des questions concernant la situation dans un État membre en particulier. Ce nombre de demandes pour le moment assez faible a permis de fournir des réponses un peu plus personnalisées qui soulignent les aspects importants et qui informent aussi, par exemple, sur les documents liés à ces sujets adoptés par le Groupe de l'article 29.

La majorité des demandes reçues étaient formulées en anglais ou en français, mais un nombre important de demandes l'étaient aussi dans les «anciennes» et les «nouvelles» langues. Dans les cas où cela était nécessaire, les réponses du CEPD ont été traduites, afin d'apporter des informations appropriées dans la langue maternelle de la personne ayant contacté le CEPD. Les demandes ont aussi été utilisées comme base pour constituer une rubrique FAQ (questions le plus souvent posées), qui sera ajoutée au site internet en 2006.

5.10. Logo et charte graphique

Un projet visant à créer un nouveau logo accompagné d'une nouvelle charte graphique a été lancé en octobre. Les travaux étaient au départ axés sur le développement d'un logo qui aurait un rapport clair avec les institutions de l'UE mais se distinguerait quand même par son individualité, tout en ayant un lien visuel clair avec les principales responsabilités du CEPD. Le nouveau logo a été progressivement lancé depuis sa finalisation à la mi-décembre 2005.

Le nouveau logo est conçu à partir des couleurs jaune et bleu du drapeau de l'Union européenne et prend la forme d'un disque en mouvement qui enregistre des données et qui évoque également un bouclier de protection pour les données. Les pixels d'information dessinent une ellipse et passent de la forme d'une personne à celle des étoiles européennes.

Le développement de la charte graphique se poursuivra pendant les premiers mois de l'année 2006 pour donner naissance à une identité visuelle entièrement remaniée qui sera utilisée dans l'ensemble de la vaste palette d'outils de communication, tels que les courriers, les avis, les documents, la newsletter et le site internet.

5.11. Visites

Dans le cadre des travaux visant à améliorer la visibilité du CEPD, deux groupes d'étudiants spécialisés en affaires européennes ont été accueillis. Ces visites ont été très appréciées et le nouveau site internet attirera plus l'attention sur cette possibilité.

6. Administration, budget et personnel

6.1. Introduction: poursuite de la mise en place de la nouvelle institution

La mise en place de la nouvelle institution qu'est le CEPD s'est poursuivie sur les bases de 2004, en vue de consolider le bon démarrage de l'institution. En 2005, le CEPD a pu disposer de ressources supplémentaires au niveau tant de son budget (qui est passé de 1 942 279 euros à 2 879 305 euros) que de son personnel. À cet égard, deux nouveaux programmes ont été lancés, qui ont permis le recrutement de stagiaires et d'experts nationaux.

La coopération avec les institutions signataires de l'accord de coopération administrative (Parlement européen, Conseil, Commission européenne) signé le 24 juin 2004 s'est encore améliorée et a été étendue à de nouveaux services, ce qui a permis des économies d'échelle appréciables. Le ralentissement de certaines tâches, lié au principe d'assistance partagée (Commission-Parlement européen), a été constaté, mais, grâce à l'aide du personnel des institutions concernées, cet aspect devrait être réglé en 2006. Le CEPD a pleinement pris en charge certaines tâches qui étaient initialement accomplies par d'autres institutions (comme l'achat de mobilier par exemple).

La mise en place de l'environnement administratif se poursuit progressivement en procédant par priorités, en tenant compte des besoins et de la taille de l'institution. Le CEPD a adopté différentes règles internes nécessaires au bon fonctionnement de l'institution, notamment un système de normes pour le contrôle interne et des dispositions d'application du statut.

Les locaux initialement mis à la disposition du CEPD sont à présent insuffisants et des démarches ont été entreprises auprès du Parlement européen pour obtenir des locaux plus grands.

6.2. Budget

Un budget prévisionnel pour l'année 2005 a été établi en mars 2004, au moment où le CEPD commençait tout juste à se mettre en place, grâce au soutien des services du Parlement européen. Le budget adopté par l'autorité budgétaire pour 2005 s'élevait à 2 879 305 euros, soit une augmentation de 48,8 % par rapport au budget 2004 (calculé sur onze mois). Il a été calculé sur la base des paramètres définis par la Commission et des orientations générales de l'autorité budgétaire. Un budget rectificatif a été adopté à la suite de la décision de l'autorité budgétaire d'adapter les salaires et les pensions pour 2005; ces données ont été calculées avec l'aide de la Commission. Selon le budget rectificatif n° 2 de l'Union européenne arrêté pour l'exercice 2005 le 13 juillet 2005, le budget du CEPD pour 2005 s'élève à 2 840 733 euros.

Une nouvelle ligne budgétaire a été créée, sans incidence financière. Cette ligne, qui n'avait pas été prévue auparavant, permet de couvrir, en cas de nécessité, les prestations exécutées par des personnes qui n'ont pas de lien avec les institutions, y compris le personnel intérimaire.

Compte tenu de la taille réduite des services du CEPD, rendant peu judicieux l'établissement de règles internes qui lui soient spécifiques, le CEPD a décidé d'appliquer les règles internes de la Commission sur l'exécution du budget, dans la mesure où celles-ci sont applicables à la structure de son budget et à la taille de l'institution du CEPD, et dans la mesure où des règles spécifiques n'ont pas été définies.

L'assistance de la Commission s'est poursuivie, en particulier dans le domaine de la comptabilité, le comptable de la Commission ayant également été désigné comptable du CEPD.

Dans son rapport concernant l'exercice 2004, la Cour des comptes a indiqué que l'audit ne donnait lieu à aucune observation.

6.3. Ressources humaines

Le CEPD bénéficie de l'aide très efficace des services de la Commission qui fournit une assistance pour les tâches liées à la gestion des personnes de l'institution (à savoir les deux membres nommés et le personnel).

