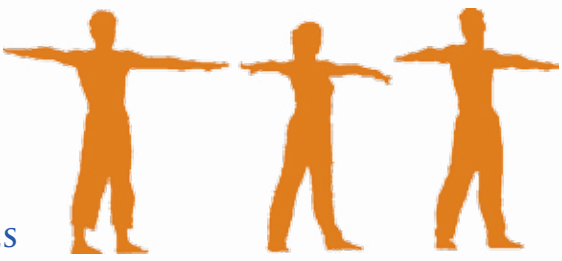
ISSN 1830-5482

Rapport annuel

2012

Le Contrôleur Européen
de la protection des données



Rapport annuel

2012

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

(*) Les informations sont fournies à titre gracieux et les appels sont généralement gratuits (sauf certains opérateurs, hôtels ou cabines téléphoniques).

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

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

Luxembourg: Office des publications de l'Union européenne, 2013

ISBN 978-92-95076-78-5
doi:10.2804/52280

Printed in Belgium

Imprimé sur papier blanchi sans chlore élémentaire (ECF)

Table des matières

1 FAITS MARQUANTS DE 2012

2 SUPERVISION ET MISE EN APPLICATION

3 CONSULTATION

7 ADMINISTRATION, BUDGET ET PERSONNEL

8 DÉLÉGUÉ À LA PROTECTION DES DONNÉES DU CEPD

9 PRINCIPAUX OBJECTIFS POUR 2013

GUIDE DE L'UTILISATEUR

Le lecteur trouvera, immédiatement après ce guide, l'avant-propos du rapport annuel 2012, rédigé par M. Peter Hustinx, contrôleur européen de la protection des données et M. Giovanni Buttarelli, contrôleur adjoint, précédé de l'énoncé de leur mission.

Le chapitre 1 — **«Faits marquants de 2012»,** présente les grands axes de nos activités en 2012, les résultats de la révision stratégique et les résultats obtenus dans les différents champs d'activité.

Le chapitre 2 — **«Supervision»,** décrit les travaux menés pour vérifier que les institutions et les organes de l'Union européenne (UE) s'acquittent de leurs obligations en matière de protection des données. Ce chapitre présente une analyse des principales problématiques dans le domaine des contrôles préalables, de la suite donnée aux réclamations et du contrôle du respect des règles et des avis sur les mesures administratives traitées en 2012. Il contient également des informations sur les lignes directrices adoptées par le CEPD concernant les consultations dans le domaine de la supervision et de la mise en application et les lignes directrices concernant le traitement de données à caractère personnel en matière de congé et d'horaire flexible.

Le chapitre 3 — **«Consultation»,** traite de l'évolution de notre rôle consultatif. Il s'intéresse principalement aux avis et observations formulés sur les propositions législatives et documents connexes, ainsi qu'à leur incidence dans un nombre croissant de domaines. Ce chapitre aborde également l'implication du CEPD dans les litiges soumis à la Cour de justice de l'UE. Il contient une analyse de certains thèmes horizontaux, comme par exemple l'évolution des politiques et de la législation et le réexamen en cours du cadre juridique de la protection des données de l'UE.

Le chapitre 4 — **«Coopération»,** décrit notre travail dans des forums importants comme, par exemple, le groupe de travail «Article 29» sur la protection des données et les conférences européenne et internationale sur la protection des données. Il aborde également la supervision coordonnée (par le CEPD et par les autorités nationales chargées de la protection des données) des systèmes informatiques à grande échelle.

Le chapitre 5 — **«Suivi technologique»,** donne une large vue d'ensemble des tendances en matière de technologie susceptibles d'avoir une incidence sur le respect de la vie privée et la protection des données personnelles dans un avenir proche.

Le chapitre 6 — **«Communication»,** présente nos activités d'information et de communication et les résultats obtenus, y compris les activités de communication extérieure avec les médias, les événements de sensibilisation, l'information du public et les outils d'information en ligne.

Le chapitre 7 — **«Administration, budget et personnel»,** détaille les principales évolutions intervenues au sein de l'organisation du CEPD, notamment en ce qui concerne les aspects budgétaires, la question des ressources humaines et les accords de nature administrative.

Le chapitre 8 — **«Délégué à la protection des données (DPD) du CEPD»,** inclut un rapport sur la mise à jour du registre des traitements du CEPD en 2012, qui a débouché sur 25 nouvelles notifications.

Le chapitre 9 — **«Principaux objectifs pour 2013»,** donne un aperçu de notre travail et de nos priorités principales pour l'année 2013.

Des **annexes** complètent ce rapport. Parmi celles-ci, un aperçu du cadre juridique pertinent, les dispositions du règlement (CE) n° 45/2001, la liste des délégués à la protection des données, la liste des avis en vue d'un contrôle préalable et des avis consultatifs du CEPD, les discours prononcés par le contrôleur et son adjoint, et la composition du secrétariat du CEPD.

Un résumé de ce rapport est également disponible, avec une vue d'ensemble synthétique des principaux développements intervenus en 2012 dans les activités du CEPD.

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

De plus amples informations concernant le CEPD sont disponibles sur son site internet: http://www.edps.europa.eu.

Le site internet contient également une fonction d'abonnement à la newsletter du CEPD.

 @EU_EDPS

DÉCLARATION DE MISSION, VALEURS ET PRINCIPES

Le Contrôleur européen de la protection des données est l'autorité indépendante de protection des données de l'Union européenne instituée par le règlement (CE) n° 45/2001 (ci-après «le règlement»)[1]. Il a pour mission de protéger les informations personnelles et la vie privée et de promouvoir les bonnes pratiques au sein des institutions et organes de l'Union européenne.

- Nous **contrôlons** et **veillons** à la protection des données à caractère personnel et de la vie privée dans le cadre du traitement des informations personnelles des individus effectué par les institutions et organes de l'UE.
- Nous **conseillons** les institutions et organes de l'UE sur toutes les questions relatives au traitement des informations personnelles. Nous sommes consultés par le législateur de l'UE au sujet des propositions législatives et de l'élaboration de nouvelles politiques susceptibles d'avoir une incidence sur le respect de la vie privée.
- Nous **suivons** également le développement des nouvelles technologies qui pourraient avoir une incidence sur la protection des informations personnelles.
- Nous **intervenons** devant la Cour de justice de l'UE pour fournir des avis d'experts sur l'interprétation des textes de loi concernant la protection des données.
- Enfin, nous **coopérons** avec les autorités de contrôle nationales et les autres organes de contrôle en vue d'améliorer la cohérence en matière de protection des données à caractère personnel.

Les valeurs et principes suivants déterminent la manière dont nous abordons notre mission et dont nous travaillons avec les parties prenantes.

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

Valeurs fondamentales

- Impartialité – travailler au sein du cadre législatif et politique existant tout en faisant preuve d'indépendance et d'objectivité et en trouvant le juste équilibre entre les différents intérêts en jeu.
- Intégrité – observer les normes de conduite les plus élevées et faire ce qui est juste même si cela s'avère impopulaire.
- Transparence – expliquer ce que nous faisons et pourquoi nous le faisons dans un langage clair et accessible à tous.
- Pragmatisme – comprendre les besoins des parties prenantes et rechercher des solutions qui fonctionnent dans la pratique.

Principes directeurs

- Nous servons l'intérêt général dans le but de garantir que les institutions de l'UE respectent les politiques et pratiques mises en place dans le domaine de la protection des données. Nous contribuons à l'élaboration des politiques au sens large dès lors qu'elles affectent la protection des données européenne.
- En nous appuyant sur notre expertise, notre autorité et nos pouvoirs officiels, nous entendons sensibiliser l'opinion à la protection des données en tant que droit fondamental et élément essentiel d'une politique publique saine et de la bonne administration au sein des institutions de l'UE.
- Nous centrons notre attention et nos efforts sur des domaines politiques ou administratifs où les risques de non-respect des règles de protection des données et les répercussions sur la vie privée sont les plus élevés. Nous agissons de manière sélective et proportionnée.

AVANT-PROPOS

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

Le présent rapport concerne l'année 2012, neuvième année d'activité du CEPD en tant qu'autorité de contrôle indépendante, dont la mission est de veiller à ce que, lors du traitement de données à caractère personnel, les libertés et droits fondamentaux des personnes physiques, en particulier leur vie privée, soient respectés par les institutions et organes de l'UE. Ce rapport couvre également la quatrième année de notre mandat commun en tant que membres de cette autorité.

Dans le climat actuel d'austérité, des efforts particuliers ont été consacrés cette année au renforcement de l'efficacité et de l'efficience de notre organisation. C'est dans ce contexte que nous avons réalisé une révision stratégique approfondie qui a abouti à la définition d'objectifs clairs pour 2013-2014, à l'adoption d'un règlement intérieur couvrant toutes les activités du CEPD et à l'adoption d'un plan de gestion annuel.

Au cours de l'année 2012, nous avons une fois de plus défini de nouvelles références dans différents domaines d'activité. Concernant la supervision des institutions et organes de l'UE, lors du traitement de données à caractère personnel, nous avons interagi plus que jamais avec les délégués à la protection des données d'un nombre record d'institutions et organes. De plus, nous avons constaté les effets de notre nouvelle politique d'application: la plupart des institutions et organes de l'UE font de notables progrès dans le respect du règlement relatif à la protection des données, tandis que d'autres devraient renforcer leurs efforts.

Dans le cadre de la procédure de consultation pour les nouvelles mesures législatives, nous avons émis un nombre record d'avis portant sur un large éventail de sujets. La révision du cadre juridique de l'UE pour la protection des données personnelles était en tête de nos priorités. Toutefois, l'entrée en vigueur du programme de Stockholm dans le domaine de la liberté, de la sécurité et de la justice et la stratégie numérique, les questions liées au marché intérieur comme la réforme du secteur financier ou encore les débats relatifs à la santé publique et à la protection des consommateurs ont eu des répercussions sur la protection des données. Nous avons également renforcé notre coopération avec d'autres autorités de surveillance.

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

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

Peter Hustinx
Contrôleur européen de la protection des données

Giovanni Buttarelli
Contrôleur adjoint

1 FAITS MARQUANTS DE 2012

1.1. Aperçu général de 2012

Le volume et la portée des principales activités du CEPD ont continué de progresser en 2012, alors même que les contraintes budgétaires ont entraîné une réduction effective des ressources. La révision stratégique annoncée dans le dernier rapport annuel a été achevée, et la stratégie pour 2013-2014 qui en découle exprime la vision et la méthodologie requises pour améliorer notre capacité à travailler de manière efficace et efficiente dans un climat d'austérité. Outre cette stratégie, le CEPD a adopté un règlement intérieur et un plan de gestion annuel. Ces documents sont étroitement liés et présentés au point 1.2 ci-dessous.

Le cadre juridique[2] dans lequel le CEPD opère définit un certain nombre de tâches et de compétences qui permettent de distinguer nos trois fonctions principales, à savoir la **supervision**, la **consultation** et la **coopération**. Ces fonctions continuent de faire office de cadre stratégique pour nos activités et sont présentées dans l'énoncé de sa mission:

- une **fonction de supervision**, qui consiste à superviser et assurer le respect des garanties juridiques existantes par les institutions et organes de l'UE[3] chaque fois qu'ils traitent des informations personnelles;
- une **fonction de consultation**, qui consiste à conseiller les institutions et les organes de l'UE sur toutes les questions pertinentes, et en particulier sur les propositions législatives ayant une incidence sur la protection des informations personnelles;
- une **fonction de coopération**, qui consiste à collaborer avec les autorités nationales de contrôle et les organes de contrôle relevant de l'ancien troisième pilier de l'UE chargés de la coopération policière et judiciaire en matière pénale, en vue d'améliorer la cohérence en matière de protection des informations personnelles.

Ces fonctions sont analysées dans les chapitres 2, 3 et 4, qui présentent notre vision, nos principales activités et les progrès réalisés en 2012. Certains éléments-clés sont toutefois résumés dans ce chapitre.

En 2012, un nouveau secteur dédié à la politique des technologies de l'information (le secteur de «Politique IT») a été créé afin de mieux traiter les différentes questions liées à l'utilisation des nouvelles technologies de l'information. Le nouveau chapitre 5, qui met l'accent sur le suivi technologique, reflète cette évolution.

L'importance de l'information et de la communication pour nos activités principales continue également de croître, et le chapitre 6 présente nos travaux en matière de communication en 2012. Toutes nos activités reposent sur une gestion efficace des ressources financières, humaines et autres, qui font l'objet du chapitre 7.

Supervision et mise en application

Le CEPD assume des tâches de supervision très larges allant du conseil et de l'aide aux délégués à la protection des données (DPD) à la conduite

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

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

d'enquêtes, notamment des inspections sur place et le traitement des réclamations, en passant par l'orientation, la formation et le contrôle préalable des opérations de traitement des données à risque.

Nous considérons les DPD comme des acteurs essentiels pour garantir le respect du règlement relatif à la protection des données. C'est pourquoi nous avons continué de soutenir leur travail en participant aux réunions des DPD, en organisant des formations ou des ateliers à l'attention des DPD, en rencontrant individuellement les DPD ayant besoin de conseils spécifiques, en créant une ligne d'assistance pour les questions des DPD et en créant un espace consacré aux DPD sur notre site internet.

En mai 2012, dans le cadre de nos efforts de soutien au travail des DPD, nous avons lancé une enquête sur le statut des DPD. Basée sur un questionnaire, cette enquête portait principalement sur le mandat, la position et les ressources des DPD afin de recueillir des informations homogènes sur la situation et l'évolution du rôle des DPD. Les conclusions de cet exercice ont été rassemblées dans un rapport qui met en évidence un certain nombre de points positifs, mais aussi certains sujets de préoccupation que nous entendons suivre de près.

Le **contrôle préalable** des traitements à risque a encore constitué un aspect important du travail de supervision. En 2012, nous avons reçu 119 notifications de contrôle préalable et adopté 71 avis de contrôle préalable. À l'issue d'une analyse minutieuse, 11 dossiers n'ont pas fait l'objet d'un contrôle préalable. En 2012, contrairement aux années précédentes où les avis du CEPD étaient fréquemment adressés aux grandes institutions de l'Union européenne, nous avons adressé la majorité de nos avis aux agences et aux organes de l'Union. De manière générale, les avis adoptés en 2012 concernaient des procédures administratives standard, comme l'évaluation du personnel ou le traitement de données en matière de santé, mais aussi les activités principales des organisations concernées, comme les opérations de traitement liées aux activités de gel des actifs par la Commission, les procédures d'enquête révisées de l'OLAF et les déclarations annuelles d'intérêts. En ce qui concerne le suivi des avis du CEPD, nous avons eu le plaisir de clore 92 dossiers en 2012.

Nous avons reçu 86 réclamations en 2012, soit une diminution d'environ 20 % par rapport à 2011, ce qui confirme l'efficacité du formulaire de réclamation en ligne pour réduire le nombre des réclamations irrecevables. Sur ces 86 réclamations, 46 ont été jugées irrecevable à première vue. Les 40 autres ont donné lieu à des enquêtes plus approfondies. Sur les affaires résolues en 2012, nous avons conclu qu'il n'y avait pas de violation des règles de protection des données ou que les mesures nécessaires avaient été prises dans 26 dossiers. À l'inverse, dans quatre dossiers, nous avons constaté un non-respect des règles de protection des données et transmis des recommandations au responsable du traitement des données.

Outre nos activités générales de contrôle, comme celle concernant le statut des DPD, nous avons concentré nos actions de contrôle dans des domaines où nous avions des raisons de nous inquiéter du degré de conformité avec le règlement. En 2012, nous avons visité six agences pour lesquelles nous soupçonnions un manque d'engagement en faveur du respect des règles ou un manque de communication avec le CEPD. Ces visites se sont révélées très efficaces pour sensibiliser les personnes concernées à la question et susciter un engagement à respecter le règlement. Nous avons **inspecté** 15 institutions ou organes de l'Union et assuré le suivi des inspections antérieures.

Le 23 novembre 2012, nous avons publié une **politique en matière de consultations dans le domaine de la supervision et de la mise en application**. Ce document fournit aux institutions, organes de l'Union et DPD des orientations relatives aux consultations du CEPD sur la base des articles 28, paragraphe 1, et 46, sous d), du règlement. Cette politique insiste sur leur responsabilité en tant qu'institutions et sur le rôle essentiel joué par leurs DPD.

Nous avons également fourni des orientations aux institutions et agences de l'Union européenne avec l'adoption des **lignes directrices concernant le traitement de données à caractère personnel en matière de congé et d'horaire flexible**.

Consultation

En 2012, poursuivant la tendance des années précédentes, notre travail de consultation relatif à la législation a encore augmenté pour atteindre un record de 33 avis, 15 observations formelles et 37 observations informelles. Notre inventaire reflète le nombre croissant de propositions législatives qui nous sont soumises pour consultation, qui témoigne de l'importance croissante accordée à la protection des données dans la législation de l'Union européenne.