6.3.1. Recrutement

En tant que nouvelle institution, le CEPD est et sera dans les années qui viennent en phase de construction; le CEPD prend sa place dans l'environnement communautaire, et sa visibilité croissante a pour effet un accroissement des tâches; l'augmentation sensible en 2005 du nombre de dossiers traités et des tâches a été présentée dans les chapitres précédents; les ressources humaines jouent bien évidemment un rôle fondamental pour soutenir ce processus.

Le choix du Contrôleur est néanmoins de limiter dans un premier temps cet accroissement des tâches et du personnel par une progression contrôlée permettant d'assurer une intégration des nouvelles matières traitées ainsi que l'insertion et la formation des nouveaux collègues. Le CEPD a donc demandé la création de seulement quatre postes en 2005 (deux A, un B, un C); cette demande ayant été autorisée par l'autorité budgétaire, le tableau des effectifs est passé de quinze personnes en 2004 à dix-neuf en 2005. Les avis de vacance ont été publiés en février, et quatre nouveaux collègues ont été recrutés. Les recrutements sont effectués conformément aux règles en vigueur dans les institutions: priorité est donnée aux transferts entre institutions; ensuite, consultation des listes de réserve et, enfin, recours à du personnel extérieur. Parmi les nouveaux collègues recrutés, deux ont le statut de fonctionnaire et deux sont agents temporaires.

L'aide de la Commission dans ce domaine est précieuse, particulièrement celle de l'Office «Gestion et liquidation des droits individuels» (PMO) (fixation des droits, paiement des salaires, calcul et paiement des indemnités et contributions diverses, missions et déplacements...) ainsi que celle du service médical. Certains aspects de la procédure de recrutement sont à présent entièrement traités par le CEPD, à savoir la gestion des candidatures et l'accès aux listes de l'Office européen de sélection du personnel, l'organisation des entretiens, la préparation des dossiers de recrutement pour les personnes retenues, la création du dossier avec toutes les pièces justificatives et sa transmission au PMO pour la fixation des droits. Il convient de souligner ici la très bonne collaboration avec d'autres institutions, en particulier avec le Comité des régions et le Médiateur, qui a permis l'échange d'informations et de bonnes pratiques dans ce domaine.

Le CEPD a accès aux services de l'Office européen de sélection du personnel et participe aux travaux du conseil d'administration en tant qu'observateur pour le moment. Des négociations en vue de sa pleine participation ont été lancées.

6.3.2. Programme de stages

Une des réalisations importantes de 2005 a été la création d'un programme de stages, mis en place par la décision du 27 mai 2005, publiée sur le site internet. Cette décision est similaire à celles des autres institutions européennes, en particulier celle de la Commission, qui a été adaptée pour être compatible avec la taille et les besoins du CEPD.

Le principal objectif de ce programme est d'offrir aux jeunes diplômés des universités la possibilité de mettre en pratique les connaissances acquises durant leurs études, en particulier dans leur domaine de compétences spécifique, et d'acquérir ainsi une expérience pratique des activités quotidiennes du CEPD. En conséquence, le CEPD va améliorer sa visibilité auprès des jeunes citoyens de l'UE, en particulier auprès des étudiants des universités et des jeunes diplômés spécialisés dans des domaines intéressant le CEPD. Outre le programme de stages principal, des dispositions spéciales ont été prévues pour accepter des étudiants des universités et des étudiants en doctorat pour des stages de courte durée non rémunérés. Cette seconde partie du programme

donne aux jeunes étudiants la possibilité de mener des recherches dans le cadre de leur thèse, selon des critères d'admission spécifiques restrictifs, conformément au processus de Bologne et à l'obligation qu'ont les étudiants des universités d'effectuer un stage dans le cadre de leurs études.

Le programme principal prévoit l'accueil de deux à trois stagiaires par session, avec deux sessions de cinq mois par an. La première session du programme a commencé en octobre 2005 et s'est terminée en février 2006.

Expérience et ressources sont nécessaires à l'organisation concrète d'un programme de stages. Le CEPD reçoit une assistance administrative de la part du bureau des stages de la direction générale de l'éducation et de la culture, qui gère tous les programmes de stages pour la Commission. Un accord au niveau des services a été conclu entre les deux parties afin de préciser les modalités de cette assistance. En outre, le CEPD coopère avec les bureaux des stages d'autres institutions européennes, dont le Conseil, le Comité des régions et le Comité économique et social européen, en particulier dans le cadre de l'organisation de visites.

Les résultats des trois premiers mois de stage des trois premiers stagiaires du CEPD sont très positifs. Le niveau des stagiaires sélectionnés était élevé; durant le processus de sélection, les compétences et les parcours des candidats ont été soigneusement évalués, une attention particulière étant accordée à la spécialisation dans le domaine de la protection des données. Les stagiaires ont contribué à la fois au travail théorique et pratique, acquérant ainsi une expérience directe et une formation sur le tas concernant les questions relatives à la protection des données, ainsi qu'une connaissance concrète des institutions européennes.

6.3.3. Programme pour les experts nationaux détachés

Par sa décision du 10 novembre 2005, le CEPD a adopté des dispositions relatives au régime applicable aux experts nationaux détachés auprès de ses services.

Le détachement d'experts nationaux permet au CEPD de bénéficier de leurs connaissances et de leur expérience professionnelle, notamment dans le domaine de la protection des données, où l'expertise requise n'est pas toujours disponible dans l'immédiat dans les différentes langues. Ce programme permet également aux experts nationaux de se familiariser avec les connaissances et pratiques européennes dans ce domaine. Simultanément, le CEPD accroît sa visibilité sur le terrain au niveau opérationnel.

La décision du CEPD relative aux experts nationaux détachés est fondée sur la décision correspondante de la Commission. Toutefois, certaines modifications ont été apportées au processus de recrutement pour tenir compte de la taille des services du CEPD et des compétences spécifiques nécessaires pour travailler dans le domaine de la protection des données. Le CEPD a pour politique de recruter les experts nationaux détachés dans le cadre de contacts officiels avec les États membres, en s'adressant directement aux autorités nationales de protection des données (APD). Les représentations permanentes nationales sont informées du programme et sont invitées à coopérer à la recherche de candidats correspondant au profil recherché. Concrètement, le CEPD transmet une lettre aux APD les invitant à participer au programme, et les employeurs intéressés soumettent une proposition au CEPD.

Il y a lieu de mentionner en particulier la DG Personnel et administration de la Commission, qui fournit une aide administrative pour l'organisation de ce programme.

6.3.4. Organigramme

L'organigramme des services du CEPD est resté sensiblement le même depuis 2004: une unité, composée de cinq personnes, est chargée de l'administration, du personnel et du budget; le reste de l'équipe, chargé des tâches opérationnelles liées à la protection des données et composé de quatorze personnes, travaille directement sous la direction du Contrôleur et du Contrôleur adjoint. Une certaine souplesse a été maintenue dans l'attribution des tâches au personnel, dans la mesure où celles-ci sont encore en évolution.

6.3.5. Formation

Le personnel du CEPD a accès aux cours organisés par la Commission en ce qui concerne la formation générale et linguistique et aux cours organisés par l'École européenne d'administration (EAS). Un ac-

cord a été signé avec l'EAS, définissant les conditions d'accès pour le personnel du CEPD aux formations dispensées par l'école. Le CEPD a pour le moment le statut d'observateur au conseil d'administration; il a entamé des consultations des membres fondateurs de l'école en vue de sa participation en qualité de membre, aux mêmes conditions que les institutions fondatrices.

6.4. Consolidation de la coopération

6.4.1. Suivi de l'accord de coopération administrative

En 2005, la coopération interinstitutionnelle s'est poursuivie dans les domaines où le CEPD est assisté par les autres institutions en vertu de l'**accord de coopération administrative** conclu avec les secrétaires généraux de la Commission, du Parlement européen et du Conseil le 24 juin 2004. Il convient de rappeler qu'une telle coopération représente une valeur ajoutée non négligeable pour le CEPD, car elle permet, d'une part, d'avoir recours à l'expertise des autres institutions dans les domaines d'assistance, et, d'autre part, de réaliser des économies d'échelle.

La coopération s'est poursuivie avec différents services de la Commission (principalement la DG Personnel et administration, la DG Budget, l'Office «Gestion et liquidation des droits individuels», mais aussi la DG Éducation et culture et la DG Emploi, affaires sociales et égalité des chances), du Parlement européen (informatique, notamment l'aide à la mise en place du nouveau site internet; aménagement des surfaces occupées; sécurité des bâtiments; imprimerie; courrier; téléphonie; fournitures, etc.) et du Conseil (traductions).

Afin de faciliter la coopération entre les services de la Commission et le CEPD, l'accès direct, depuis les locaux du CEPD, aux principaux logiciels de gestion des ressources humaines et financières de la Commission (SIC, Syslog, SI2, ABAC...) a été demandé. Cet accès direct devrait permettre un meilleur échange d'informations et une gestion plus efficace et plus rapide des dossiers tant par le CEPD que par la Commission. Cet accès a été possible pour SI2 et partiellement pour Syslog, mais pas encore pour les autres logiciels. En effet, des difficultés liées aux différents environnements informatiques des institutions qui fournissent une assistance au CEPD dans ces domaines ont ralenti ce processus. Le CEPD espère qu'il sera complètement opérationnel au cours de 2006.

Des **accords au niveau des services** (voir liste à l'annexe H) ont été signés avec les différentes institutions et leurs services. Il s'agit notamment de:

— l'accord avec le Conseil, qui fournit une assistance remarquable au CEPD, tant par la rapidité que par la qualité des travaux, dans le domaine de la traduction. Parallèlement à l'augmentation de la visibilité du CEPD, le nombre de documents à traduire a augmenté. Le CEPD s'efforce toutefois de limiter, dans la mesure du possible, le nombre de traductions demandées;

— l'accord avec le bureau des stages de la Commission (DG Éducation et culture), qui a permis le lancement du premier programme de stages du CEPD en 2005;

— l'accord avec la DG Emploi, affaires sociales et égalité des chances de la Commission, afin d'apporter au CEPD l'assistance technique nécessaire à la réalisation d'un stand portable et d'autres services complémentaires pour le CEPD (élaboration d'un logo; nouvelle présentation du site internet...).

6.4.2. Coopération interinstitutionnelle

Le CEPD a engagé des pourparlers avec l'Agence européenne chargée de la sécurité des réseaux et de l'information en vue de conclure un accord d'assistance administrative. Cet accord définira les modalités d'exécution de l'audit de sécurité de la base de données Eurodac et les conditions de déroulement de cette coopération (voir point 2.8).

La participation à l'appel d'offres interinstitutionnel pour le mobilier a représenté pour le CEPD une première étape vers une certaine autonomie en ce qui concerne l'équipement de ses bureaux. L'appel d'offres avait pour objet la conclusion de différents contrats-cadres portant sur la fourniture du mobilier.

En tant que nouvelle institution, le CEPD est invité à participer aux travaux de différents comités et organes interinstitutionnels; en raison de sa taille, cette participation a toutefois dû être limitée, en 2005, à certains d'entre eux. Cette participation a permis

d'accroître la visibilité du CEPD auprès des autres institutions et a favorisé l'échange continu d'informations et de bonnes pratiques.

6.4.3. Relations extérieures

Le processus consistant à faire reconnaître l'institution auprès des autorités belges a été mené à bien, ce qui a permis au CEPD et à son personnel de bénéficier des privilèges et immunités prévus par le protocole sur les privilèges et immunités des Communautés européennes.

6.5. Infrastructure

L'infrastructure générale s'est améliorée durant l'année 2005. Toutefois, avec l'augmentation des effectifs et leur nouvelle augmentation prévue en 2006, le CEPD est confronté à un problème de place, que l'on espère résoudre par l'acquisition d'espace supplémentaire en 2006.

La sécurité du sixième étage du nº 63 de la rue Montoyer a revêtu la plus haute importance, compte tenu de la sensibilité des données traitées par le CEPD.