Nous sommes restés étroitement associés au travail en cours en vue de la réforme du cadre européen relatif à la protection des données[4]. Nous avons rendu en mars un avis sur la **proposition relative au train de réformes** composé d'un règlement et d'une directive, publiée au mois de janvier. Par la suite, nous avons continué de mettre en évidence les sujets de préoccupation éventuels et les améliorations possibles dans des discours, des communiqués de presse et autres forums tout au long de l'année. De manière générale, nous considérons que le règlement proposé, un instrument **directement applicable** dans tous les États membres, constitue un grand pas en avant. Nous regrettons toutefois qu'un instrument distinct, la directive proposée, assurant un degré de protection nettement inférieur, ait été choisi afin de réglementer le domaine répressif. Cette directive **ne répond pas à l'exigence d'un degré uniforme et élevé** de protection des données, et assure est de ce fait une protection nettement inférieure à celle du règlement proposé. Le principal point faible de ce train de réformes est qu'il ne remédie pas au caractère généralement incomplet des règles européennes en matière de protection des données.

La protection des données revêt une importance croissante: outre les priorités habituelles liées à l'espace de liberté, de sécurité et de justice (ELSJ) et aux transferts internationaux de données, le CEPD a rendu un nombre croissant d'avis relatifs au marché intérieur et au secteur de la santé en 2012. Dans l'intervalle, l'évolution rapide dans le domaine de la stratégie numérique entraîne un flux important de propositions législatives en la matière. Les faits marquants suivants incluent une sélection des avis adoptés dans ces domaines.

Dans le domaine de l'**ELSJ**, la question de la nécessité est devenue un thème récurrent et les services répressifs plaident en faveur d'un accès accru à d'autres bases de données à des fins de prévention de la criminalité. Nous avons mis en garde contre cette tendance au détournement d'usage et insisté sur ses effets néfastes potentiels, comme le montrent nos avis concernant EURODAC, SIS II et le Centre européen de lutte contre la cybercriminalité. Parmi les autres problèmes rencontrés dans ce domaine, on peut citer les transferts de données excessifs et l'apparente indifférence quant à l'utilité d'appliquer des principes adéquats de protection des données pour garantir la réussite des initiatives en matière répressive. Nous avons souligné ces préoccupations dans nos observations concernant, respectivement, EUROSUR et la stratégie de l'UE en vue de l'éradication de la traite des êtres humains 2012-2016.

Dans le domaine de la **stratégie numérique et de la technologie**, nous avons publié un avis sur l'informatique en nuage mettant en évidence les défis particuliers posés en matière de protection des données par l'informatique en général ainsi que la façon dont la proposition de règlement relatif à la protection des données va s'attaquer à ces défis. L'impact des nouvelles technologies est et restera de la plus haute importance dans ce domaine et nécessite la mise en œuvre de principes de protection des données tels que la *prise en compte du respect de la vie privée dès la conception et du respect de la vie privée par défaut*. Nous avons également souligné cette nécessité dans les autres avis que nous avons formulés dans ce domaine, concernant par exemple les compteurs intelligents, la sécurité des réseaux et de l'information dans l'Union, l'internet ouvert et la neutralité du réseau.

En ce qui concerne le **marché intérieur**, nous avons rendu une série d'avis sur les propositions de réformes en vue d'une surveillance accrue des marchés financiers. Ces avis concernent principalement les conséquences pour la protection des données du contrôle des données financières et des transferts transfrontaliers. Si le souhait d'un plus grand contrôle des données financières peut se justifier, nous insistons sur le fait que ces données peuvent aussi inclure des informations personnelles. Les propositions en la matière doivent donc prévoir des mesures de protection adéquates. En 2012, le CEPD a aussi rendu des avis importants sur la coopération administrative dans le domaine des droits d'accises, sur les contrôles légaux, sur les fonds européens de capital-risque et les fonds d'entreprenariat social, sur la médiation en matière d'assurances, les OPCVM, et les documents contenant des informations essentielles relatives aux produits d'investissement. Nous avons fréquemment recommandé une justification plus claire de la portée des pouvoirs d'enquête des autorités réglementaire.

L'équilibre entre la transparence et la protection des données est un thème récurrent de notre travail. En 2012, nous avons adopté plusieurs avis dans différents domaines portant sur la **publication d'informations personnelles**. Ces cas peuvent être subdivisés en différentes catégories telles que la réutilisation d'informations du secteur public (ISP) et la publication d'informations personnelles dans le contexte d'une dénonciation publique («naming and shaming»). Dans ces avis comme dans d'autres, nous avons insisté sur la nécessité de trouver un équilibre entre le principe de transparence, le droit au respect

[4] http://www.edps.europa.eu/EDPSWEB/edps/Consultation/Reform_package

de la vie privée et à la protection des données et la nécessité de garanties spécifiques.

Concernant la **santé publique et les consommateurs, nous avons constaté une tendance croissante à associer les nouvelles technologies** numériques aux pratiques existantes afin d'améliorer la qualité du service. Ces efforts sont louables, et la personnalisation des soins et des services dispose d'un potentiel élevé. Cependant, étant donné le caractère sensible des données personnelles en matière de santé, il est indispensable de respecter les principes fondamentaux en matière de protection des données pour gagner et conserver la confiance des consommateurs dans ces nouveaux services. La consolidation de données précédemment non pertinentes et d'informations recueillies à d'autres fins reste un défi propre à ce domaine.

Nous avons également formulé des observations sur d'autres propositions, comme la création du Corps volontaire européen d'aide humanitaire, une proposition relative au dépôt des archives historiques des institutions auprès de l'Institut universitaire européen de Florence ou encore la proposition de règlement relatif au statut et au financement des partis politiques européens et des fondations politiques européennes.

Affaires portées devant les tribunaux

En 2012, nous sommes intervenus dans cinq affaires devant la Cour de justice de l'Union européenne et le Tribunal de la fonction publique.

La première affaire portait sur le manque d'indépendance allégué de l'autorité autrichienne chargée de la protection des données (DSK). Le CEPD a soutenu la position de la Commission, selon laquelle l'indépendance fonctionnelle de la DSK prévue par la législation autrichienne n'était pas suffisante. La Cour a suivi ce raisonnement et conclu que les liens étroits unissant la DSK à la Chancellerie fédérale autrichienne ne permettaient pas à la DSK de se placer au-dessus de tout soupçon de partialité.

Nous sommes également intervenus aux côtés du requérant dans l'affaire *Egan et Hackett* c. *Parlement européen* (Affaire T-190/10). Il s'agit de la dernière de trois affaires dans lesquelles le Tribunal a dû se prononcer sur la relation entre le règlement sur l'accès public aux documents et le règlement relatif la protection des données depuis l'arrêt dans l'affaire *Bavarian lager* c. *Commission* du 29 juin 2010 (affaire C-28/08 P). Comme dans les deux autres affaires, le CEPD a plaidé en faveur d'une plus grande transparence.

Nous sommes intervenus dans deux autres affaires qui étaient encore pendantes au moment de la rédaction du présent rapport. La première de ces affaires est une procédure d'infraction contre la Hongrie concernant l'indépendance de son autorité de protection des données. La deuxième affaire, portée devant le Tribunal de la fonction publique, concerne une violation alléguée par la BEI du règlement (CE) n° 45/2001 relatif à la protection des données lors d'une enquête interne sur un cas de harcèlement.

Nous avons également suivi de près plusieurs autres affaires sans intervenir, comme l'affaire Google en Espagne portant sur l'applicabilité aux activités de Google de la législation espagnole mettant en œuvre la directive européenne relative à la protection des données ainsi que deux autres affaires concernant la validité de la directive européenne sur la conservation des données.

Coopération

La principale plate-forme de coopération entre les autorités de protection des données en Europe est le Groupe de travail de l'article 29 (GT29) sur la protection des données. Le CEPD participe à ses activités et joue ainsi un rôle important dans l'application uniforme de la directive relative à la protection des données.

Le CEPD et le GT29 ont collaboré sur un grand nombre de sujets, et notamment sur les avis relatifs à la limitation de la finalité et à l'utilisation compatible, aux modèles d'évaluation de l'impact du réseau électrique intelligent sur la protection des données et sur les données ouvertes, pour lesquels le CEPD a agi en tant que rapporteur. Nous avons également contribué de manière significative aux avis adoptés au sujet de discussions sur la réforme de la protection des données, de l'informatique en nuage, de l'exemption de l'obligation de consentement pour certains cookies et de l'évolution des technologies biométriques.

Nous avons également été très actifs dans le domaine de la supervision coordonnée des grandes bases de données comme **EURODAC**, une base de données européenne contenant des empreintes digitales et destinée à identifier les demandeurs d'asile et les personnes qui traversent les frontières de manière irrégulière. Le groupe de coordination du contrôle d'EURODAC, composé des autorités nationales chargées de la protection des données et du CEPD, s'est réuni à deux reprises à Bruxelles en 2012. Ce groupe a adopté un plan d'inspection standardisé pour les points d'accès nationaux (PAN) à EURODAC afin de faciliter les inspections nationales et s'est accordé sur la nécessité de

définir une pratique uniforme de gestion des empreintes digitales illisibles après la finalisation du rapport correspondant en 2013.

Un arrangement similaire régit la supervision du **système d'information douanier** (SID), et nous avons organisé deux réunions du groupe de coordination du contrôle du SID en 2012. Lors de ces réunions, le groupe, en collaboration avec l'autorité de contrôle commune des douanes, a adopté un avis commun concernant le manuel FIDE ainsi qu'un rapport d'activités pour les deux années précédentes. Son secrétariat a présenté deux projets de rapports qui, après leur adoption en 2013, formeront la base des activités de suivi possibles du groupe à l'avenir.

Le nouveau groupe de coordination du contrôle du **Système d'information sur les visas** (VIS) a tenu sa première réunion en novembre 2012. VSI, une base de données incluant des données biométriques sur les demandes de visas présentées par des ressortissants de pays tiers, vise à empêcher la fraude en matière de visas et les demandes de visas multiples dans les divers États membres (*visa shopping*), à faciliter l'identification des titulaires de visas au sein de l'Union européenne, et à vérifier que le demandeur et l'utilisateur du visa sont la même personne. Principalement chargé de superviser le déploiement progressif en cours du système et de faciliter la coopération entre les États membres, le groupe a discuté de son premier programme de travail et partagé l'information concernant les activités du CEPD et les inspections nationales dans différents États membres.

La coopération au sein de **forums internationaux** a continué d'attirer l'attention, notamment la conférence européenne et la conférence internationale des commissaires à la protection des données et de la vie privée. En 2012, la Conférence européenne a été organisée au Luxembourg et était notamment consacrée aux développements récents dans la modernisation des cadres de protection des données de l'UE, du Conseil de l'Europe et de l'OCDE. La Conférence internationale qui s'est tenue en Uruguay était principalement axée sur thème général de l'«*Équilibre entre vie privée et technologie*» («*Privacy and Technology in Balance*»), et portait notamment sur les pays émergents et les questions liées au profilage et à la circulation massive de données («big data»).

Organisation interne

En 2012, le nouveau secteur «Politique IT» a été créé au sein de l'organisation afin de développer et de concentrer notre expertise en matière de technologies de l'information et de protection des données. Ce secteur est composé d'experts en informatique disposant d'une expérience dans les questions informatiques d'ordre pratique ainsi qu'en matière de politique et de supervision. Il améliore notre capacité à évaluer les risques que font peser les nouvelles technologies sur le respect de la vie privée, échanger avec les experts en technologie des autres autorités de protection des données et à fournir aux responsables du traitement des orientations sur les principes de *respect de la privée dès la conception* et de *respect de la vie privée par défaut*. Il nous permet également de développer nos méthodes et outils de contrôle en fonction de l'évolution des technologies, notamment en ce qui concerne les systèmes informatiques à grande échelle soumis à une supervision coordonnée. Ce secteur soutiendra également le développement d'une politique informatique interne plus cohérente pour l'institution.

Gestion des ressources

À la suite des examens trimestriels de l'exécution du budget, qui ont impliqué le conseil d'administration de l'institution, l'exécution de notre budget est passée de 75,66 % en 2010 à 90,16 % en 2012. De nouveaux outils informatiques tels que Sysper2 (RH) et MIPs (gestion des missions) ont permis de rendre la gestion des ressources humaines du CEPD plus efficace et plus professionnelle.

Chiffres-clés du CEPD en 2012

→ 71 avis de contrôle préalable adoptés, et 11 avis sur l'absence de contrôle préalable

→ 86 réclamations reçues, dont 40 recevables

→ 27 consultations reçues concernant des mesures administratives.

→ 15 inspections sur place et 6 visites effectuées

→ 1 document de lignes directrices publié concernant le traitement de données à caractère personnel en matière de congé et d'horaire flexible

→ 33 avis législatifs rendus concernant, entre autres, des initiatives relatives à l'espace de liberté, de sécurité et de justice, aux évolutions technologiques, à la coopération internationale, au transfert des données, à la santé publique ou au marché intérieur.

→ 15 séries d'observations formelles publiées, concernant notamment les droits de propriété intellectuelle, la sécurité de l'aviation civile, la politique criminelle de l'UE, le système de surveillance du financement du terrorisme, l'efficacité énergétique et le programme «Droits et citoyenneté».

→ 37 séries d'observations informelles publiées

1.2. Vision et méthodologie: révision stratégique, règlement intérieur et plan de gestion annuel

De gauche à droite, les membres du comité de direction du CEPD: Giovanni Buttarelli, Contrôleur adjoint, Peter Hustinx, Contrôleur, et Christopher Docksey, Directeur

En 2012, l'institution a atteint sa pleine maturité du fait de processus coordonnés qui ont abouti à l'adoption de trois documents en décembre: le rapport sur la révision stratégique, le règlement intérieur et le plan de gestion annuel.

Ces trois documents sont étroitement liés. Ainsi, les valeurs fondamentales et les principes directeurs définis lors de la révision stratégique sont-ils inscrits à l'article 15 du règlement intérieur. Les actions qui sous-tendent la nouvelle stratégie pour 2013-2014 sont mises en œuvre dans le plan de gestion annuel pour 2013.

Ces trois documents reposent sur notre expérience et sur des initiatives menées avant ou pendant leur élaboration. La contribution des parties prenantes pendant la révision stratégique a mis en évidence la nécessité d'améliorer notre compréhension des questions informatiques et de mettre en place une vision cohérente et faisant autorité sur l'influence de la mondialisation et de la technologie sur la protection des données dans l'Union européenne. En réaction, comme indiqué au point précédent, le secteur «Politique IT» a été créé en 2012.

1.2.1 Révision stratégique et stratégie 2013-2014

Le CEPD a lancé un processus de révision stratégique en juillet 2011, comme l'indique le rapport annuel relatif à cette année. Ce processus a été guidé par différents facteurs. Tout d'abord, la révision était l'étape finale du processus de restructuration interne entamé par les contrôleurs en octobre 2009. Le CEPD, qui était à l'origine un organe modeste composé de deux membres et d'un petit secrétariat, est devenu une institution à part entière comptant près de 50 membres du personnel. Dans le cadre de ce processus, le secrétariat a été restructuré en 2010 pour lui donner une forme institutionnelle effective.

Deuxièmement, après l'entrée en vigueur du traité de Lisbonne, l'institution est entrée dans une phase marquée par de nouveaux défis, et notamment l'utilisation croissante de l'internet et des nouvelles technologies, le développements de programmes tels que le programme de Stockholm et la stratégie numérique, la révision du cadre législatif en matière de protection des données, et la mise en œuvre du traité de Lisbonne lui-même. Ces évolutions ont entraîné une augmentation significative des activités et de la charge de travail.

Troisièmement, les incidences en termes de ressources imposent de plus en plus à l'institution d'en faire «plus avec moins». S'il est vrai que les ressources augmentent lentement, mais de manière constante, cette augmentation ne suit pas le rythme de l'augmentation des activités du CEPD au fil des années dans tous les domaines.

En conséquence, la révision stratégique a été lancée afin d'identifier les priorités et de permettre une mise en correspondance aussi efficace que possible des ressources avec les activités. Ce processus a été dirigé par un groupe de travail composé du directeur et de représentants de toutes les équipes et de toutes les disciplines professionnelles représentées en interne. La révision s'est achevée en 2012 à l'issue d'un processus intensif de consultation des parties prenantes internes et externes. Cette consultation a été réalisée par des réunions internes et une enquête en ligne auprès de quelque 500 parties prenantes externes, suivies de groupes de discussion et d'entretien.

De manière générale, le CEPD est perçu par les parties prenantes externes comme un organisme compétent faisant autorité dans son domaine, qui joue un rôle de premier plan et qui dispose d'une solide

expertise en matière de protection des données. Cependant, les parties prenantes ont formulé plusieurs propositions d'actions, notamment la nécessité pour le CEPD:

- de collaborer plus étroitement avec les parties prenantes et de mieux comprendre leurs politiques et contraintes institutionnelles;
- de redoubler d'efforts pour sensibiliser à la protection des données;
- d'améliorer ses connaissances concernant les questions liées aux technologies de l'information;
- d'être sélectif et de se concentrer sur des domaines hautement prioritaires ou à haut risque;
- de soutenir les délégués à la protection des données (DPD) et les coordinateurs/points de contact de la protection des données (CPD), qui interviennent en première ligne dans ce domaine au sein des institutions et organes de l'UE.

Ces précieuses contributions nous ont permis de développer nos principes directeurs et de définir un plan d'action détaillé pour la réalisation de nos objectifs stratégiques ainsi qu'une liste d'indicateurs-clés de performances permettant de mesurer le degré de réussite.