Sur la base de l'accord de coopération administrative, dans le cadre duquel les services du Parlement européen assistent le CEPD en ce qui concerne les facilités matérielles, un premier mobilier a été fourni par le Parlement en 2004. Cette assistance s'est achevée en 2005.

6.6. Environnement administratif

6.6.1. Mise en place de normes de contrôle interne

Sur la base de l'accord interinstitutionnel du 24 juin 2004, l'auditeur interne de la Commission a été nommé auditeur du CEPD.

Par sa décision du 7 novembre 2005 et en conformité avec l'article 60, paragraphe 4, du règlement financier du 25 juin 2002, le Contrôleur européen a décidé de mettre en place des procédures de contrôle interne propres au CEPD.

En raison de la structure et de la taille de l'institution ainsi que de ses activités, le CEPD a adopté des normes adaptées aux besoins de l'institution et aux risques associés à l'exercice de ses activités, avec la possibilité de les réviser annuellement pour tenir compte de l'évolution des activités. Ces normes portent surtout sur l'organisation générale de l'institution, compte tenu de sa taille et de la nature du budget à gérer qui porte principalement sur le fonctionnement administratif de l'institution, et compte tenu également de la simplicité des circuits financiers mis en place pour la gestion financière.

6.6.2. Constitution du comité du personnel ad interim au sein des services du CEPD

Un **comité du personnel ad interim** a été constitué en 2005. Il a été consulté sur une première série de dispositions générales d'application du statut et sur d'autres règles internes adoptées par l'institution (par exemple l'horaire flexible).

Conformément à l'article 9 du statut des fonctionnaires des Communautés européennes, le Contrôleur européen a adopté, le 8 février 2006, une décision instituant un comité du personnel au sein des services du CEPD. Les élections en vue de la constitution d'un **comité du personnel définitif** auront lieu en mars 2006. En attendant, des règles simples de fonctionnement et d'organisation du comité ont été adoptées par le personnel réuni en assemblée générale.

6.6.3. Horaire flexible

En tant que nouvelle institution et dans l'esprit de la réforme du statut, le CEPD a souhaité offrir à son personnel des conditions de travail modernes, comme l'horaire flexible. L'horaire flexible n'est pas une obligation statutaire; il s'agit plutôt d'une mesure d'organisation du temps de travail visant à permettre au personnel de concilier vie professionnelle et vie privée et au CEPD d'organiser le temps de travail en fonction de ses priorités. Tout membre du personnel a la possibilité de choisir entre l'horaire normal et l'horaire flexible, la possibilité de récupérer les heures supplémentaires prestées étant prévue.

6.6.4. Règles internes

Un premier ensemble de règles internes nécessaires au bon fonctionnement de l'institution et de dispositions générales d'application du statut a été adopté (voir annexe H). Lorsque ces dispositions concernent des matières pour lesquelles le CEPD bénéficie de l'assistance de la Commission, elles sont semblables à celles de la Commission, moyennant quelques adaptations liées à la spécificité du CEPD. Dans certains cas, certains accords ont dû être complétés (par exemple, il a fallu prévoir un avenant, pour le CEPD, au contrat d'assurance accident de la Commission visant à couvrir les experts nationaux détachés). Les règles internes sont transmises, pour information, aux nouveaux collègues dès leur arrivée.

6.7. Objectifs pour 2006

Les objectifs prévus pour 2005 ayant été atteints, le CEPD peut envisager le passage à une nouvelle étape visant, d'une part, à consolider l'acquis et, d'autre part, à développer certaines activités. Cette évolution est possible grâce à l'accord donné par l'autorité budgétaire au recrutement de cinq nouveaux collègues en 2006 et à l'adoption d'un budget de 3 447 233 euros.

La poursuite de la coopération administrative restera néanmoins un facteur essentiel du développement du CEPD; en effet, la taille de l'institution ne lui permet pas encore d'assumer les différentes tâches actuellement effectuées par la Commission, le Parlement européen et le Conseil pour le CEPD. C'est la raison pour laquelle le Contrôleur se propose de demander la prolongation de l'accord de coopération administrative qui vient à échéance à la fin de 2006.

2006 verra la création d'une fonction interne de protection des données, et un délégué à la protection des données sera nommé au sein de l'institution.

Les indicateurs de performance adoptés en 2005 seront pleinement mis en œuvre, et le CEPD poursuivra le développement de son environnement administratif; une attention particulière sera accordée au développement d'activités sociales.

Les négociations actuellement en cours pour obtenir des espaces de bureaux supplémentaires devraient aboutir au premier semestre 2006 à une nouvelle phase d'installation.

Annexe A

Extraits du règlement (CE) nº 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), 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 B

Liste des abréviations

ACC	autorité de contrôle commune
API	informations anticipées sur les voyageurs
CdT	Centre de traduction des organes de l'Union européenne
CE	Communautés européennes
CEDH	convention européenne des droits de l'homme
CPD	coordinateur de la protection des données
CS-VIS	système central d'information sur les visas
DPD	délégué à la protection des données
EAS	École européenne d'administration
ENISA	Agence européenne chargée de la sécurité des réseaux et de l'information
EUMC	Observatoire européen des phénomènes racistes et xénophobes
FEOGA	Fonds européen d'orientation et de garantie agricole
LIBE	commission des libertés civiles, de la justice et des affaires intérieures (du Parlement européen)
NI-VIS	interface nationale du système d'information sur les visas
OCDE	Organisation de coopération et de développement économiques
OHMI	Office de l'harmonisation dans le marché intérieur (marques, dessins et modèles)
OIM	Organisation internationale pour les migrations
OLAF	Office européen de lutte antifraude
ONU	Organisation des Nations unies
OTAN	Organisation du traité de l'Atlantique Nord
PNR/DP	passenger name record/dossiers passagers
REC	rapport d'évolution de carrière
RFID	identification par radiofréquence
SIS	système d'information Schengen
UE	Union européenne
UIT	Union internationale des télécommunications
VIS	système d'information sur les visas