La stratégie qui en découle a été adoptée en décembre 2012 sous la forme d'un rapport sur la stratégie pour 2013-2013, intitulé «*Vers un niveau d'excellence en matière de protection des données*». Ce rapport a été publié le 22 janvier 2013 et présenté à un groupe restreint de parties prenantes au sein des institutions de l'UE et de la communauté de la protection des données. Il est désormais disponible sur le site internet du CEPD ainsi qu'une brève séquence vidéo des débats.

Sur la base des suggestions de nos parties prenantes, nous avons revu nos priorités et réaffecté nos ressources afin d'améliorer notre efficacité et notre efficience dans un environnement difficile et en constante mutation.

De gauche à droite: Peter Hustinx, CEPD, Viviane Reding, Vice-Présidente de la Commission européenne, Cecilia Malmström, Commissaire européenne, et Giovanni Buttarelli, Contrôleur adjoint

En agissant de manière sélective et proportionnée, nous chercherons à obtenir que la protection des données fasse partie intégrante de l'élaboration des politiques et du processus législatif dans tous les domaines de compétence de l'UE.

Nous centrerons notre attention et nos efforts sur les domaines politiques ou administratifs où les risques de non-respect des règles de protection des données et les répercussions sur la vie privée sont les plus élevés.

En nous appuyant sur notre expertise, notre autorité et nos pouvoirs officiels, nous entendons sensibiliser l'opinion à la protection des données en tant que droit fondamental et élément essentiel d'une politique publique saine et de la bonne administration au sein des institutions de l'UE.

Nous avons notamment identifié des activités mettant l'accent sur la responsabilisation des décideurs et des responsables du traitement des données, ainsi que des activités reposant sur le rôle crucial des DPD. Ces activités sont des composantes essentielles des réformes législatives proposées et nous espérons qu'elles montreront dans quelle mesure les niveaux de conformité peuvent être rehaussés en ces temps de restrictions budgétaires.

La stratégie adoptée en 2012 est conçue pour optimiser l'impact de notre travail en matière de protection des données à l'échelle de l'UE et augmenter son efficacité en exploitant au mieux les ressources disponibles. Nous allons poursuivre le développement de la stratégie et continuer de viser l'excellence en matière de protection des données au niveau européen au-delà de 2014.

1.2.2 Règlement intérieur

Le règlement intérieur a également été adopté en décembre 2012 sur la base de l'article 46 sous k) du règlement. L'adoption de ce règlement intérieur constitue une étape importante pour le CEPD sur la voie de la maturité en tant qu'institution européenne.

Le règlement intérieur découle du même processus que celui qui a abouti à la conclusion de la révision stratégique. Il définit, en un même document global, l'organisation et les procédures de travail de l'institution. Il repose sur une expérience importante et reflète les pratiques développées au fil des années, notamment à la suite de la réorganisation administrative de 2010.

Ce règlement intérieur vient s'ajouter aux règles définies par le règlement ainsi qu'à d'autres dispositions du droit de l'Union européenne définissant les missions et compétences du CEPD, par exemple le statut des fonctionnaires, le règlement financier et les diverses mesures relatives à la supervision coordonnée.

Ainsi, il rappelle et applique le principe d'indépendance, de bonne gouvernance et de bonne conduite administrative et prévoit les fonctions d'autorité investie du pouvoir de nomination, d'ordonnateur délégué et de comptable.

D'autre part, il fixe des règles détaillées concernant les processus internes de prise de décision, les rôles des contrôleurs et du conseil d'administration, l'organisation et le fonctionnement du secrétariat, la planification, l'administration interne et l'ouverture et la transparence de l'institution. Comme noté ci-dessus, il consacre également les valeurs fondamentales et les principes directeurs définis au cours du processus de révision stratégique.

La majorité des règles concernent les procédures spécifiques à suivre dans le cadre des activités fondamentales de l'institution. Certaines de ces procédures sont déjà décrites dans le règlement proprement dit, comme la procédure de contrôle préalable des opérations de traitement, que le règlement intérieur vient compléter. D'autres règles ne sont pas décrites dans le règlement, ou ne sont décrites que partiellement, comme les règles relatives à la coopération, au soutien des DPD ou encore les règles relatives aux consultations administratives et législatives.

Le règlement intérieur est disponible sur le site internet du CEPD et sera publié au Journal officiel dans toutes les langues officielles de l'UE.

1.2.3 Plan de gestion annuel

L'article 13 du règlement intérieur prévoit que, conformément aux principes de bonne administration et de bonne gestion financière, le CEPD doit établir un plan de gestion annuel (PGA).

Le plan de gestion annuel est le fondement de la planification des activités et de la gestion de la charge de travail. Il complète la planification stratégique à long terme élaborée dans le cadre de la révision stratégique et la planification à court terme menée sur une base hebdomadaire. Un projet pilote lancé en 2012 a montré que, du fait de la nature de notre mission réglementaire et consultative, il n'est pas possible de planifier l'ensemble de notre travail. Contraints par des ressources fixes, nous devons pouvoir adapter notre planning en conséquence. Les leçons tirées de ce projet pilote ont abouti à l'adoption, à la fin de l'année 2012, du premier plan de gestion annuel pour 2013.

Conformément aux mesures et aux objectifs spécifiques définis par la stratégie 2013-2014, le plan de gestion annuel définit les activités à mener en 2013 dans le cadre de chaque objectif spécifique. Pour mesurer les progrès accomplis dans le cadre de la réalisation de nos objectifs, nous mesurerons régulièrement les performances de ces activités.

En outre, au cours de la révision stratégique, nous avons identifié les activités qui jouent un rôle-clé dans la réalisation de nos objectifs et qui constituent par conséquent la base des indicateurs clés de performance (ICP) présentés ci-dessous.

1. nombre d'inspections ou de visites effectuées;
2. nombre d'initiatives de sensibilisation et de formation organisées ou co-organisées au sein des institutions et organes de l'UE;
3. niveau de satisfaction des DPD/CPD par rapport aux formations et aux orientations;
4. nombre d'avis formels et informels formulés à l'endroit du législateur;
5. taux d'exécution des dossiers dans notre inventaire de politiques devant faire l'objet d'une action;
6. nombre d'affaires traitées par le groupe de travail «Article 29» pour lesquelles le CEPD a apporté une contribution écrite importante;
7. nombre d'affaires pour lesquelles des orientations sur les développements technologiques sont fournies;
8. nombre de visites sur le site Web du CEPD;
9. taux d'exécution du budget;
10. taux de mise en œuvre des formations destinées au personnel du CEPD.

Ces indicateurs nous permettront d'évaluer l'impact de notre travail, ainsi que notre niveau d'efficacité quant à l'utilisation des ressources. Ils seront revus régulièrement et adaptés si nécessaire afin d'améliorer nos performances futures. Nous présenterons les premiers résultats à ce sujet dans notre rapport d'activité annuel 2013.

2 SUPERVISION ET MISE EN APPLICATION

Notre objectif stratégique

Promouvoir une «culture de protection des données» au sein des institutions et organes de l'UE de manière à ce qu'ils soient conscients de leurs obligations et assument la responsabilité du respect des exigences relatives à la protection des données

Nos principes directeurs

1. Nous usons de notre expertise et de notre autorité pour exercer nos pouvoirs de supervision et de mise en application. Nous cherchons à garantir la protection des informations à caractère personnel, ainsi qu'un juste équilibre, tout en poursuivant des objectifs politiques plus larges.
2. Dans le cadre de nos activités de supervision et de mise en application:
   - nous reconnaissons que les institutions (responsables du traitement des données, DPD/CPD) endossent une responsabilité de premier plan;
   - nous nous efforçons d'aider les institutions à assumer efficacement leurs responsabilités en veillant à mettre à leur disposition l'assistance, les formations et les conseils appropriés;
   - nous usons de nos pouvoirs de supervision pour renforcer la responsabilité;
   - nous sommes prêts à user de nos pouvoirs d'exécution chaque fois que cela s'avère nécessaire.

2.1. Introduction

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

Tout au long de l'année, nous avons mené à bien nos principales activités de supervision notamment dans le domaine des contrôles préalables, des réclamations et des consultations sur les mesures administratives. Le contrôle préalable des traitements présentant des risques spécifiques est resté un aspect important des activités de supervision du CEPD en 2012. Malgré une diminution du nombre de notifications reçues, il y a eu une légère augmentation du nombre d'avis adoptés (71 avis, dont 14 avis conjoints couvrant 44 notifications). Bien que le nombre des réclamations reçues ait également diminué de 20 %, le nombre des décisions a augmenté (26 dossiers en 2012). Dans le cadre des consultations sur des procédures administratives, le CEPD a adopté une politique en matière de consultations dans le domaine de la supervision et de la mise en application. Ce document a pour objectif de fournir aux institutions et organes de l'Union des orientations relatives aux consultations du CEPD sur la base des articles 28, paragraphe 1, et/ou 46, sous d), du règlement. En 2012, le CEPD a reçu 27 consultations sur des mesures administratives et donné 23 réponses.

Outre nos activités de supervision courantes, nous avons également élaboré d'autres moyens permet-

tant de veiller au respect du règlement conformément à la politique de conformité et d'application adoptée en décembre 2010. Nous avons réalisé deux enquêtes, l'une sur le statut des DPD dans toutes les institutions de l'UE et l'autre sur le statut des coordinateurs de la protection des données au sein de la Commission européenne. Les résultats de ces enquêtes ont été présentés dans des rapports, dont le premier, relatif au statut des DPD, a été publié en décembre 2012. En plus de ce bilan général, nous avons effectué des exercices de contrôle ciblés dans les cas où, à la suite des activités de supervision, nous avions des raisons de nous inquiéter du degré de conformité de certaines institutions ou de certains organes. Ces exercices ont pris la forme d'une correspondance avec l'institution ou l'organe concerné, de visites d'une journée réalisées par l'encadrement aux fins de remédier aux défauts de conformité ou d'inspections visant à vérifier la conformité par rapport à des points spécifiques.

Nous avons également poursuivi nos activités de sensibilisation et d'orientation afin de contribuer à promouvoir une culture de la protection des données au sein des institutions de l'Union européenne. En 2012, ce travail d'orientation a pris la forme de lignes directrices en matière de congé et d'horaire flexible, de formations pour les DPD, d'un atelier pour les responsables du traitement, de la création d'un espace réservé aux DPD sur le site internet du CEPD et d'une ligne d'assistance pour les DPD.

2.2. Délégués à la protection des données

Conformément à l'article 24, paragraphe 1, du règlement, les institutions et organes de l'Union européenne sont obligés de désigner au moins un délégué à la protection des données (DPD). Certaines institutions ont associé à ce DPD un assistant ou un adjoint. La Commission a également nommé un DPD pour l'Office européen de lutte antifraude (l'OLAF, une direction générale de la Commission), compte tenu de la fonction indépendante de celui-ci. Plusieurs institutions ont également nommé des coordinateurs ou contacts de la protection des données (CPD) chargés de coordonner tous les aspects de la protection des données au sein d'une direction ou d'une unité particulière.

En 2012, 11 nouveaux DPD ont été nommés au sein d'institutions et d'organes existants ou au sein des nouvelles agences ou entreprises communes, portant le nombre total des DPD à 58 (le DPD de la Banque centrale européenne fait également office de DPD du Comité européen du risque systémique).

Depuis plusieurs années, les DPD se rencontrent régulièrement afin de partager leurs expériences et d'examiner les questions horizontales. Ce réseau informel a fait la preuve de son efficacité en matière de collaboration, ce qui a continué d'être le cas en 2012.

Un «quatuor de délégués à la protection des données», composé des quatre DPD du Conseil, du Parlement européen, de la Commission européenne et de l'Agence européenne de sécurité des aliments, a été désigné afin de coordonner le réseau des DPD. Le CEPD a étroitement collaboré avec ce quatuor.

Le CEPD a assisté aux réunions que les DPD ont tenues en mars 2012 à l'Agence européenne des produits chimiques (ECHA) à Helsinki et en novembre à la Banque centrale européenne. Nous avons profité de ces réunions pour fournir aux DPD des informations sur nos récents travaux et leur donner un aperçu de l'évolution récente de la protection des données dans l'UE. Cette année, nous nous sommes particulièrement concentrés sur la réforme de la protection des données, sur les évolutions au niveau international, sur la feuille de route du CEPD pour 2012 qui décrit notre activité de supervision pour l'année, sur le rapport relatif au statut des DPD, et sur la révision stratégique du CEPD. Ces réunions ont également été l'occasion de discussions ouvertes entre les DPD et le CEPD concernant des questions et problèmes communs tels que la conservation des informations personnelles dans le cadre des procédures d'évaluation.

En 2012, nous avons organisé plusieurs formations et ateliers pour les DPD et CPD (voir le point 2.7 «Orien-

tations en matière de protection des données»). Des réunions individuelles ont également été organisées entre les membres du personnel et certains DPD en fonction de leurs besoins spécifiques d'orientation.

Les membres de notre unité «Supervision et mise en application» traitent également les questions posées par téléphone par les DPD et, dans la mesure du possible, leur apportent une aide et des conseils immédiats concernant certaines questions particulières. Les questions plus complexes sont traitées dans le cadre de consultations par écrit. Au cours du deuxième semestre de 2012, les membres du personnel du CEPD ont traité plus de 40 demandes par téléphone. En réponse à l'augmentation du nombre des demandes téléphoniques, nous avons mis en place une ligne d'assistance directe pour les DPD, avec un membre du personnel disponible à des heures précises pour répondre aux questions par téléphone. Cette initiative s'est révélée utile, puisqu'elle nous permet de répondre rapidement et de manière informelle aux questions simples et de renforcer la coopération et les relations entre la communauté des DPD et le CEPD.

2.3. Contrôles préalables

2.3.1. Base juridique

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

L'article 27, paragraphe 2, du règlement dresse une liste non exhaustive des traitements susceptibles de présenter des risques. En 2012, le CEPD a continué d'appliquer les critères élaborés au cours des années précédentes[5] lors de l'interprétation de cette disposition, tant pour décider qu'un cas notifié par un DPD ne devait pas faire l'objet d'un contrôle préalable que pour émettre un avis dans le cadre d'une consultation sur la nécessité de procéder à un tel contrôle (voir également le point 2.3.4).

2.3.2. Procédure

2.3.2.1. Notification

Les contrôles préalables doivent être effectués par le CEPD après réception de la notification adressée par le DPD au secrétariat du CEPD au moyen du formulaire standard du CEPD (article 19 du règlement intérieur). Les informations supplémentaires éventuelles concernant l'opération de traitement notifiée doivent être fournies en annexe du formulaire de notification. Si le DPD hésite quant à la nécessité de soumettre un traitement à un contrôle préalable, il peut consulter le CEPD (voir le point 2.3.4).

Les contrôles préalables concernent les traitements qui ne sont pas encore en cours, mais aussi les traitements qui ont commencé avant le 17 janvier 2004 (date de nomination du premier contrôleur et du premier contrôleur adjoint) ou avant l'entrée en vigueur du règlement (contrôles préalables ex post). Dans ces situations, un contrôle dans le cadre de l'article 27 ne peut être «préalable» au sens strict du terme, mais doit être traité a posteriori. Au début des activités du CEPD, il existait un arriéré de dossiers de contrôles préalables ex post concernant des opérations de traitement déjà en place. Il a donc été décidé d'accepter des notifications ex post malgré l'absence de base juridique pour cette pratique. Nous considérons que les institutions et organes de l'Union européenne ont eu suffisamment de temps pour notifier leurs activités de traitement existantes conformément à l'article 27 du règlement, et cette phase touche donc à sa fin.

C'est pourquoi nous avons rappelé aux responsables du traitement de vérifier que toutes les opérations de traitement sensibles ont été notifiées au DPD afin de permettre à celui-ci de notifier le CEPD de tous les contrôles préalables en attente pour la fin du mois de juin 2013.

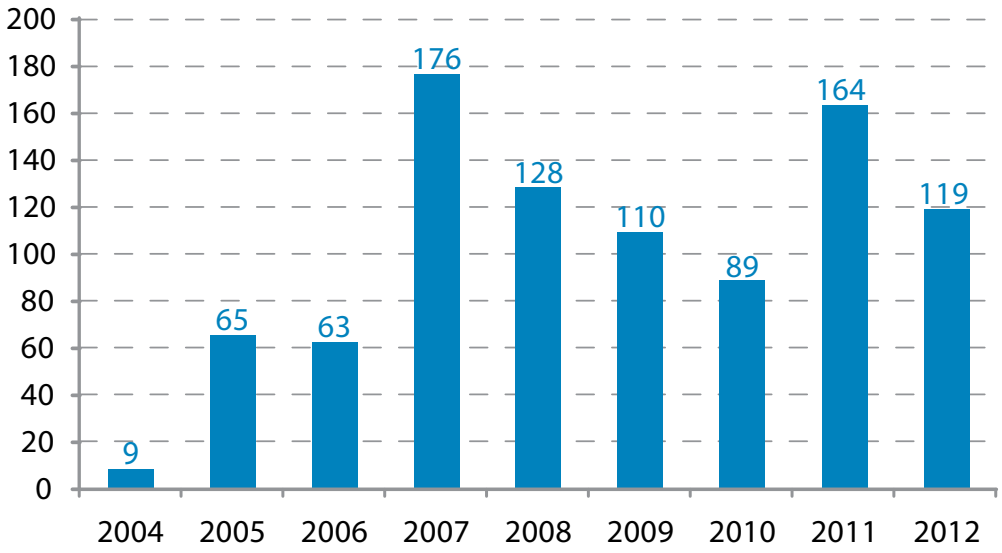
2.3.2.2. Délai, suspension et prolongation

En vertu de l'article 27, paragraphe 4, du règlement et de l'article 21 du règlement interne, le CEPD doit rendre un avis dans un délai de deux mois après réception d'une notification. Ce délai de deux mois peut être suspendu jusqu'à la réception d'informations supplémentaires éventuellement demandées par le CEPD. Lorsque la complexité du dossier le rend nécessaire, ce délai peut également être prolongé pour une nouvelle période de deux mois. Si, au terme du délai de deux mois, éventuellement prolongé, l'avis n'est pas rendu, il est réputé favorable. Jusqu'à présent, ce cas de figure dans lequel l'avis aurait été rendu de manière tacite ne s'est jamais produit. Le délai de deux mois commence à courir le lendemain de la réception du formulaire de notification. Si l'échéance est un jour férié ou un autre jour de fermeture des services du CPED, le jour ouvrable suivant est considéré comme la date ultime à laquelle l'avis doit être rendu.

Avant l'adoption d'un avis, nous sommes tenus d'envoyer le projet d'avis à l'institution concernée pour lui permettre de faire des commentaires sur les aspect pratiques et les inexactitudes factuelles

5 Voir le rapport annuel 2005, point 2.3.1.

Notifications au CEPD



éventuelles. Ces commentaires doivent nous parvenir dans un délai de 10 jours. Ce délai peut être prolongé moyennant une demande motivée par le responsable du traitement. Si aucun commentaire n'est reçu dans les délais, le contrôle préalable adopte l'avis (article 22 du règlement intérieur).

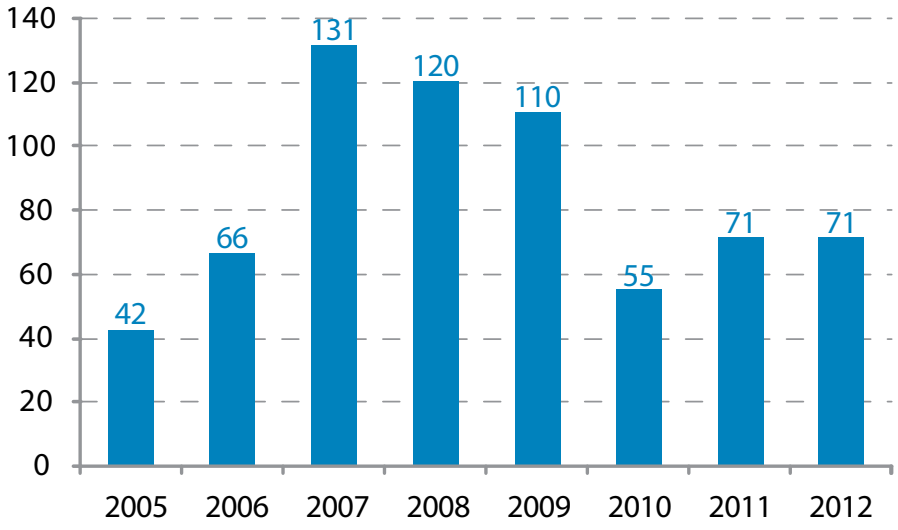
2.3.2.3. Registre

En 2012, nous avons reçu 119 notifications de contrôle préalable (dont 2 ont été retirées). Même si nous sommes venus à bout de l'arriéré des contrôles préalables *ex post* pour la plupart des institutions de l'UE, les traitements mis en place par les agences de l'UE, en particulier les agences récemment créées, le suivi des lignes directrices publiées, ainsi que plusieurs visites à des agences en 2012, ont entraîné une hausse du nombre de notifications.

L'article 27, paragraphe 5, du règlement prévoit que nous devons tenir un registre de tous les traitements qui nous sont notifiés en vue d'un contrôle préalable. Ce registre contient les informations visées à l'article 25 et indique l'échéance de mise en œuvre des recommandations formulées dans nos avis. Par souci de transparence, le registre est publié sur notre site internet (à l'exception des mesures de sûreté, qui ne sont pas mentionnées dans le registre public).

2.3.2.4. Avis

Avis de contrôle préalable du CEPD par an



Conformément à l'article 27, paragraphe 4, du règlement, notre position finale concernant une opération de traitement revêt la forme d'un avis qui est notifié au responsable de cette opération et au délégué à la protection des données de l'institution ou de l'organe. En 2012, nous avons rendu **71 avis de contrôle préalable** et **11 avis sur l'absence de contrôle préalable** (voir le point 2.3.5). Ces chiffres prennent en considération le fait que nous avons traité un nombre important de dossier en rendant des avis conjoints: en 2012, nous avons rendu 13 avis conjoints en réponse à un total de 41 notifications (le point 2.3.2.5 présente une brève explication des avis conjoints).

En 2012, contrairement aux années précédentes où les avis du CEPD étaient fréquemment adressés aux grandes institutions de l'Union européenne (Commission européenne, Parlement européen et Conseil), nous avons adressé la majorité de nos avis à des agences et des organes de l'Union. Les agences de l'UE ont continué de notifier leurs activités principales et leurs procédures administratives standardisées conformément aux procédures pertinentes (voir le point 2.3.2).

Les avis contiennent habituellement une description de la procédure, un résumé des faits et une analyse juridique examinant si le traitement respecte les dispositions applicables du règlement. Si nécessaire, des recommandations sont formulées à l'intention du responsable du traitement en vue de garantir le respect du règlement. Dans ses remarques de conclusion, le CEPD indique généralement que le traitement ne semble pas enfreindre les dispositions du règlement à condition que ces recommandations soient prises en compte, mais il peut bien sûr également exercer d'autres pouvoirs qui lui sont conférés en vertu de l'article 47 du règlement.

Une fois que nous avons rendu notre avis, celui-ci est rendu public. Tous nos avis publiés sont disponibles sur notre site internet en trois versions linguistiques (à mesure de leur disponibilité) avec, dans la plupart des cas, un résumé du dossier.

Un manuel garantit que l'ensemble du personnel adopte la même approche et que nos avis sont adoptés à l'issue d'une analyse complète de toutes les informations pertinentes. Ce manuel comprend un modèle d'avis basé sur l'expérience pratique accumulée et est régulièrement amélioré et mis à jour. Nous utilisons également un système de gestion des tâches pour vérifier que toutes les recommandations relatives à un dossier donné sont mises en œuvre et, le cas échéant, que toutes les décisions sont respectées (voir le point 2.3.6).

2.3.2.5. Procédure applicable aux contrôles préalables ex post dans les agences de l'UE

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

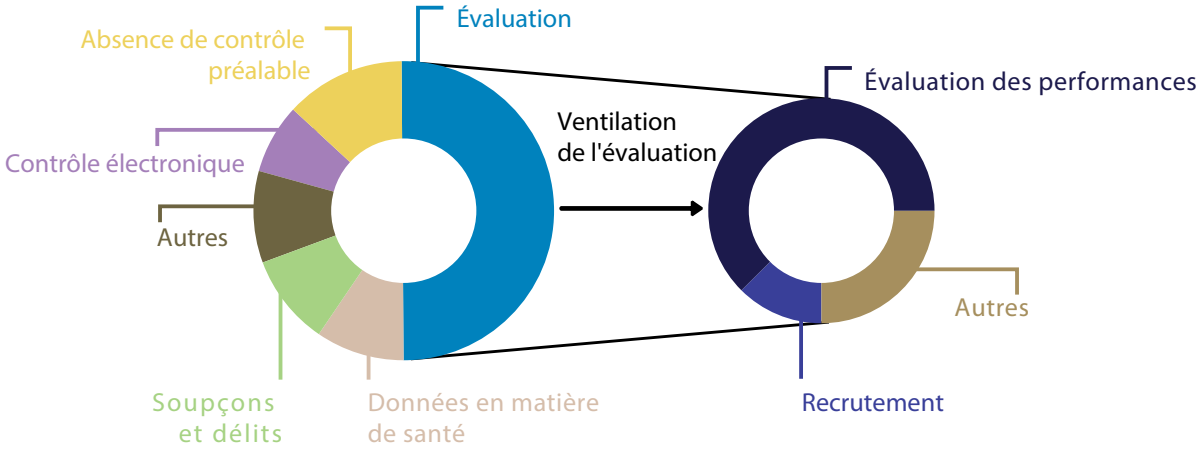
Le thème du premier ensemble de lignes directrices était le **recrutement**, qui a fait l'objet d'un avis horizontal du CEPD en mai 2009, couvrant les notifications de 12 agences. Un deuxième ensemble de lignes directrices a été envoyé aux agences à la fin septembre 2009 concernant le **traitement des données relatives à la santé**, donnant lieu à la publication, en février 2011, d'un avis conjoint sur les traitements de 18 agences dans le domaine des visites d'embauche, des visites annuelles et des congés maladie. En avril 2010, nous avons publié des lignes directrices concernant le traitement des données à caractère personnel dans les **enquêtes administratives et les procédures disciplinaires** par les institutions et organes de l'Union. En juin 2011, le CEPD a rendu un avis conjoint portant sur les traitements en place dans cinq agences. D'autres lignes directrices dans le domaine des **procédures anti-harcèlement** ont donné lieu à l'adoption, en octobre 2011, d'un avis portant sur les notifications reçues par neuf agences.

En juillet 2011, nous avons publié nos lignes directrices concernant **l'évaluation du personnel statutaire** dans le contexte des évaluations annuelles, des périodes probatoires, des promotions ou en ce qui concerne les certifications et attestations. Nous avons adopté une approche différente et adopté, dans la mesure du possible, des avis couvrant les procédures d'évaluation de manière générale pour chaque agence. Depuis la publication de ces lignes directrices, nous avons adopté 24 avis (dont 21 en 2012) sur la base de 48 notifications reçues.

En décembre 2012, nous avons publié des lignes directrices sur la gestion du traitement des informations personnelles en matière de **congé et d'horaire flexible** (sur les orientations thématiques, voir le point 2.7).

2.3.3. Principales questions liées aux contrôles préalables

Avis 2012 par catégorie principale



2.3.3.1. Traitement d'informations personnelles dans le contexte de règlements imposant le gel des actifs dans le cadre de mesures restrictives liées à la politique étrangère et de sécurité commune (PESC)

Le 22 février 2012, nous avons rendu un avis de contrôle préalable concernant le traitement par la Commission des informations personnelles dans le contexte des mesures restrictives prises dans le cadre de la politique étrangère et de sécurité commune. Ces mesures incluent le **gel de fonds**; certaines d'entre elles ont été adoptées au niveau de l'ONU, d'autres au niveau de l'UE. Cet avis décrit la mise en place d'un cadre pour la gestion de ces mesures à long terme.

Afin d'accomplir sa mission en vertu des différentes bases juridiques qui sous-tendent ces mesures, la Commission traite les informations personnelles des personnes visées et de leurs avocats. Ces informations sont utilisées pour correspondre avec les personnes figurant sur les listes, pour une procédure d'examen et pour la publication des listes de sanctions. Ces listes sont publiées au Journal officiel de l'Union européenne et servent de base à une liste consolidée publiée sur l'internet.

Notre avis recommande notamment de **limiter le plus possible le traitement des informations personnelles** aux informations strictement nécessaires pour identifier les personnes figurant sur les listes, d'améliorer le processus d'examen et de fournir de meilleures informations aux personnes reprises sur les listes. Nous recommandons également d'appliquer ces recommandations aux règlements futurs imposant des mesures restrictives.

2.3.3.2. Procédures d'enquête révisées de l'OLAF

Le 3 février 2012, nous avons rendu un avis de contrôle préalable sur les nouvelles procédures d'enquêtes de l'OLAF. Même si les modifications apportées sont principalement d'ordre organisationnel, nous avons rappelé de manière générale les recommandations formulées dans nos avis antérieurs concernant les procédures de l'OLAF et nous avons formulé plusieurs recommandations spécifiques supplémentaires. Nous avons notamment recommandé au responsable du traitement:

- de renforcer **les protections et les garanties** applicables aux catégories de données spéciales dans le cadre des enquêtes;
- d'évaluer la **nécessité et la proportionnalité** des délais actuels de conservation des informations personnelles;
- de transmettre les rapports définitifs des enquêtes internes uniquement sur la base d'une **évaluation concrète de la nécessité de ce transfert**, surtout dans les cas où aucun suivi n'est recommandé;
- de mettre en place un mécanisme efficace permettant de respecter le **droit d'opposition** ou de traiter les réclamations en matière de protection des données formulées dans le contexte d'inspections, de contrôles sur place ou d'analyses criminalistiques d'ordinateurs.

Nous avons également souligné les risques inévitables pour le respect de la vie privée liés à l'analyse criminalistique d'ordinateurs dans les cas où la totalité du disque dur d'un employé fait l'objet d'une copie à des fins d'enquête. C'est pourquoi nous avons demandé à l'OLAF de préparer un rapport d'évaluation concernant la mise en œuvre de son protocole axé sur les aspects liés plus strictement au traitement d'informations en vue d'une révision possible du document et des pratiques actuelles.

Dans le cadre de cette procédure, il est apparu que l'OLAF compte créer une nouvelle base de données interne dont l'objectif est de comparer automatiquement les nouvelles données entrantes aux informations (champs de données) extraites d'autres dossiers. Cette analyse appuierait la procédure de sélection des dossiers et pourrait faciliter les enquêtes ultérieures. Nous avons conclu que cette nouvelle base de données devrait faire l'objet d'une notification et d'un contrôle préalable distincts en raison de ses caractéristiques particulières, et demandé à l'OLAF de suspendre la mise en œuvre et l'utilisation de cette base de données jusqu'à la réalisation du contrôle préalable.

2.3.3.3. Safe Mission Data

La collecte d'informations dans le système «Safe Mission Data» (SMD) du Parlement européen a pour finalité de fournir un soutien aux délégations du Parlement européen en dehors des trois lieux de travail principaux du Parlement dans les situations d'urgence nécessitant une réaction rapide et efficace.

Notre avis du 24 mai 2012 se concentre principalement sur l'une des raisons ayant poussé à créer le SMD: le traitement des données relatives à la santé afin de sauvegarder les intérêts vitaux des personnes concernées. Le traitement de données relatives à la santé est en principe interdit, mais le consentement de la personne concernée est l'une des exceptions autorisant un tel traitement.

Nous avons estimé que cette exception était d'application dans le cas du SMD: les données relatives à la santé sont communiquées volontairement par les personnes concernées au moyen d'un formulaire de collecte, et ce formulaire indique explicitement qu'il n'y a aucune obligation de fournir ces informations. Notre avis souligne également l'importance de garder les données relatives à la santé exactes et à jour.

2.3.3.4. Organisation de réunions du Conseil des chefs d'État ou de gouvernement, de sommets ou de rencontres officielles avec des pays tiers

Le 16 mars 2012, nous avons rendu un avis sur une notification de contrôle préalable reçue du DPD du Conseil de l'Union européenne concernant l'organisation des réunions et des repas des réunions des chefs d'État ou de gouvernement, des sommets ou des réunions officielles avec des pays tiers et du Conseil de l'Union européenne et d'autres réunions au niveau ministériel ou supérieur.

La collecte d'informations personnelles pour ces différentes réunions a pour but de faire en sorte que les participants se voient servir des repas appropriés conformément à leurs prescriptions médicales ou diététiques et dans le respect de leurs convictions religieuses et philosophiques. Le groupe sanguin des chefs de délégation est également noté en cas d'urgence médicale.

Nous avons considéré que le traitement de ces informations était justifié tant que les participants fournissent volontairement les informations relatives à leurs restrictions médicales et diététiques

ainsi que leur groupe sanguin. Pour obtenir ce consentement, le Conseil doit également indiquer aux personnes concernées la raison pour laquelle ces informations sont recueillies. Le traitement du groupe sanguin se justifie également dans la mesure où il est nécessaire à la sauvegarde des intérêts vitaux des personnes concernées.

Enfin, nous avons relevé qu'outre l'importance de la déclaration de respect de la vie privée que le Conseil devrait mettre à la disposition de tous les participants, les membres du personnel du Conseil chargés de recueillir ces informations devraient également signer des déclarations de respect de la confidentialité prévues à cet effet précis.

2.3.3.5. Télétravail – Conseil de l'Union européenne

Le 23 novembre 2012, nous avons adopté un avis sur une notification de contrôle préalable concernant le télétravail reçue du DPD du Conseil de l'Union européenne.

Malgré les doutes sur la nécessité de soumettre le télétravail à un contrôle préalable, le CEPD a considéré que l'opération de traitement concernée devait faire l'objet d'un contrôle préalable en ce qui concerne l'évaluation et la sélection des membres du personnel qui peuvent y avoir droit (article 27, paragraphe 2, point b)). Dans certains autres cas, il se peut que des données relatives à la santé soient traitées, ce qui peut également justifier un contrôle préalable par le CEPD (article 27, paragraphe 2, point a)).

L'opération de traitement en question concerne le traitement des demandes à l'issue d'un appel à manifestations d'intérêt pour le télétravail (soutien administratif à la procédure de sélection des participants) et le suivi administratif du télétravail. Le responsable du traitement procède donc à une évaluation au sens de l'article 27, paragraphe 2, point b).