Annexe C

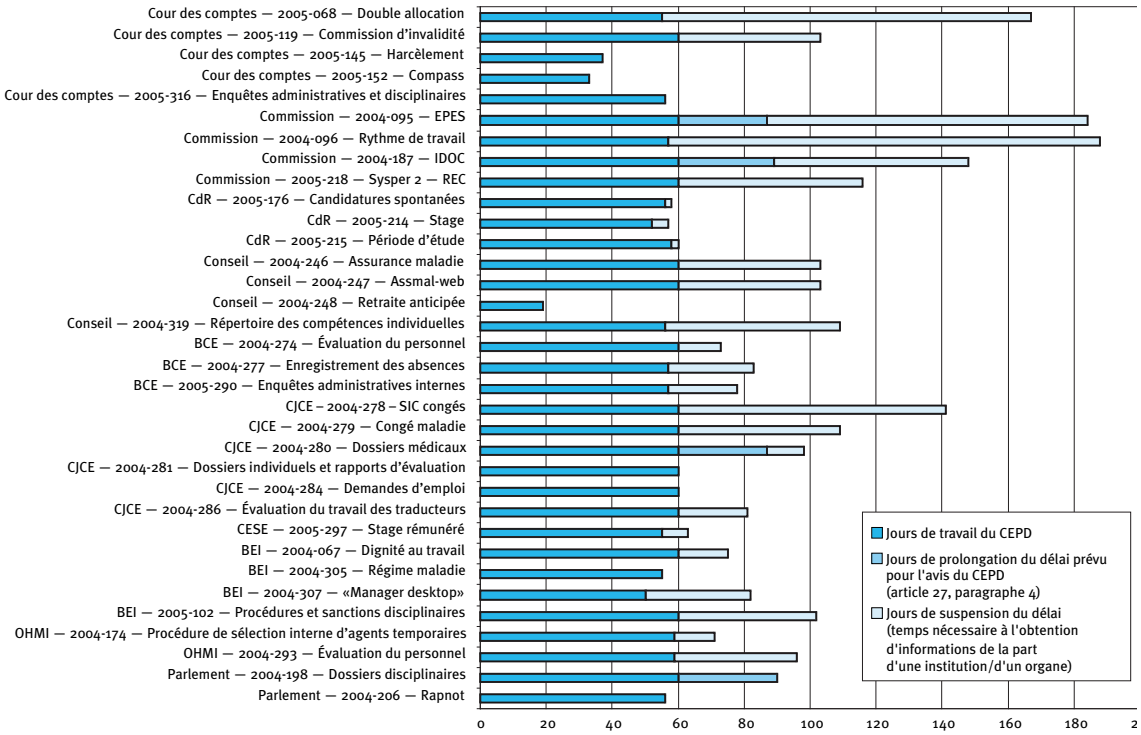
Liste des délégués à la protection des données

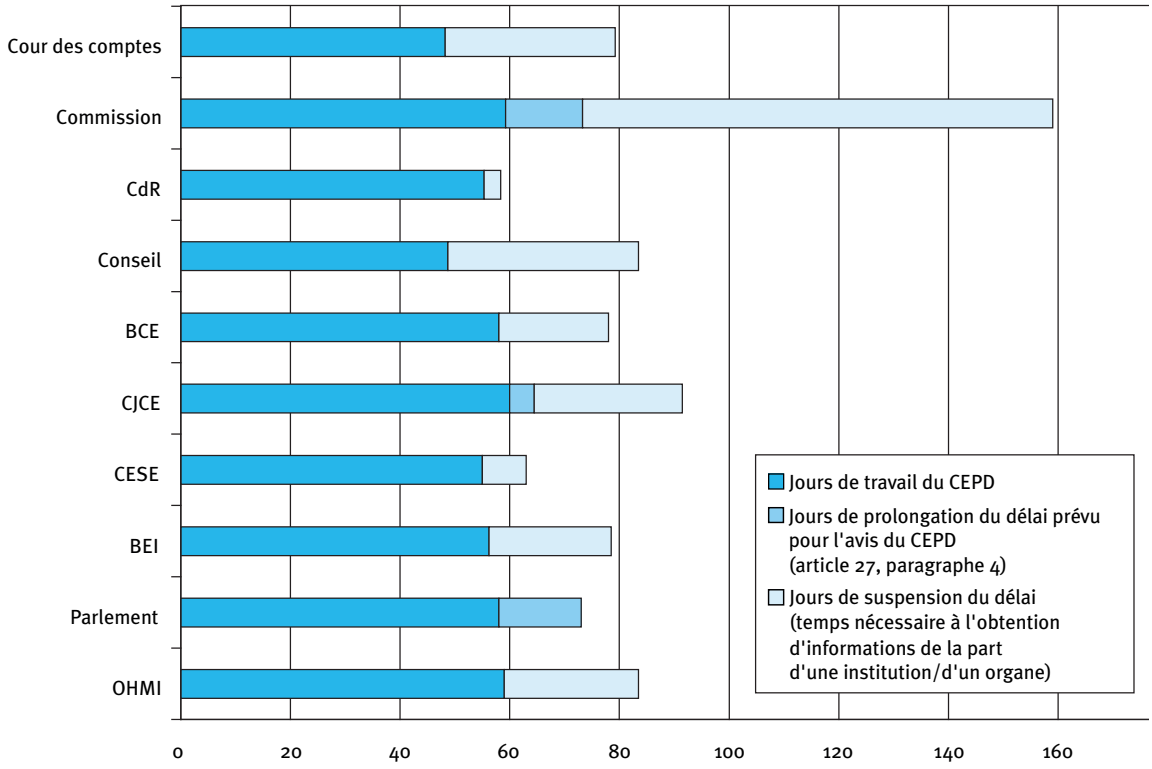
Organisation	Nom	E-mail
Parlement européen	Jonathan STEELE	DG5Data-Protection@europarl.eu.int
Conseil de l'Union européenne	Pierre VERNHES	data.protection@consilium.eu.int
Commission européenne	Nico HILBERT *(faisant office de délégué à la protection des données)*	Data-Protection-Officer@cec.eu.int
Cour de justice des Communautés européennes	Marc SCHAUSS	DataProtectionOfficer@curia.eu.int
Cour des comptes européenne	Jan KILB	data-protection@eca.eu.int
Comité économique et social européen	Elena FIERRO	data.protection@esc.eu.int
Comité des régions	Petra CANDELLIER	data.protection@cor.eu.int
Banque européenne d'investissement	Jean-Philippe MINNAERT	DataProtectionOfficer@eib.org
Banque centrale européenne	Wolfgang SOMMERFELD	dpo@ecb.int
Médiateur européen	Loïc JULIEN	dpo-euro-ombudsman@europarl.eu.int
Office européen de lutte antifraude	Laraine L. LAUDATI	laraine.laudati@cec.eu.int
Centre de traduction des organes de l'Union européenne	Benoît VITALE	data-protection@cdt.eu.int
Office de l'harmonisation dans le marché intérieur (marques, dessins et modèles)	*(à désigner)*	DataProtectionOfficer@oami.eu.int
Observatoire européen des phénomènes racistes et xénophobes	Niraj NATHWANI	Niraj.Nathwani@eumc.eu.int
Agence européenne des médicaments	Vincenzo SALVATORE	data.protection@emea.eu.int
Office communautaire des variétés végétales	Martin EKVAD	ekvad@cpvo.eu.int
Fondation européenne pour la formation	Romuald DELLI PAOLI	DataProtectionOfficer@etf.eu.int
Agence européenne chargée de la sécurité des réseaux et de l'information	Andreas MITRAKAS	dataprotection@enisa.eu.int
Fondation européenne pour l'amélioration des conditions de vie et de travail	*(à désigner)*	dataprotectionofficer@eurofound.eu.int
Observatoire européen des drogues et des toxicomanies	Arne TVEDT	arne.tvedt@emcdda.eu.int
Autorité européenne de sécurité des aliments	Claus REUNIS	claus.reunis@efsa.eu.int