Notre avis prend en considération les recommandations formulées dans le cadre du projet-pilote de télétravail approuvé par le CEPD, à savoir que le Conseil doit communiquer toutes les conclusions et modifications mises en œuvre à la fin du projet-pilote avant la mise en œuvre à grande échelle du télétravail, il doit inclure la motivation des candidats au télétravail dans ses critères d'évaluation, et il doit traiter uniquement les informations nécessaires aux fins du télétravail.

2.3.3.6. Déclarations annuelles d'intérêts

Le Centre européen de prévention et de contrôle des maladies (CEPCM) a notifié au CEPD une procédure mise en place pour sauvegarder son indépendance par rapport à l'industrie, notamment dans l'élaboration d'avis, d'orientations, de conseils et de recommandations concernant les menaces émergentes pour la santé que représentent les maladies infectieuses.

Un système de déclarations annuelles d'intérêts (DAI) et de déclarations spécifiques d'intérêts (DSI) a été mis en place pour les membres du conseil d'administration et du forum consultatif ainsi que pour tous les experts, les experts nationaux détachés et les membres du personnel (à partir du grade AST 5).

Dans notre avis du 19 juillet 2012, nous avons recommandé que le CEPCM examine minutieusement la façon dont il préserve l'équilibre entre deux droits fondamentaux, à savoir le respect de la vie privée et l'accès public aux documents, en justifiant la nécessité d'étendre la procédure des déclarations d'intérêts (DI) à tous les membres de son personnel, et de clarifier la politique en matière de publication des DI et le caractère potentiellement public des informations recueillies via les DSI.

En ce qui concerne la publication des DAI et la divulgation publique possible des DSI, nous avons également recommandé au CEPCM d'agir de manière proactive, par exemple en informant les personnes concernées et en demandant leur consentement avant la divulgation publique possible des DSI en cas de demande et en leur faisant prendre conscience de leurs droits au titre des règlements relatifs à la protection des données et à l'accès public.

Dans sa lettre de suivi, le CEPCM a justifié l'utilisation des DI pour tous les membres du personnel par leur participation possible à des comités d'évaluation et des panels scientifiques. En ce qui concerne la publication des DI, la politique du CEPCM a été actualisée et le droit d'opposition a été inclus dans les informations adressées aux personnes concernées.

2.3.3.7. Contrôle de l'internet au CEDEFOP (traitement de données en rapport avec un système de proxy)

Le 15 novembre 2012, nous avons rendu un avis concernant le contrôle de l'utilisation de l'internet au Centre européen pour le développement de la formation professionnelle (CEDEFOP).

Nous avons approuvé la méthode adoptée par le CEDEFOP pour contrôler l'utilisation de l'internet, qui repose sur les piliers de la transparence et de l'information préalable, sur une approche progressive du contrôle électronique et sur les droits des membres du personnel.

Nous nous réjouissons en particulier que le CEDEFOP ait fixé un seuil général d'identification d'utilisation excessive de l'internet et défini une méthodologie permettant aux membres du personnel de contrôler en temps réel leur niveau d'utilisation de l'internet.

Nous avons souligné la nécessité de modifier certains aspects des activités du traitement. Parmi d'autres recommandations, nous avons conseillé au CEDEFOP de mettre en place des garanties techniques afin de limiter le plus possible, et uniquement aux cas où il est réellement inévitable, le traitement accidentel de catégories spéciales d'informations (sans lien avec l'enquête). Dans ces cas, ces informations ne doivent pas être enregistrées ni traitées plus en profondeur aux étapes suivantes de la procédure. En outre, le CEDEFOP doit informer individuellement les utilisateurs, par exemple en leur envoyant par courrier électronique la politique en matière d'internet et la déclaration de confidentialité.

2.3.4. Consultations concernant la nécessité d'un contrôle préalable

En cas de doute, les institutions et les organes de l'UE peuvent consulter le CEPD quant à la nécessité d'un contrôle préalable en vertu de l'article 27, paragraphe 3, du règlement. En 2012, nous avons reçu 8 consultations de ce type de la part de DPD.

2.3.4.1. Enquête de satisfaction du personnel à l'Agence européenne pour la compétitivité et l'innovation

L'Agence exécutive pour la compétitivité et l'innovation (EACI) a soumis une notification relative à son enquête sur la satisfaction de ses employés au travail parce que les opérations de traitement effectuées dans le cadre de cette étude devaient inclure une évaluation de la hiérarchie et de l'EACI par les membres du personnel relevant de l'article 27, paragraphe 1, du règlement.

Dans notre réponse du 19 octobre 2012, nous avons conclu que ce traitement ne devait pas faire l'objet d'un contrôle préalable. En outre, même si, en d'autres circonstances, le traitement de certaines réponses des membres du personnel pourrait être considéré comme un traitement d'informations personnelles en matière de santé, dans ce cas précis, plusieurs mesures de précaution (le fait que les membres du personnel ne sont pas obligés de participer, l'utilisation de données agrégées pour

l'analyse, la publication de résultats généraux uniquement, etc.) ont été prises.

Nous avons néanmoins formulé différentes recommandations afin de garantir la mise en œuvre correcte du règlement, parmi lesquelles des recommandations relatives à la conservation des données brutes dans l'outil utilisé pour réaliser l'enquête de satisfaction, des modifications à apporter à la déclaration de confidentialité, la notification au personnel de la base juridique du traitement et la méthode de compilation des informations agrégées.

2.3.5. Notifications non soumises au contrôle préalable ou retirées

À l'issue d'une analyse minutieuse, il a été conclu que huit dossiers ne devaient pas faire l'objet d'un contrôle préalable en 2012. Dans ces situations («traitements non soumis à un contrôle préalable»), le CEPD peut malgré tout faire des recommandations. Par ailleurs, deux notifications ont été retirées et une notification a été remplacée.

2.3.5.1. Horaire flexible et application Matrix à la FRA

Le 12 avril et le 12 septembre 2012, nous avons conclu que deux notifications reçues de l'Agence des droits fondamentaux (FRA) concernaient des opérations non soumises à un contrôle préalable dans le contexte des horaires flexibles et de l'application Matrix. Ces deux notifications étaient liées, dans la mesure où elles concernaient toutes deux le système de gestion de l'information de l'Agence (appelé Matrix).

Nous avons conclu que les opérations de traitement relatives aux horaires flexibles n'étaient pas soumises à un contrôle préalable parce que ces traitements n'avaient pas pour objet d'évaluer l'efficacité, les compétences ou l'aptitude au travail des membres du personnel. Nous avons néanmoins formulés différentes recommandations afin de faire en sorte que le traitement des données respecte pleinement le règlement. Nous avons demandé à l'agence d'indiquer plus clairement dans sa procédure que les opérations de traitement étaient sans aucun lien avec l'évaluation des performances. Nous avons également recommandé que l'agence adopte une note d'information à l'intention des membres du personnel et apporte la preuve que cette note leur avait été communiquée.

En ce qui concerne la notification relative aux opérations de traitement des applications Matrix, le CEPD a conclu qu'au titre du règlement, il n'y a avait pas lieu de soumettre les opérations de traitement effectuées dans l'application Matrix à un contrôle préalable. Ces opérations de traitement n'ont pas pour objet d'évaluer des personnes, mais d'évaluer l'état d'avancement des projets et les progrès accomplis par l'Agence dans son ensemble vers la réalisation des objectifs de son programme annuel.

Le CEPD a recommandé à l'Agence de réexaminer la nécessité de sa politique de conservation des données enregistrées dans le système Matrix. Nous avons également recommandé à l'Agence de rendre les données à caractère personnel anonymes, dès qu'elles ne sont plus nécessaires à la gestion des projets dans le contexte du cadre pluriannuel, et de communiquer au CEPD la période de conservation révisée. Enfin, nous avons invité l'Agence à adopter une note d'information à l'intention des membres du personnel et d'apporter la preuve que cette note leur avait été communiquée.

2.3.5.2. Enquête du PE sur l'équilibre entre travail et vie privée pour les députées

Le CEPD a été consulté sur la nécessité de soumettre à un contrôle préalable une enquête portant sur l'équilibre entre travail et vie privée pour les femmes députées au Parlement européen (PE). Le 23 octobre 2012, nous avons conclu que les opérations de traitement concernées ne seraient pas soumises à un contrôle préalable.

Ce traitement de données avait pour finalité d'identifier les liens entre le travail et la vie privée des députées et de recueillir des informations sur les mesures que l'administration pourrait prendre pour faciliter leur travail au PE.

La principale base juridique d'un contrôle préalable aurait pu être l'article 27, paragraphe 2, point a) (traitement potentiel de certaines données relatives à la santé). La conclusion de non-contrôle préalable repose sur une analyse des mesures prises afin d'atténuer les risques décrits à l'article 27, paragraphe 2, point a) du règlement. Nous avons tenu compte du fait que ce traitement n'a pas pour objet de traiter des données relatives à la santé, mais de tirer des conclusions statistiques sur la base de données agrégées. En outre, une déclaration de confidentialité informait les députées européennes qu'elles n'étaient pas tenues de participer à cette enquête, qu'elles pouvaient décider de ne pas répondre à certaines questions et que le traitement se limiterait aux informations nécessaires.

Dans nos recommandations, nous avons suggéré que le PE établisse une distinction entre le stockage des questionnaires individuels et l'enregistrement des données agrégées, la finalité du traitement étant d'utiliser les informations sous forme agrégée afin de tirer des conclusions statistiques, et de conserver les réponses individuelles pendant une très courte période. Nous avons également demandé au PE de compléter son projet de formulaire de consentement afin de respecter les articles 11 et 12 du règlement.

2.3.6. Suivi des avis de contrôle préalable

*Le CEPD conclut généralement ses avis de contrôle préalable en indiquant que le traitement ne semble pas enfreindre les dispositions du règlement, à condition que certaines **recommandations** soient prises en considération. Des recommandations sont également formulées lorsque le CEPD examine un dossier afin de vérifier la nécessité d'un contrôle préalable et lorsque certains aspects essentiels semblent nécessiter des rectifications. Une fois l'avis rendu, le CEPD accorde aux institutions concernées un délai de trois mois pour rendre compte de la mise en œuvre des recommandations contenues dans cet avis. 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.*

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

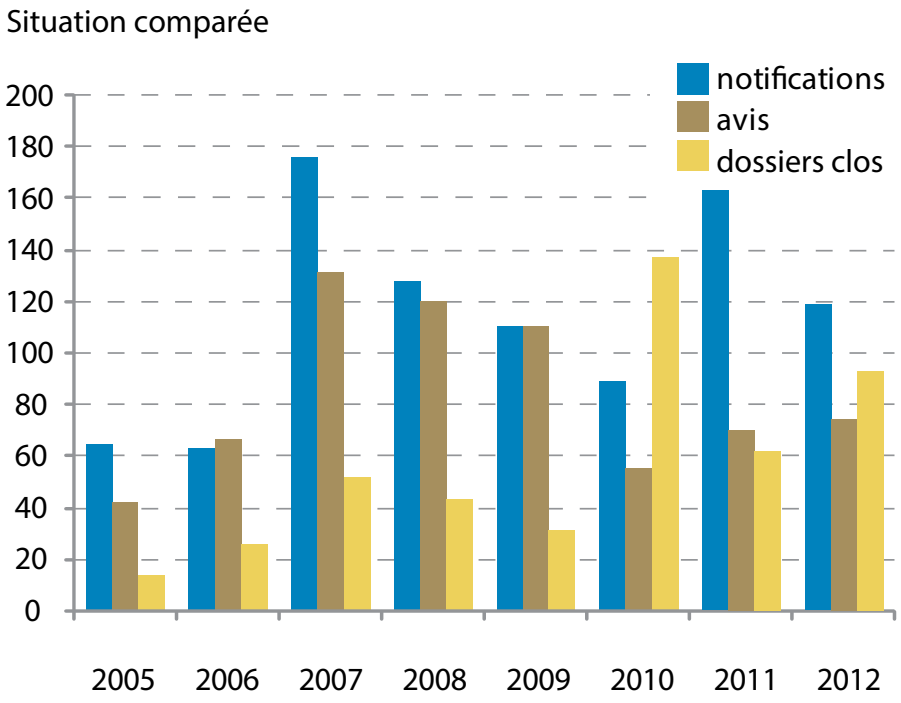
Nous considérons ce suivi comme un **élément fondamental du respect intégral** du règlement. Conformément à notre document stratégique de 2010 intitulé «Contrôler et garantir le respect du règlement (CE) n° 45/2001», nous attendons des institutions et des organes qu'ils se montrent **responsables** des recommandations éventuellement formulées. Cela signifie qu'ils sont chargés de les mettre en œuvre, et qu'ils doivent pouvoir nous en apporter la preuve. Toute institution ou tout organe qui ne donne pas suite à ces recommandations s'expose donc à une mesure formelle d'exécution.

2.3.7. Conclusions

Les 71 avis de contrôle préalable formulés ont jeté une lumière précieuse sur les traitements des administrations européennes et nous ont permis de formuler des recommandations qui protègeront de manière uniforme le droit fondamental des personnes à la protection de leurs données à caractère personnel. L'importance de cette activité réside dans le fait qu'elle nous permet de vérifier la conformité avec les règles de protection des données avant la mise en place de l'activité de traitement.

Ce contrôle est effectué en cas de présence de risques spécifiques identifiés selon les critères définis par le règlement. Cette approche sélective de notre fonction de supervision nous permet de nous focaliser sur les cas susceptible de représenter un danger pour les droits fondamentaux et de jouer ainsi un rôle préventif et de précaution.

Les dossiers de contrôle préalable traités en 2012 nous ont permis de garantir le respect de bon nombre d'aspects intrinsèques de la protection des données à caractère personnel, comme la réduction des données au minimum, la prise en considération



du respect de la vie privée dès la conception, la proportionnalité, etc. Nous continuerons de fournir ces orientations aux institutions et agences et de faciliter le processus de notification des agences.

Concernant le suivi de nos avis de contrôle préalable, 92 dossiers ont été clos en 2012. Nous continuerons de contrôler et de suivre de près nos recommandations afin de faire en sorte que les institutions et agences les intègrent en temps utile et de façon satisfaisante.

2.4. Réclamations

2.4.1. Le mandat du CEPD

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

En principe, une personne ne peut présenter une réclamation que pour une violation présumée de ses droits en matière de protection des informations personnelles. Cependant, le personnel de l'UE peut se plaindre de toute violation présumée des règles en matière de protection des données, que le plaignant soit directement touché par le traitement ou pas. Le statut des fonctionnaires de l'Union européenne permet également de soumettre une réclamation au CEPD (article 90 ter).

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

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

Une réclamation au CEPD ne peut avoir trait qu'au traitement d'informations personnelles. Le CEPD n'est pas compétent pour traiter les cas de mauvaise administration, pour modifier le contenu des documents que le plaignant souhaite contester ou pour octroyer des dommages et intérêts.

Le responsable d'un institut de recherche qui avait contribué à un projet de recherche géré par une institution de l'UE s'est plaint du résultat d'un audit effectué sur ce projet. Le service d'audit de l'institution qui avait financé le projet a jugé que certaines dépenses du plaignant n'étaient pas justifiées et a demandé leur remboursement. Au cours de cet audit, certaines informations personnelles ont été traitées par les auditeurs. Le plaignant a considéré que l'audit était illégal parce que les personnes concernées n'avaient pas consenti au traitement de leurs informations personnelles. Le CEPD n'a pas suivi le raisonnement du plaignant, parce que le traitement d'informations personnelles à l'occasion d'un audit repose sur une autre base juridique que le consentement de la personne concernée. C'est pourquoi aucune enquête relative à la réclamation n'a été lancée dans ce dossier.

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

Un ressortissant britannique a déposé une réclamation auprès du CEPD à la suite du refus, par l'autorité autrichienne chargée de la protection des données, de traiter sa réclamation en anglais plutôt qu'en allemand. Le plaignant a demandé au CEPD d'ordonner à l'autorité autrichienne de traiter sa réclamation en anglais ou de traduire la réclamation et ses annexes en allemand. Nous avons informé le plaignant que le CEPD n'est pas compétent pour superviser les autorités nationales de protection des données et n'est pas en mesure de proposer des services de traduction aux citoyens qui se heurtent à des obstacles linguistiques dans l'exercice de leurs droits dans différents États membres.

2.4.2. Procédure de traitement des réclamations

Le CEPD examine les réclamations en vertu du cadre juridique en vigueur, du règlement intérieur du CEPD, des principes généraux du droit de

l'Union européenne et des bonnes pratiques administratives communes aux institutions et organes de l'UE.

À tous les stades du traitement de la réclamation, et conformément à l'article 33 du règlement intérieur, le CEPD respecte les principes de proportionnalité et d'équité. Guidé par les principes de transparence et de non-discrimination, il prend les mesures appropriées en tenant compte:

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

En février 2011, nous avons actualisé notre procédure de dépôt des réclamations en créant un **formulaire en ligne de dépôt de plainte** interactif sur notre site internet. Ce formulaire aide les plaignants à évaluer la recevabilité de leur réclamation, et donc à ne soumettre au CEPD que des cas pertinents. Il nous permet également d'analyser des informations plus complètes et pertinentes afin d'accélérer le traitement des réclamations et de réduire le nombre des réclamations manifestement irrecevables. Le formulaire existe en anglais, en français et en allemand. Depuis septembre 2011, si une réclamation est reçue par courrier électronique dans l'une de ces langues, le plaignant est invité à remplir le formulaire en ligne. Cette mesure a réduit d'environ 38 % le nombre des réclamations irrecevables reçues en 2012.