Annexe D

Délais de traitement des contrôles préalables par dossier et par institution

Les deux graphiques suivants illustrent le travail du CEPD et des institutions et organes en détaillant le temps de travail consacré au traitement des dossiers de contrôle préalable. Le premier graphique présente en détail chaque dossier de contrôle préalable traité en 2005, le second résume les cas par institution et organe.





Les graphiques indiquent le nombre de jours de travail du CEPD, le nombre de jours de prolongation nécessaires au CEPD et le nombre de jours de suspension (temps nécessaire à l'obtention d'informations de la part des institutions ou organes) ([1]). On peut en tirer les conclusions suivantes:

— Nombre de jours de travail du CEPD par contrôle préalable

  Le nombre de jours de travail du CEPD est en moyenne de 55,5 jours par dossier, ce qui peut être considéré comme satisfaisant dans la mesure où c'est moins que le délai de deux mois stipulé.

— Nombre de jours de travail dans le cadre d'une prolongation du délai prévu pour l'avis du CEPD

  Pour 4 des 34 dossiers de contrôle préalable (12 %), un délai supplémentaire a été demandé au titre de l'article 27, paragraphe 4. Ce délai supplémentaire n'a jamais dépassé un mois et atteint en moyenne 28,5 jours pour ces 4 dossiers.

— Nombre de jours écoulés dans le cas d'une suspension du délai prévu

  Il s'agit du délai nécessaire à la réception d'informations complémentaires demandées par le CEPD aux institutions ou organes. En moyenne, le délai a été de 30 jours.

  Ce nombre n'est pas très représentatif car il recouvre des écarts considérables: par exemple, le délai le plus court a été de 2 jours, le plus long de 131 jours. Idéalement, l'institution ou l'organe devrait fournir l'information dans un délai inférieur à deux mois. En moyenne, les graphiques montrent clairement qu'il faut parfois disposer d'un long délai pour répondre aux questions du CEPD. Il peut y avoir plusieurs raisons à cela. La première tient à la complexité du dossier. Il existe une certaine relation entre le temps dont doit disposer le CEPD (notamment lorsqu'une prolongation du délai a été accordée) et le temps nécessaire pour fournir les informations complémentaires demandées. La deuxième raison tient à la qualité des notifications: plus la notification est complète, plus le délai d'obtention des informations est court. La troisième raison tient clairement à la charge de travail du DPD ou du responsable du traitement de l'institution ou de l'organe concerné par la demande d'information.

([1]) L'article 27, paragraphe 4, du règlement est expliqué au point 2.3.2.

Ces chiffres et ces moyennes sont cependant basés sur un nombre limité de dossiers puisqu'il s'agit de la première année complète d'activité du CEPD. L'année 2006 montrera si ces tendances se poursuivent.

En outre, un plus grand nombre d'agences vont communiquer leurs traitements soumis au contrôle préalable du CEPD.

Annexe E

Liste des avis rendus à la suite d'un contrôle préalable

Enquêtes administratives et procédures disciplinaires — Cour des comptes

Avis du 22 décembre 2005 rendu à la suite d'un contrôle préalable à propos du dossier «Enquêtes administratives et procédures disciplinaires internes» (dossier 2005-316)

Enquêtes administratives — Banque centrale européenne

Avis du 22 décembre 2005 rendu à la suite d'un contrôle préalable concernant les enquêtes administratives internes (dossier 2005-290)

Sysper 2/REC — Commission

Avis du 15 décembre 2005 rendu à la suite d'un contrôle préalable à propos du dossier «Sysper 2: évaluation professionnelle — REC» (dossier 2005-218))

Stage rémunéré — Comité économique et social européen

Avis du 15 décembre 2005 rendu à la suite d'un contrôle préalable concernant la gestion des demandes de stage rémunéré (dossier 2005-297)

Congé maladie — Cour de justice

Avis du 15 novembre 2005 rendu à la suite d'un contrôle préalable concernant le «SUIVI: congé maladie de la direction de la traduction» (dossier 2004-279)

Candidatures spontanées en ligne — Comité des régions

Avis du 28 octobre 2005 rendu à la suite d'un contrôle préalable concernant la gestion des candidatures spontanées en ligne (dossier 2005-176)