La réclamation doit identifier la personne dont elle émane. Elle doit être déposée par écrit dans une langue officielle de l'Union et fournir toutes les informations nécessaires pour comprendre son objet. Le CEPD examine attentivement chaque réclamation qu'il reçoit. L'examen préliminaire de la réclamation est spécifiquement destiné à vérifier si cette dernière remplit les conditions d'ouverture d'une enquête et s'il existe des éléments suffisants pour justifier l'ouverture d'une enquête.

Notre **manuel interne** a été conçu pour mettre des orientations en matière de traitement des réclamations à la disposition de notre personnel. Ce manuel a été mis à jour en septembre 2011 afin de refléter les modifications apportées à notre structure organisationnelle et d'intégrer les récents développements dans la pratique du traitement des réclamations. Nous avons également mis en place un **outil statistique** conçu pour examiner les activités liées aux réclamations, et en particulier pour suivre l'évolution de certains dossiers.

Une réclamation dont l'objet ne relève pas de notre **compétence juridique** est déclarée irrecevable et le plaignant en est informé. Le cas échéant, nous informons également le plaignant des autres organes compétents (par exemple le tribunal, le Médiateur, les autorités nationales chargées de la protection des données, etc.) auxquels il peut soumettre sa réclamation.

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

Un citoyen de l'Union a été informé que ses informations personnelles apparaissaient sur une liste, gérée par une institution de l'Union européenne, de personnes et d'entreprises interdites de participation aux procédures publiques d'appel d'offres. Il a porté plainte auprès du CEPD parce qu'il n'avait pas été informé par cette institution des raisons pour lesquelles il avait été porté dans cette liste. Nous lui avons fait savoir que sa réclamation auprès du CEPD ne serait recevable que si l'institution traitant ses informations personnelles n'avait pas répondu à une requête expresse de sa part. Il devait donc tout d'abord soumettre sa requête à l'institution concernée et ne contacter le CEPD que si l'accès à ces informations ne lui était pas accordé dans les délais fixés par les règles en matière de protection des données.

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

Un membre du personnel d'une institution de l'UE a introduit une réclamation auprès du CEPD concernant la communication de ses rapports médicaux à d'autres membres du personnel dans le contexte d'une procédure administrative. Après le lancement d'une enquête par le CEPD sur cette réclamation, le plaignant a intenté une action devant le Tribunal de la fonction publique portant en partie sur les mêmes faits. Le CEPD a décidé de suspendre son enquête jusqu'à l'arrêt du Tribunal. Étant donné la gravité de la violation alléguée des règles de protection des données, le CEPD a décidé d'intervenir à l'appui du plaignant devant le Tribunal.

Si la question est déjà examinée par un organe administratif, par exemple si une enquête interne par l'institution concernée est en cours, la réclamation est en principe encore recevable. Nous pouvons toutefois décider, sur la base des éléments particuliers du dossier, d'attendre l'issue de ces procédures administratives avant de commencer notre enquête. À l'inverse, si la même question (ou les mêmes circonstances factuelles) fait déjà l'objet d'un examen par un tribunal, la réclamation est déclarée irrecevable.

Pour assurer le traitement cohérent des réclamations concernant la protection des données et éviter toute redondance inutile, le **Médiateur européen** et le CEPD ont signé un mémorandum d'accord en novembre 2006. Si une réclamation portant sur les mêmes faits a déjà été déposée auprès du Médiateur européen, le CEPD examine sa recevabilité à la lumière de ce mémorandum d'accord. Le mémorandum d'accord stipule entre autres qu'une réclamation qui a déjà été examinée ne peut être rouverte par une autre institution, sauf si des éléments nouveaux importants sont apportés.

L'article 32, paragraphe 3, de notre règlement intérieur fixe un **délai à respecter** pour le dépôt d'une réclamation. Une plainte doit en principe être introduite dans les deux ans qui suivent la date à laquelle la personne qui dépose la plainte a appris les faits sur lesquels elle se fonde.

Si une réclamation est recevable, nous ouvrirons **une enquête** dans la mesure nécessaire. Cette enquête peut inclure une demande d'informations à l'institution concernée, un examen des documents pertinents, une réunion avec le responsable du traitement ou une inspection sur place. Le CEPD a compétence pour obtenir de l'institution ou de l'organe concernés l'accès à toutes les informations personnelles et à toutes les informations nécessaires à l'enquête. Nous pouvons également avoir accès à tous les locaux dans lesquels un responsable du traitement, une institution ou un organe exerce ses activités.

À la fin de l'enquête, une **décision** est envoyée au plaignant ainsi qu'au responsable du traitement des données. Dans sa décision, le CEPD exprime son avis sur une éventuelle violation des règles de protection des données par l'institution concernée. La **compétence du CEPD est vaste**, allant du conseil aux personnes concernées à l'interdiction du traitement ou la saisine de la Cour de justice, en passant par un avertissement ou une admonestation au responsable du traitement.

Toute partie intéressée peut demander une **révision** de la décision du CEPD. La demande de révision doit être introduire dans un délai d'un mois à partir de la date de réception de la décision et ne peut porter que sur des éléments ou des arguments juridiques nouveaux que nous n'avons pas encore pris en considération. Indépendamment de la possibilité de demander une révision de notre décision, celle-ci peut également être contestée devant la Cour de justice de l'Union européenne conformément aux conditions fixées à l'article 263 du traité sur le fonctionnement de l'Union européenne.

Aucune décision du CEPD n'a fait l'objet d'une contestation devant la Cour en 2012.

2.4.3. Confidentialité garantie aux plaignants

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

Généralement, les réclamations sont traitées de manière confidentielle. Le **traitement confidentiel** signifie que les informations personnelles sont utilisées uniquement par nous pour le traitement des réclamations. Toutefois, pour le déroulement correct de l'enquête, il est généralement nécessaire d'informer les services de l'institution concernée et les tierces parties impliquées du contenu de la réclamation et de l'identité du plaignant. Conformément à l'article 33, paragraphe 3, de notre règlement, le CEPD ne divulgue le contenu d'une réclamation et l'identité du plaignant que dans la mesure nécessaire au bon déroulement de l'enquête. Nous envoyons également une copie de notre correspondance avec l'institution au délégué à la protection des données (DPD) de ladite institution.

Si le plaignant exige l'**anonymat** envers l'institution, le DPD ou les tiers concernés, il est invité à en expliquer les raisons. Nous analysons ensuite les arguments du plaignant et examinons les conséquences pour la viabilité de notre enquête future. Si nous estimons que l'anonymat du plaignant ne s'impose pas, nous expliquons pourquoi et demandons au plaignant s'il accepte que nous examinions la réclamation sans garantir l'anonymat ou s'il préfère retirer sa réclamation.

Si le plaignant décide de retirer sa réclamation, l'institution concernée ne sera pas informée de l'existence de cette dernière. Dans ce cas, nous pouvons entreprendre d'autres actions en la matière sans révéler à l'institution concernée l'existence de la réclamation, comme une enquête d'initiative ou une demande de notification d'un traitement de données.

Au cours et au terme d'une enquête, nous ne divulguons à des tiers **aucun document relatif à la réclamation**, en ce compris la décision finale, à moins qu'une obligation légale nous l'impose. Nous pouvons publier des informations relatives à la réclamation sur notre site internet ou dans notre rapport annuel sous une forme ne permettant pas d'identifier le plaignant ou d'autres parties impliquées.

2.4.4. Réclamations traitées en 2012

2.4.4.1. Nombre des réclamations

Le CEPD a reçu **86** réclamations en 2012, une **diminution** d'environ 20 % par rapport à 2011, ce qui confirme l'efficacité du **formulaire de dépôt de réclamation en ligne** pour réduire le nombre des réclamations irrecevables. Sur ce total, **46 réclamations ont été jugées irrecevables** d'emblée, la majorité portant sur un traitement au niveau national, et pas au niveau d'une institution ou d'un organe de l'UE.

Les 40 réclamations restantes ont nécessité une enquête approfondie (une hausse de 54 % par rapport à 2011). De plus, 15 réclamations recevables déposées les années précédentes (quatre en 2009, trois en 2012 et huit en 2011) en étaient toujours à la phase de l'enquête, de l'examen ou du suivi au 31 décembre 2012.

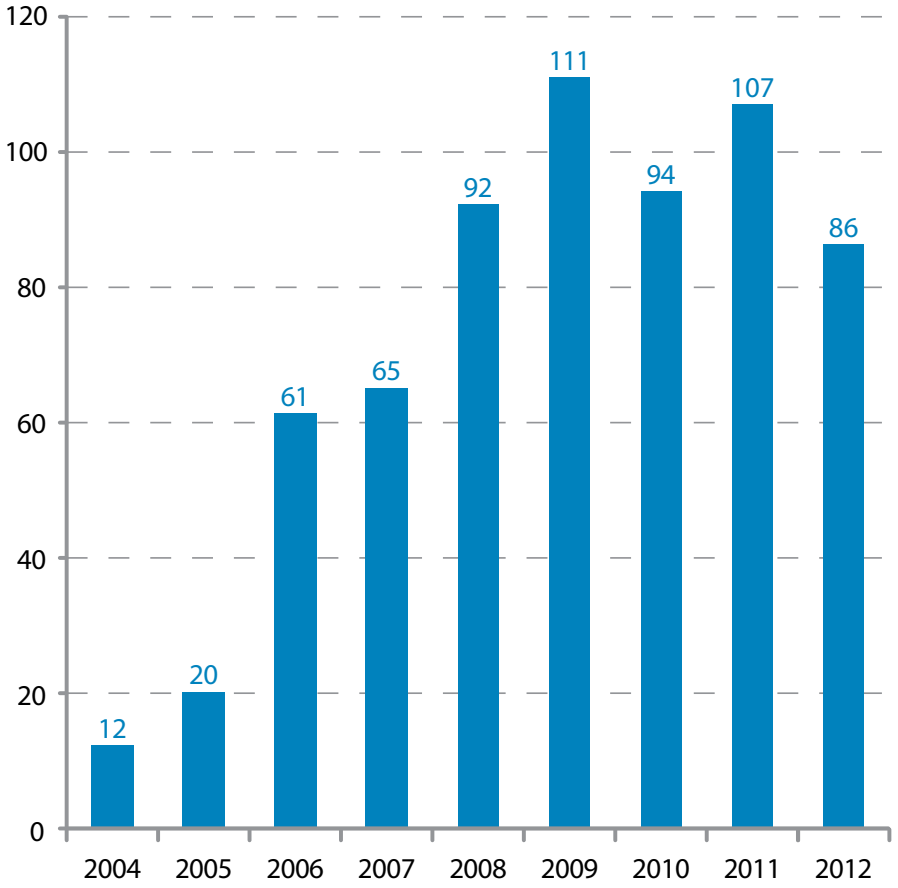
2.4.4.2. Nature des plaignants

Sur les 86 réclamations déposées, 20 (23 %) ont été soumises par des membres du personnel des institutions ou organes de l'UE, y compris des anciens membres et des candidats à un emploi. En ce qui concerne les 66 autres réclamations, le plaignant ne semblait pas avoir de lien professionnel avec l'administration de l'UE.

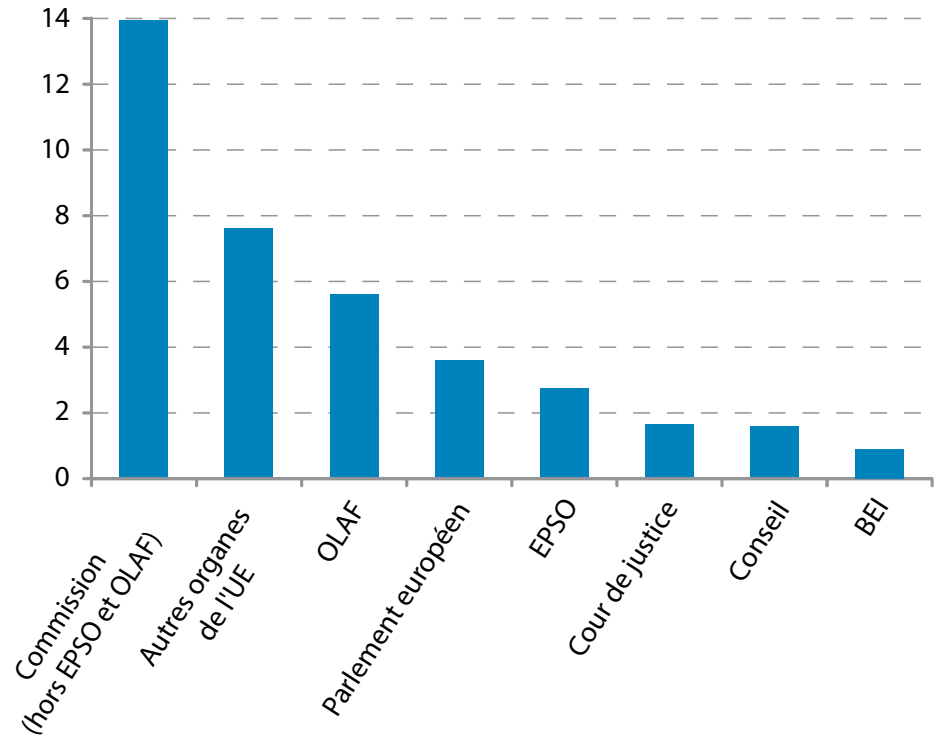
2.4.4.3. Institutions et nombre de réclamations

Sur les 40 réclamations recevables déposées en 2012, la plupart étaient dirigées contre la **Commission européenne, le Parlement européen, l'OLAF et l'EPSO**. Cette situation est prévisible dans la mesure où la Commission et le Parlement traitent plus d'informations personnelles que les autres institutions et organes de l'UE. Le nombre relativement élevé de réclamations concernant l'OLAF et l'EPSO peut s'expliquer par la nature des activités exercées par ces organes.

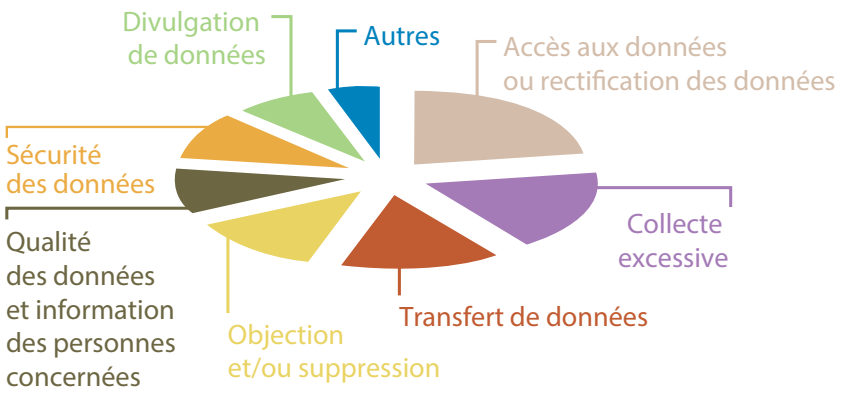
Nombre de réclamations reçues



Institutions et organes de l'UE concernés



Types de violations invoqués



2.4.4.4. Langue des réclamations

La majorité des réclamations ont été déposées en anglais (69 %), en français (13 %) ou en allemand (8 %). Les réclamations dans d'autres langues sont relativement rares (10 %).

2.4.4.5. Types de violations invoqués

Les violations des règles en matière de protection des données alléguées par les plaignants en 2012 concernaient principalement :

- Une atteinte aux droits des personnes concernées, comme les droits d'accès ou de rectification des données (23 %) ou le droit d'objection et de suppression (13 %);
- Une collecte excessive d'informations personnelles (18 %), des transferts de données (15 %), la qualité des données et l'information des personnes concernées (10 %), la sécurité des données (10 %) ou la divulgation des données (8 %).

2.4.4.6. Résultats des enquêtes du CEPD

Dans 26 affaires résolues courant 2012, le CEPD a conclu qu'il n'y avait pas eu violation des règles de protection des données ou que le responsable du traitement des données avait adopté les mesures nécessaires au cours de l'enquête du CEPD.

Le CEPD a reçu une plainte concernant la mise à la disposition de tous les membres du personnel de certains dossiers du comité du personnel d'un organe de l'UE. Le CEPD a conclu qu'il n'y avait aucune preuve de violation flagrante des règles en matière de protection des données justifiant une enquête plus approfondie dans ce dossier. Le CEPD a par conséquent clos le dossier.

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

Le CEPD a reçu une réclamation affirmant qu'un organe de l'UE avait communiqué le nom d'un informant membre du personnel d'une institution de l'Union européenne à la hiérarchie de cet informant. À la suite d'une enquête dans cette affaire, le CEPD a conclu que la divulgation de l'identité de l'informant constituait une divulgation non autorisée d'informations personnelles en violation de l'article 22 du règlement.

Dans une affaire, les allégations communiquées au CEPD dans le contexte d'une réclamation ont entraîné la décision par celui-ci de lancer une inspection plus large dans les locaux de l'institution européenne concernée.

2.5. Contrôle du respect du règlement

*Le CEPD est chargé d'assurer le suivi et de **veiller à l'application du règlement (CE) n° 45/2001**. Le contrôle prend la forme **d'enquêtes générales** périodiques. En plus de ce **bilan d'ensemble**, nous avons également effectué **des contrôles ciblés** dans les cas où, à la suite de nos activités de supervision, nous avions des raisons de nous inquiéter du degré de conformité aux normes de certaines institutions ou certains organes. Ces contrôles ont pris la forme d'une **visite** d'une journée de l'organe concerné aux fins de remédier aux défauts de conformité. Enfin, des **inspections** ont été opérées dans certaines institutions et certains organes pour vérifier leur respect du règlement concernant des questions spécifiques.*

2.5.1. Exercice général de contrôle et de compte rendu : rapport sur le statut des délégués à la protection des données et enquête sur le rôle de coordinateur de la protection des données

Dans notre document stratégique de décembre 2010, le CEPD annonce qu'il «*continuera de mener des 'enquêtes' périodiques afin de s'assurer qu'il dispose d'un aperçu représentatif du respect de la protection des données au sein des institutions ou organes de l'Union, et qu'il peut fixer des objectifs internes appropriés pour traiter ses constatations*».

Nous avons été un fervent défenseur de la fonction de DPD dans l'administration de l'UE. C'est pourquoi, en mai 2012, nous avons lancé une enquête consacrée au délégué à la protection des données (DPD) afin de contrôler la conformité des institutions et organes de l'UE avec l'article 24 du règlement. Le train de réformes des règles européennes en matière de protection des données actuellement débattu par le législateur européen reconnaît également l'importance de la fonction de DPD.

Basée sur un questionnaire, cette enquête portait principalement sur le mandat, la position et les ressources (temps, soutien et formation) des DPD afin de recueillir des informations homogènes sur la situation et l'évolution du rôle de DPD. Les conclusions de cet exercice ont été rassemblées dans un rapport. Les réponses ont été présentées dans trois tableaux comparatifs, par groupes d'institutions et d'organes, afin de permettre les comparaisons.

Dans les conclusions, nous saluons la désignation d'un DPD par la plupart des institutions et organes de l'UE, le respect général d'une durée de mandat située entre deux et cinq ans, l'expérience déjà engrangée au sein du réseau des DPD, l'association d'une majorité de DPD au chef de l'institution ou organe concerné, et l'existence d'un personnel de soutien important pour de nombreux DPD.

Mais ce rapport révèle également plusieurs points préoccupants. Nous allons notamment surveiller de près la durée effective du mandat des DPD qui font partie du personnel contractuel, la rotation élevée des DPD, les conflits d'intérêts possibles, en particulier pour les DPD à temps partiels rattachés à l'administration. Si nécessaire, nous réglerons ces problèmes au cas par cas.

Nous tiendrons également compte des conclusions de cet exercice pour planifier nos futures activités de supervision et de mise en application. Le rapport relatif au statut des DPD a été publié en décembre 2012.

En juin 2012, nous avons lancé une enquête sur la fonction de coordinateur de la protection des données (CPD) à la Commission européenne. Sous la forme d'un questionnaire, cette enquête s'inscrira dans un projet plus vaste concernant la fonction du CPD dans tous les services ou institutions de l'UE qui ont créé un réseau de CPD. Les informations recueillies via cette enquête générale seront ensuite utilisées pour rédiger un document sur la fonction de CPD au sein des institutions de l'Union européenne. Les résultats de cette enquête seront rassemblés dans un rapport dont la publication est prévue pour 2013.

2.5.2. Visites

Le CEPD encourage la responsabilité, mais prend également des mesures si nécessaire. Les visites sont un moyen typique pour nous de prendre des mesures ciblées.

Les visites sont un outil de conformité, dont l'objectif est d'obtenir l'engagement de la haute hiérarchie d'une institution ou agence de respecter le règlement. La décision d'organiser une visite est généralement prise en cas de non-respect des règles de protection des données, de manque de communication ou tout simplement dans un but de sensibilisation. Cette décision se fonde sur les informations que nous avons recueillies lors du contrôle du respect du règlement, par exemple dans le cadre d'une enquête générale. La visite se compose d'une visite sur site par le CEPD ou le CEPD adjoint, et est suivie d'une correspondance portant sur une feuille de route spécifique adoptée d'un commun accord par l'organe visité et nous-mêmes.

Entre janvier et décembre 2012, nous avons visité six agences de l'UE: la REA, l'AECER, l'ETF, l'AESA, le CEPCM et FRONTEX.

Ces visites ont pour résultat de sensibiliser à la protection des données, de renforcer le respect du règlement par un engagement de la hiérarchie, d'accroître notre connaissance des agences et, de façon générale, de favoriser une meilleure coopération avec les agences visitées. L'ETF, en particulier, a fait preuve d'une collaboration active avec nous en adoptant des mesures concrètes pour mettre en œuvre les recommandations figurant dans la feuille de route.

Dans le cadre de nos actions visant à sensibiliser au respect des règles de protection des données et d'assurer l'engagement de la direction, Giovanni Buttarelli, contrôleur adjoint, a participé à la réunion des chefs d'agences à Stockholm en octobre 2012. Il a présenté les grands principes du nouveau projet de règlement relatif à la protection des données, comme la responsabilité, la réduction du fardeau

administratif, la transparence, la sécurité et l'efficacité de la supervision et de la mise en application, afin de souligner la nécessité d'anticiper l'intégration de ces concepts au sein des agences de l'UE. Il a également souligné l'importance du rôle du DPD et insisté sur l'importance de lui apporter un soutien. M. Buttarelli a également profité de l'occasion pour présenter notre nouvelle politique en matière de consultations dans le cadre de la supervision et de la mise en application (voir le point 2.6.1).

2.5.3. Inspections

Les inspections constituent un autre instrument essentiel qui permet au CEPD de contrôler et garantir l'application du règlement. Elles se fondent sur l'article 41, paragraphe 2, l'article 46, point c), et l'article 47, paragraphe 2, du règlement.

Le CEPD dispose de pouvoirs étendus lui permettant d'accéder à toutes les informations et données à caractère personnel nécessaires à ses enquêtes et d'obtenir l'accès à tous les locaux dans lesquels le responsable du traitement ou une institution ou un organe de l'UE exerce ses activités. Ces pouvoirs lui permettent de disposer de moyens efficaces pour s'acquitter de ses fonctions.

Les inspections peuvent résulter d'une réclamation ou être effectuées de la propre initiative du CEPD.

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

Au cours des inspections, nous **vérifions les faits sur place**, l'objectif étant également d'assurer le respect du règlement. À l'issue d'une inspection, nous communiquons toujours un suivi adéquat à l'institution inspectée.

En 2012, nous avons procédé au suivi des inspections antérieures. Nous avons également inspecté EURODAC en avril et l'OHMI en avril. Des inspections ciblées sur place ont été effectuées en juin et en juillet auprès de 13 institutions et organes basés à Bruxelles. Ces inspections ont porté sur la façon dont ces institutions et organes informent le grand public de la vidéo-surveillance dans leurs locaux.

Suivi de l'inspection au Centre commun de recherche – Commission européenne

Fin 2010, nous avons effectué une inspection sur place au Centre commun de recherche d'Ispra. Le rapport d'inspection décrivait la sélection et le recrutement du personnel du CCR et les différentes procédures mises en place par le service chargé de la sécurité (contrôle de sécurité avant l'embauche, enquêtes de sécurité, contrôle de l'accès et enregistrement des appels d'urgence). En 2012, nous avons contrôlé la mise en œuvre de nos recommandations par le biais de rapports trimestriels du CCR. Le quatrième et dernier rapport a été reçu du CCR après l'été 2012.

La partie du rapport d'inspection portant sur la sélection et le recrutement du personnel du CCR a été close fin 2012, tandis que nos recommandations concernant les problèmes de sécurité analysés ont abouti à la suppression d'une procédure de contrôle de sécurité par la Commission européenne. Le rapport a également suscité l'adoption d'un nouvel ensemble de règles de sécurité. Les notifications relatives à ces nouvelles procédures de sécurité nous ont été envoyées en décembre 2012 et seront analysées en 2013.

Suivi de l'audit de sécurité de l'unité centrale du système d'information sur les visas

En novembre 2011, nous avons procédé à un audit de sécurité de l'unité centrale du système d'information sur les visas (VIS). Cet audit nous a permis de déterminer si l'infrastructure physique, le personnel, l'organisation et les technologies informatiques étaient conformes aux exigences de sécurité prévues par la législation en vigueur et également par la décision 260/2010 de la Commission relative au plan de sécurité pour le fonctionnement du système.

L'audit n'a révélé aucun problème de sécurité critique justifiant une interdiction temporaire du traitement, mais nous avons identifié plusieurs risques importants compromettant la sécurité que nous avons décrits dans notre rapport de juin 2012. Nous avons demandé à l'autorité de gestion de prendre des mesures immédiates pour éliminer ces risques.

Nous avons reçu des rapports de suivi adéquats de la Commission européenne. Des progrès substantiels ont été accomplis dans le respect des recommandations de l'audit de sécurité. Au moment du transfert à la nouvelle agence européenne chargée des grands systèmes informatiques, plusieurs problèmes restaient toutefois en suspens. Cette agence est devenue opérationnelle le 1er décembre 2012.

Inspection d'EURODAC

En février 2012, nous avons procédé à une deuxième inspection d'EURODAC. Cette inspection de suivi avait pour objet de vérifier la mise en œuvre de nos recommandations de la première inspection de 2006 et de l'audit de sécurité de 2007, et d'évaluer les procédures organisationnelles et techniques générales mises en place pour protéger les informations personnelles et la sécurité dans le cadre d'EURODAC Plus.

Notre inspection a comporté un audit de sécurité et couvert les systèmes d'information de l'Unité centrale opérationnelle (CU) et du site de secours (BCU). Les opérations générales de traitement de données par l'unité centrale d'EURODAC ont été examinées au niveau de l'application, de la base de données et des serveurs, et les mesures de sécurité organisationnelles, techniques et physiques ont également été évaluées.

Nous avons conclu que l'unité centrale d'EURODAC présentait un degré général élevé de protection des données et de sécurité. Les dispositions du règlement EURODAC en matière de traitement de données sont respectées (nature des informations enregistrées, périodes de conservation des données, prescriptions spéciales concernant la suppression préalable et le blocage de données, etc.). EURODAC applique une politique de sécurité spécifique qui définit clairement les rôles et responsabilités de son équipe de gestion et comprend des procédures détaillées concernant les divers aspects de la sécurité informatique.

Diverses mesures techniques de sécurité ont été mises en œuvre afin de sauvegarder les informations personnelles au niveau des applications, des bases de données et des serveurs. Des mesures strictes de sécurité physique ont été prises sur tous les sites d'EURODAC. EURODAC Plus tient compte de la plupart de nos recommandations formulées à l'issue de l'inspection de 2006 et de l'audit de sécurité de 2007.

Inspection à l'OHMI

En avril 2012, nous avons inspecté l'Office de l'harmonisation dans le marché intérieur (OHMI) afin de sensibiliser le personnel à l'existence du CEPD, à nos pouvoirs, et à l'importance du respect des règles en matière de protection des données. L'OHMI a été sélectionné en vue d'une inspection sur la base d'un exercice d'évaluation des risques: il avait obtenu un score inférieur à l'une des références établies dans son groupe de pairs lors de l'enquête de 2011 du CEPD. Cette inspection avait pour objectif général de vérifier les faits et les pratiques, en particulier à la suite de réclamations spécifiques, et de contrôler la mise en œuvre complète de nos recommandations à la suite de différents avis de contrôle préalable.

L'OHMI a collaboré pleinement et de manière constructive tout au long de notre inspection. À la suite d'une évaluation complète des preuves rassemblées, nous avons formulé un certain nombre de recommandations. L'OHMI les a mises en œuvre rapidement, nous permettant ainsi de clore ce dossier en novembre 2012.

Inspection ciblée de la vidéo-surveillance

Le 14 novembre 2012, nous avons adopté un rapport sur les conclusions de différentes inspections sur place effectuées entre le 15 juin et le 18 juillet 2012 dans les locaux de 13 institutions et organes de l'Union européenne basés à Bruxelles. Ces inspections thématiques étaient l'une des mesures annoncées dans notre rapport de suivi de février 2012 sur le respect par les institutions et organes de l'UE de nos lignes directrices de 2010 en matière de vidéo-surveillance.

Sur la base de nos constatations, et afin de mieux informer le public de la vidéo-surveillance, nous avons adressé aux institutions et organes inspectés des recommandations portant notamment sur les points suivants:

- le placement, la localisation, et le contenu d'un avis sur place (pictogramme avec quelques informations de base) indiquant clairement que la zone fait l'objet d'une vidéo-surveillance;
- un avis plus complet concernant la protection des données et synthétisant la raison et les modalités de la vidéo-surveillance, une description des garanties et de la façon dont les personnes concernées peuvent exercer leurs droits;
- une politique de vidéo-surveillance publiée en ligne et décrivant l'approche adoptée par l'institution ou l'organe concerné de l'UE.

Le retour d'information des institutions et organes de l'Union inspectés est actuellement en cours d'examen.

2.6. Consultations relatives aux mesures administratives

2.6.1. Consultations au titre de l'article 28, paragraphe 1, et de l'article 46, point d)

Le 23 novembre 2012, nous avons publié une politique relative aux consultations dans le domaine de la supervision et de la mise en application. Ce document a pour objectif de fournir aux institutions et organes de l'Union des orientations relatives aux consultations du CEPD sur la base des articles 28, paragraphe 1, et 46, sous d), du règlement.

L'article 28, paragraphe 1, du règlement prévoit que les institutions et organes de l'Union européenne doivent informer le CEPD des mesures administratives relatives au traitement des données à caractère personnel. En outre, l'article 46, point d), du règlement impose au CEPD de conseiller 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 d'informations personnelles.

Lorsqu'une institution ou un organe de l'Union élabore des mesures ayant une incidence sur les droits à la protection des données, il doit accorder une attention suffisante au respect de ses obligations au titre du règlement avant l'adoption de ces mesures. L'un des meilleurs moyens de garantir de respect est d'impliquer dès le départ le DPD et de lui demander son avis d'expert en interne.

Comme indiqué dans le document stratégique, nous encourageons les responsables du traitement à nous consulter dans les cas particuliers et limités où ce traitement: a) présente un caractère nouveau ou une certaine complexité (en cas de doute véritable dans le chef du DPD ou de l'institution) ou b) a une incidence manifeste sur les droits des personnes concernées (que ce soit en raison des risques entraînés par les activités de traitement, du fait de l'extension d'une mesure, etc.). En principe, le CEPD examine uniquement les consultations qui ont été soumises préalablement au DPD de l'institution concernée (article 24, paragraphe 3, du règlement intérieur).

Dans le cadre des consultations menées sur des mesures administratives envisagées par une institution ou un organe, plusieurs questions ont été examinées en 2012. Les sous-points suivants rendent compte de certains de ces dossiers.

2.6.1.1. Facturation individuelle des utilisateurs passant des appels non liés au travail sur les téléphones fixes - EFSA

Le 1er mars 2012, nous avons répondu à une consultation relative à la politique de l'EFSA de facturer individuellement les utilisateurs qui passent des appels non liés au travail sur leurs téléphones fixes.

Nous avons tout d'abord examiné la question de savoir si la politique de l'EFSA nécessitait une notification au CEPD en vue d'un contrôle préalable. Nous avons insisté sur la nécessité d'opérer une distinction entre le traitement d'informations aux seules fins de facturation et de gestion du trafic sans évaluer le comportement des personnes, d'une part, et le traitement d'informations aux fins de contrôler et d'évaluer le comportement des personnes, d'autre part (par exemple pour détecter l'utilisation excessive ou non autorisée du téléphone par les membres du personnel). Le deuxième type de traitement est soumis à un contrôle préalable, contrairement au premier. La politique écrite de l'EFSA évoquait la vérification de l'utilisation autorisée des systèmes de télécommunications, mais le DPD de l'EFSA a clarifié que cette politique avait pour seule finalité la facturation et la gestion du budget et a donc proposé de supprimer la mention de la vérification.

Nous avons estimé que certaines catégories d'informations reprises dans le modèle de facture envoyé par l'opérateur de télécommunications n'étaient pas nécessaires à des fins de facturation. Nous avons suggéré en particulier de supprimer de la facture les champs relatifs à l'identification des personnes appelées et aux appels restés sans réponse.

Nous avons également recommandé à l'EFSA de limiter le nombre des personnes ayant accès aux données et de rappeler à ces personnes autorisées que ces données devaient servir uniquement à la facturation et à la gestion du budget. Enfin, nous avons recommandé à l'EFSA de fournir des informations adéquates aux membres actuels et futurs de son personnel conformément aux articles 11 et 12 du règlement.

2.6.1.2. Publication sur l'internet du répertoire officiel des agents des institutions et organes de l'Union européenne

La publication par une institution ou un organe de l'Union européenne des noms, fonctions et coordonnées de fonctionnaires sur leurs sites internet nécessite le traitement d'informations personnelles par cette institution ou cet organe et tombe par conséquent sous le coup du règlement. Par conséquent, la publication de ces informations doit être fondée sur l'un des motifs de traitement visés à l'article 5 du règlement.