Demandes de stage — Comité des régions

Avis du 27 octobre 2005 rendu à la suite d'un contrôle préalable concernant la gestion des demandes de stage rémunéré (dossier 2005-214)

Demandes de stage non rémunéré — Comité des régions

Avis du 27 octobre 2005 rendu à la suite d'un contrôle préalable concernant la gestion des demandes spontanées de stage non rémunéré (dossier 2005-215)

SIC congés — Cour de justice

Avis du 28 septembre 2005 rendu à la suite d'un contrôle préalable concernant le dossier «SIC congés» (dossier 2004-278)

Absences — Banque centrale européenne

Avis du 23 septembre 2005 rendu à la suite d'un contrôle préalable à propos du dossier «Enregistrement des absences des membres du personnel de la BCE dans l'incapacité de travailler en raison d'une maladie ou d'un accident» (dossier 2004-277)

Double allocation — Cour des comptes

Avis du 30 août 2005 rendu à la suite d'un contrôle préalable à propos du dossier «Double allocation» (dossier 2005-68)

Commission d'invalidité — Cour des comptes

Avis du 30 août 2005 rendu à la suite d'un contrôle préalable à propos du dossier «Commission d'invalidité» (dossier 2005-119)

Évaluation périodique du personnel — OHMI

Avis du 28 juillet 2005 rendu à la suite d'un contrôle préalable relatif au rapport d'évaluation périodique (dossier 2004-293)

Procédure disciplinaire — Banque européenne d'investissement

Avis du 25 juillet 2005 rendu à la suite d'un contrôle préalable à propos du traitement des données dans le cadre de la procédure disciplinaire (dossier 2005-102)

Harcèlement — Cour des comptes

Avis du 20 juillet 2005 rendu à la suite d'un contrôle préalable à propos du dossier «Harcèlement» (dossier 2005-145)

Système d'évaluation Compass — Cour des comptes

Avis du 19 juillet 2005 rendu à la suite d'un contrôle préalable à propos du dossier «Compass» (dossier 2005-152)

Manager Desktop — Banque européenne d'investissement

Avis du 12 juillet 2005 rendu à la suite d'un contrôle préalable à propos du dossier «Manager Desktop» (dossier 2004-307)

Évaluation du travail — Cour de justice

Avis du 12 juillet 2005 rendu à la suite d'un contrôle préalable sur l'évaluation du travail (dossier 2004-286)

Assmal — Conseil

Avis du 4 juillet 2005 rendu à la suite d'un contrôle préalable à propos du dossier «Application Assmal» et du dossier «Assmal-web» (dossiers 2004-246 et 2004-247)

Rapports de stage et de notation — Cour de justice

Avis du 4 juillet 2005 rendu à la suite d'un contrôle préalable concernant les «dossiers individuels: rapport de stage et rapport de notation» (dossier 2004-281)

Demandes d'emploi — Cour de justice

Avis du 4 juillet 2005 rendu à la suite d'un contrôle préalable concernant les demandes d'emploi et les CV des candidats (dossier 2004-284)

Dossiers médicaux — Cour de justice

Avis du 17 juin 2005 rendu à la suite d'un contrôle préalable concernant des dossiers médicaux (dossier 2004-280)

Retraite anticipée — Conseil

Avis du 18 mai 2005 rendu à la suite d'un contrôle préalable concernant la procédure «Sélection des fonctionnaires et agents temporaires admis à la retraite anticipée» (dossier 2004-248)

IDOC — Commission

Avis du 20 avril 2005 rendu à la suite d'un contrôle préalable concernant le dossier «Enquêtes administratives et procédures disciplinaires internes de la Commission européenne» — IDOC (dossier 2004-187)

Évaluation du personnel — Banque centrale européenne

Avis du 20 avril 2005 rendu à la suite d'un contrôle préalable concernant la procédure d'évaluation du personnel (dossier 2004-274)

Dignité au travail — Banque européenne d'investissement

Avis du 20 avril 2005 rendu à la suite d'un contrôle préalable concernant la politique en matière de dignité de la personne au travail (dossier 2004-67)

Gestion des frais médicaux — Banque européenne d'investissement

Avis du 6 avril 2005 rendu à la suite d'un contrôle préalable concernant le dossier «Procédures relatives à la gestion administrative des frais médicaux» (dossier 2004-305)

Répertoire des compétences — Conseil

Avis du 4 avril 2005 rendu à la suite d'un contrôle préalable concernant le répertoire des compétences (dossier 2004-319)

Dossiers disciplinaires — Parlement

Avis du 21 mars 2005 rendu à la suite d'un contrôle préalable concernant le traitement de données dans le cadre de dossiers disciplinaires (dossier 2004-198)

Rapnot — Parlement

Avis du 3 mars 2005 rendu à la suite d'un contrôle préalable concernant la procédure de notation et le système Rapnot (dossier 2004-206)

EPES — Commission

Avis du 4 février 2005 rendu à la suite d'un contrôle préalable concernant le dossier «Évaluation du personnel d'encadrement supérieur» — EPES (dossier 2004-95)

Rythme de travail — Commission

Avis du 28 janvier 2005 rendu à la suite d'un contrôle préalable concernant le dossier «Rythme de travail» (dossier 2004-96)

Sélection d'agents temporaires — OHMI

Avis du 6 janvier 2005 rendu à la suite d'un contrôle préalable concernant une procédure de sélection interne d'agents temporaires (dossier 2004-174)

Annexe F

Liste des avis sur des propositions législatives

Avis rendus en 2005

Protection des données dans le troisième pilier

Avis du 19 décembre 2005 sur la proposition de décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale [COM(2005) 475 final], JO C 47 du 25.2.2006, p. 27

Système d'information Schengen (SIS II)

Avis du 19 octobre 2005 sur trois propositions concernant le système d'information Schengen de deuxième génération (SIS II) [COM(2005) 230 final, COM(2005) 236 final et COM(2005) 237 final]

Conservation des données

Avis du 26 septembre 2005 sur la proposition de directive du Parlement européen et du Conseil concernant la conservation des données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE [COM(2005) 438 final], JO C 298 du 29.11.2005, p. 1

PNR Canada

Avis du 15 juin 2005 sur la proposition de décision du Conseil relative à la conclusion d'un accord entre la Communauté européenne et le gouvernement du Canada sur le traitement des données relatives aux informations anticipées sur les voyageurs (API)/dossiers passagers (PNR), JO C 218 du 6.9.2005, p. 6

Système d'information sur les visas

Avis du 23 mars 2005 sur la proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour [COM(2004) 835 final], JO C 181 du 23.7.2005, p. 13

Casier judiciaire

Avis du 13 janvier 2005 concernant la proposition de décision du Conseil relative à l'échange d'informations extraites du casier judiciaire [COM(2004) 664 final], JO C 58 du 8.3.2005, p. 3

Avis préparés en 2005, rendus en janvier 2006

Accès au système d'information sur les visas par les autorités responsables de la sécurité intérieure

Avis du 20 janvier 2006 sur la proposition législative concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités des États membres compétentes en matière de sécurité intérieure et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière [COM(2005) 600 final]

Annexe G

Composition du secrétariat du CEPD

Domaines placés sous la responsabilité directe du CEPD et du Contrôleur adjoint

— **Contrôle**

Sophie Louveaux
Administratrice

Eva Dimovne Keresztes
Administratrice

Maria Veronica Perez Asinari
Administratrice

Endre Szabo
Expert national

Delphine Harou (*)
Assistante superviseur

Xanthi Kapsosideri
Assistante superviseur

Sylvie Longrée
Assistante superviseur

Kim Thien Lê
Secrétaire

Vasilios Sotiropoulos
Stagiaire (octobre 2005-février 2006)

Zoi Talidou
Stagiaire (octobre 2005-février 2006)

Anna Vuori
Stagiaire (octobre 2005-février 2006)

— **Politique et information**

Hielke Hijmans
Administrateur

Laurent Beslay
Administrateur

Bénédicte Havelange
Administratrice

Alfonso Scirocco
Administrateur

Per Sjönell (*)
Administrateur/attaché de presse

Martine Blondeau (*)
Assistante/documentation

Andrea Beach
Secrétaire

Herke Kranenborg
Stagiaire (janvier-mars 2006)

— **Unité «Personnel, budget, administration»**

Monique Leens-Ferrando
Chef d'unité

Giuseppina Lauritano
Administratrice/questions statutaires et audit

Vittorio Mastrojeni
Assistant/ressources humaines

Anne Levêcque
Secrétaire/ressources humaines

Alexis Fiorentino
Commis comptable

(*) Équipe «Information».

Annexe H

Liste des accords et décisions administratifs

Liste des accords au niveau des services signés par le CEPD avec d'autres institutions

— Accords au niveau des services avec la Commission (bureau des stages de la DG Éducation et culture, et DG Emploi, affaires sociales et égalité des chances)

— Accord au niveau des services avec le Conseil

— Accord au niveau des services avec l'École européenne d'administration

Liste des décisions adoptées par le CEPD

Décision du 12 janvier 2005 du Contrôleur européen de la protection des données portant dispositions générales d'exécution en matière d'allocations familiales

Décision du 27 mai 2005 du Contrôleur européen de la protection des données portant dispositions générales d'exécution relatives au programme de stages

Décision du 15 juin 2005 du Contrôleur européen de la protection des données portant dispositions générales d'exécution en matière de travail à temps partiel

Décision du 15 juin 2005 du Contrôleur européen de la protection des données portant dispositions générales d'exécution en matière de congés

Décision du 15 juin 2005 du Contrôleur européen de la protection des données portant dispositions générales d'exécution concernant les critères applicables au classement en échelon lors de la nomination ou de la prise de fonctions

Décision du 15 juin 2005 du Contrôleur européen de la protection des données portant adoption de l'horaire flexible avec possibilité de récupération des heures supplémentaires prestées.

Décision du 22 juin 2005 du Contrôleur européen de la protection des données portant adoption d'une réglementation commune relative à la couverture des risques d'accident et de maladie professionnelle des fonctionnaires des Communautés européennes

Décision du 1er juillet 2005 du Contrôleur européen de la protection des données portant dispositions générales d'exécution en matière de congé familial

Décision du 25 juillet 2005 du Contrôleur européen de la protection des données portant dispositions d'exécution en matière de congé de convenance personnelle des fonctionnaires et de congé sans rémunération des agents temporaires et agents contractuels des Communautés européennes

Décision du 25 juillet 2005 du Contrôleur européen de la protection des données relative aux activités extérieures et aux mandats

Décision du 26 octobre 2005 du Contrôleur européen de la protection des données portant dispositions générales d'exécution relatives à l'allocation de foyer par décision spéciale

Décision du 26 octobre 2005 du Contrôleur européen de la protection des données portant dispositions générales d'exécution en matière de détermination du lieu d'origine

Décision du 7 novembre 2005 du Contrôleur européen de la protection des données établissant un système de contrôle interne au sein du CEPD

Décision du 10 novembre 2005 du Contrôleur européen de la protection des données relative au régime applicable aux experts nationaux détachés auprès de ses services

Décision du 16 janvier 2006 modifiant la décision du 15 juillet 2005 du Contrôleur européen de la protection des données portant adoption d'une réglementation commune relative à la couverture des risques de maladie des fonctionnaires des Communautés européennes

Décision du 26 janvier 2006 du Contrôleur européen de la protection des données portant adoption de la réglementation fixant les modalités d'octroi d'une aide financière complétant la pension d'un conjoint survivant affecté d'une maladie grave ou prolongée ou souffrant d'un handicap

Décision du 8 février 2006 du Contrôleur européen de la protection des données relative à la mise en place d'un comité du personnel au CEPD

Contrôleur européen de la protection des données

Rapport annuel 2005

Luxembourg: Office des publications officielles des Communautés européennes

2006 — 79 p. — 21 x 29,7 cm

ISBN 92-95030-01-X