Dans notre avis du 8 février 2012, nous avons estimé que la publication d'un répertoire des membres du personnel pouvait se baser sur l'article 5, point a) du règlement, dans la mesure où elle est effectuée dans l'intérêt général, à savoir pour renforcer l'accessibilité et la transparence conformément à l'article 1 du TUE et à l'article 15 du TFUE. Il incombe cependant à l'institution ou à l'organe concerné de déterminer au cas par cas ou par catégorie de personnel si cette publication est nécessaire dans des cas précis, et de définir les informations devant être publiées (en raison, par exemple, des fonctions de chaque membre du personnel, de ses responsabilités, de la fréquence de ses contacts avec des parties prenantes externes, etc.).

Afin de renforcer et de clarifier la base juridique du traitement, nous avons recommandé que les institutions ou organes concernés adoptent une décision ou un autre acte administratif décrivant la finalité, les conditions et les modalités de cette publication ainsi que les autres caractéristiques pertinentes du répertoire.

Les membres actuels et futurs du personnel doivent recevoir des informations claires et complètes conformément au règlement (articles 11 et 12) et avoir le droit de s'opposer à la publication pour des raisons impérieuses et légitimes (article 18). En outre, l'institution ou l'organe concerné doit prendre toutes les mesures nécessaires pour empêcher que les informations personnelles contenues dans le répertoire ne soient utilisées à des fins de marketing direct, d'envoi de courriers de masse ou à toute autre fin malveillante (voir l'article 38, paragraphe 2).

2.6.1.3. EACI: seuls les certificats pertinents doivent être collectés pour les contrats à durée indéterminée

Nous avons reçu une consultation du DPD de l'EACI au titre de l'article 46, point d) du règlement n° 45/2001 concernant la collecte de certificats CAST de tous les agents contractuels (AC) travaillant à l'EACI.

Le traitement des certificats CAST a pour but de compléter et d'actualiser le dossier des AC, une obligation imposée pour bénéficier d'un contrat à durée indéterminée au sein de l'EACI. Dans notre réponse du 23 juillet 2012, nous avons estimé que ce traitement était généralement conforme au règlement.

Nous avons cependant noté que le service RH de l'EACI demande également aux membres du personnel de fournir des certificats CAST relatifs à d'autres groupes de fonctions que ceux pour lesquels ils ont été recrutés à l'EACI et pour lesquels ils pourraient bénéficier d'un contrat à durée indéterminée. Dans ce cas particulier, nous avons insisté sur le fait que les certificats CAST ne peuvent être considérés comme pertinents pour cette nouvelle finalité et recommandé que le service HR recueille uniquement les certificats CAST pertinents pour les groupes de fonctions pour lesquels les membres du personnel ont été recrutés.

2.6.1.4. Consultation relative aux clauses contractuelles modèles révisées de l'OLAF en matière de protection des données destinées à être utilisées dans les accords de coopération administrative (ACA) conclus avec des autorités des pays tiers ou des organisations internationales

Dans nos avis du 3 avril et du 16 juillet 2012, nous avons reconnu que la possibilité pour l'OLAF de partager des informations avec des autorités des pays tiers et des organisations internationales constitue un atout important dans la lutte contre la fraude internationale. Néanmoins, tout échange d'informations personnelles doit se conformer au cadre juridique existant régissant les transferts transfrontaliers de données à caractère personnel par les institutions et organes de l'Union européenne, à savoir l'article 9 du règlement.

Nous avons pressé l'OLAF de renforcer les garanties concrètes et les mécanismes de conformité et de recours en place. Nous avons notamment formulé les recommandations suivantes:

- L'OLAF doit sélectionner ses partenaires avec soin et effectuer une analyse préliminaire de leur capacité et de leur volonté de respecter les clauses des **accords de coopération administrative** (ACA) et leurs annexes.
- L'OLAF devrait mettre en place les mesures nécessaires pour vérifier, dans la mesure du possible, la mise en œuvre correcte de l'accord par ses partenaires de l'ACA et présenter régulièrement un compte rendu au CEPD.
- En cas de problème, l'OLAF et ses partenaires doivent faire tout leur possible pour trouver une solution, y compris, si nécessaire, accorder des concessions particulières aux personnes concernées.

2.6.1.5. Transfert des données médicales des candidats en phase de pré-recrutement entre les services médicaux des institutions

À la suite de l'arrêt CST dans l'affaire F-46/09, V. vs. PE, la DG RH de la Commission a soumis une

consultation au titre de l'article 28, paragraphe 1 du règlement concernant le transfert des données médicales des candidats en phase de prérecrutement entre les services médicaux des institutions. Ils ont soumis un projet de conclusion qui devra être approuvé par le Collège des chefs d'administration (CCA), une note explicative concernant le projet de conclusion, un projet de formulaire de consentement, et une déclaration de confidentialité.

Nous avons identifié trois domaines à analyser.

- En ce qui concerne la *licéité du traitement*, nous avons clarifié le fait que le traitement ne peut être basé exclusivement sur le consentement, celui-ci étant une base juridique insuffisante en matière d'emploi. Il doit donc être considéré comme une garantie supplémentaire pour le transfert. Nous avons recommandé à la Commission d'indiquer clairement que les règles internes constituent la principale base juridique, comme l'exige l'article 5, point a) du règlement n° 45/2001.

- En ce qui concerne le principe de *nécessité*, la Commission a insisté sur les raisons «utiles» justifiant le transfert de données: le fait d'éviter un deuxième contrôle par une autre institution réduit les frais, accélère la procédure et réduit les fraudes. Nous avons cité l'arrêt dans l'affaire V c. PE (point 131), qui renforce le principe de nécessité par l'emploi du terme «indispensable». Nous avons recommandé que la Commission indique les raisons rendant un transfert nécessaire et indispensable à la lumière de l'article 7 du règlement et qu'elle supprime toute référence à une simple «utilité».

- En ce qui concerne le *consentement et le droit de retrait*, la Commission a inclus un mécanisme d'accord préalable. Nous avons cependant recommandé à la Commission de préciser que les personnes concernées peuvent retirer leur consentement à tout moment et pas seulement dans un délai de 10 jours, d'indiquer que les personnes concernées peuvent refuser leur consentement sans préjudice de leurs droits et que les personnes qui refusent leur consentement ne doivent pas être soupçonnées de fraude.

Lors du suivi de cette consultation, nous avons constaté que la Commission avait adopté des mesures adéquates mettant en œuvre nos recommandations. La Commission va donc soumettre son projet de conclusions à l'approbation du Collège des chefs d'administration afin que, dans un souci d'harmonisation, les institutions et organes de l'Union européenne puissent adopter les mêmes règles internes.

2.7. Orientations en matière de protection des données

L'expérience acquise grâce à l'application du règlement relatif à la protection des données a permis à notre personnel de traduire son expertise en une orientation générale pour les institutions et organes. En 2012, ce travail d'orientation a pris la forme d'un suivi d'orientations antérieures en matière de congé et d'horaire flexible, de formations pour les DPD, d'un atelier pour les responsables du traitement, d'un espace réservé aux DPD sur le site internet du CEPD et d'une ligne d'assistance pour les DPD.

Nous travaillons actuellement sur des lignes directrices pour les absences et les congés, la passation des marchés et la sélection des experts, le contrôle électronique et les transferts de données.

2.7.1. Lignes directrices thématiques

Rapport de suivi sur la vidéo-surveillance

En février 2012, nous avons publié notre rapport de suivi décrivant le respect, par les institutions et organes de l'UE, des lignes directrices en matière de vidéo-surveillance publiées par le CEPD en mars 2010.

Ce rapport de suivi présente une analyse systématique et comparative des rapports sur l'état d'avancement adressés au total par 42 institutions et organes de l'Union européenne. Cette analyse nous a convaincus que les lignes directrices ont contribué à accroître le niveau de sensibilisation et de transparence en matière de vidéo-surveillance au sein des institutions et organes de l'UE.

Nous avons pris note des efforts considérables consentis par les institutions et organes qui ont présenté leur rapport sur l'état d'avancement, notamment du point de vue des taux de participation généraux, de l'utilisation limitée de systèmes de vidéo-surveillance «intrusifs», et des approches basées sur la prise en compte du respect de la vie privée dès la conception.

Cependant, près de deux après l'adoption des lignes directrices et plus de deux ans après le début du processus de consultation, nous sommes déçus de constater que la mise en œuvre des lignes directrices a été mise en attente ou considérablement retardée dans plusieurs institutions. Ces retards concernent des points tels que le contenu des avis affichés sur place, la publication des politique de vidéo-surveillance en ligne, l'absence d'analyses d'incidence, ainsi qu'une formation insuffisante à la protection des données.

En plus de louer les bonnes pratiques, notre rapport de suivi souligne les lacunes des institutions qui sont en retard dans leurs efforts visant à garantir le respect des lignes directrices et annonce des mesures de suivi.

Lignes directrices sur le traitement d'informations personnelles en matière de congé et d'horaire flexible

En décembre 2012, nous avons publié des lignes directrices sur la gestion du traitement des informations personnelles en matière de congé et d'horaire flexible.

Ces lignes directrices couvrent le traitement des informations personnelles dans la gestion des congés pour cause de maladie, des congés annuels, et de tous les droits à des congés spéciaux liés aux conditions de travail des fonctionnaires, des agents temporaires, des agents contractuels et des experts nationaux détachés. Elles comportent également une analyse des opérations de traitement du système de gestion des horaires flexibles.

Ces lignes directrices ont pour objectif de proposer des conseils pratiques et une assistance à tous les

DPD et responsables du traitement dans leur mission de notification des traitements de données existants et/ou futurs au CEPD. Le réseau de DPD a été consulté à propos du projet de lignes directrices en octobre 2012. Ces lignes directrices devraient servir de base de notification pour les institutions et organes qui n'ont pas encore notifié leurs procédures, et de guide pratique pour toutes les institutions et organes.

En ce qui concerne les opérations de traitement des congés, nous insistons sur l'obligation de confidentialité imposée aux personnes responsables du traitement des données relatives à la santé (catégories spéciales de données) et sur l'obligation de garantir la qualité des données traitées. Les périodes de conservation des informations relatives aux congés sont un autre aspect important nécessitant une attention particulière.

Pour les opérations de traitement en matière d'horaires flexibles, nous présentons des exemples de cas pour lesquels une notification en vue d'un contrôle préalable n'est pas nécessaire et de cas pour lesquels cette notification est requise. Nous insistons également sur le droit d'accès et de rectification de la personne concernée. Enfin, nous analysons la possibilité d'établir des liens entre les informations figurant dans les systèmes de gestion des horaires et dans d'autres systèmes.

2.7.2. Formations et ateliers

Le CEPD a organisé deux ateliers pour les coordinateurs de la protection des données (CPD) le 14 juin et le 20 septembre à Bruxelles. Ces deux événements ont accueilli respectivement 42 et 13 participants, les CPD de 7 institutions (Commission, Parlement européen, Conseil, banque centrale européenne, Banque européenne d'investissement, Service européen pour l'action extérieure, Cour des comptes). Les présentations par des DPD et par des membres de l'équipe «Supervision» du CEPD ont donné une image réaliste de la théorie et des bonnes pratiques. Les CPD ont apprécié ces ateliers, et leurs commentaires insistent notamment sur les échanges utiles avec leurs collègues et homologues des autres institutions et avec le personnel du CEPD.

À la suite de la publication de nos lignes directrices concernant l'évaluation[6] et d'avis de contrôle préalable en la matière dans lesquels nous avons réexaminé les périodes de conservation des données d'évaluation, nous avons organisé un atelier sur la conservation des données dans le cadre des évaluations le 4 décembre 2012. Les participants à cet atelier, organisé dans nos nouveaux locaux, étaient notamment des représentants des ressources humaines, des responsables de la gestion documentaires, des DPD des trois principales institutions, de la BCE et des agences exécutives, et des membres du personnel du CEPD. Cet atelier avait pour but d'encourager les discussions concernant les périodes actuelles de conservation des données relatives à l'évaluation dans les dossiers du personnel et les règles de protection des données dans ce domaine. Nous espérions mieux comprendre les besoins de l'administration de l'Union européenne et déterminer les périodes de conservation des documents recueillis et traités dans ce contexte.

En conclusion, les participants sont convenus de la nécessité d'une enquête visant à recueillir des informations (exemples détaillés) sur les besoins des administrations en matière de conservation de certaines catégories particulières de documents. Une fois l'enquête terminée, ses résultats devraient être envoyés à tous les DPD afin que ceux-ci puissent les communiquer à tous les départements concernés et recueillir des contributions supplémentaires. Les informations recueillies pourraient servir de base à l'élaboration d'une proposition de périodes de conservation adéquates pour certaines catégories particulières de documents.

2.7.3. Coin des DPD et autres outils

Comme nous l'avons annoncé dans notre rapport annuel 2011, nous avons lancé le «Coin des DPD» («DPO Corner») du site Web du CEPD en juillet 2012. Il s'agit d'une rubrique restreinte réservée aux DPD des institutions et organes de l'Union européenne. Le Coin des DPD contient des informations utiles et des outils pratiques pour aider les DPD dans leur travail ainsi que des documents d'information sur le rôle et les missions des DPD, divers modèles et présentations pour aider les DPD dans leurs activités de sensibilisation, des résumés des évolutions récentes dans le domaine de la protection des données, et un calendrier d'événements (formations ou réunions). Ces informations sont mises à jour régulièrement.

Nous avons également créé une ligne d'assistance téléphonique pour répondre aux questions de base des DPD ou pour les réorienter vers un responsable de dossier qui pourra répondre à leurs questions concernant un thème ou un dossier particulier (voir le point 2.2 concernant les délégués à la protection des données).

[6] Ces lignes directrices sont disponibles sur le site Web du CEPD: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/11-07-15_Evaluation_Guidelines_EN.pdf

3 CONSULTATION

Notre objectif stratégique

Veiller à ce que le législateur européen (Commission, Parlement et Conseil) connaisse les exigences relatives à la protection des données et intègre cette notion aux nouvelles dispositions législatives.

Nos principes directeurs

- nous cherchons à coopérer de manière constructive avec les responsables politiques à un stade précoce de l'élaboration des politiques;
- nous cherchons des solutions créatives qui soutiennent les objectifs politiques et les principes de protection de la vie privée en nous appuyant sur nos connaissances des législations et des technologies;
- nous œuvrons pour trouver des solutions pratiques, notamment dans des domaines politiques complexes, où il peut s'avérer difficile de trouver le juste équilibre et de porter des jugements;
- nous cherchons à garantir que la protection des données fera partie intégrante de l'élaboration des politiques et du processus législatif dans tous les domaines de compétence de l'UE.

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

L'année 2012 a connu des développements majeurs dans le domaine de la protection des données. La Commission a continué de publier un grand nombre de propositions législatives ayant un impact sur la protection des données, et notamment une réforme globale des règles existantes en matière de protection des données. Ce projet a été une priorité importante du CEPD en 2012 et le restera à mesure que la procédure législative se poursuivra. Les débats passés et en cours au Parlement européen et au Conseil ont suscité un intérêt croissant pour la réforme de la part d'un grand nombre de parties prenantes du secteur privé comme du secteur public, à l'intérieur comme à l'extérieur de l'UE. Ce processus a également démontré une compréhension fondamentale des principes sous-jacents de la réforme par les institutions de l'Union européenne.

Suivant la tendance des dernières années, les domaines abordés par les avis du CEPD ont continué de se diversifier. Outre les priorités traditionnelles, telles que la poursuite du développement de l'espace de liberté, de sécurité et de justice (SLSJ) ou les transferts internationaux de données, de nouveaux domaines émergent progressivement. En 2012, différents avis se sont focalisés sur le marché numérique et sur la sécurité des consommateurs dans l'environnement en ligne. Dans ces domaines, les thèmes des données personnelles en matière de santé et des informations personnelles en matière de crédit ont revêtu une importance particulière.

En 2012, nous avons également publié un avis sur **l'informatique en nuage**, insistant sur les principes de protection des données et l'importance de leur mise en œuvre correcte dans le cadre de ce phénomène majeur. Dans cet avis, nous décrivons et motivons les normes nécessaires de protection des données dans le nuage. Ces avis sont destinés à fournir des orientations et à devenir des points de référence pour les questions et thèmes importants à venir en matière de protection des données.

L'**interopérabilité** croissante des **technologies sophistiquées au service des consommateurs** et de l'**internet** (par ex. les appareils intelligents) pose de nouveaux défis pour la limitation du traitement des informations personnelles aux fins pour lesquelles

elles ont été recueillies. L'accès à des informations dont la diffusion est restreinte ou l'utilisation de données précédemment non pertinentes ou inaccessibles pour de nouvelles finalités ont été au cœur de nos travaux récents. L'avis relatif aux compteurs intelligents, des appareils permettant des économies d'énergie considérables mais qui peuvent aussi entraîner une forme de surveillance domestique, est un exemple de proposition sur laquelle nous avons fait des observations et qui illustre cette tendance.

Concernant **l'espace de liberté, de sécurité et de justice**, la question de la nécessité a été un thème récurrent. Nous avons rendu plusieurs avis dans lesquels ce principe de protection des données a occupé une place importante. C'est notamment le cas de nos avis concernant EURODAC[7], SIS II[8] et le Centre européen de lutte contre la cybercriminalité[9]. Nous sommes très conscients de la tendance des agences répressives à plaider en faveur d'un accès accru aux autres bases de données, comme celles utilisées par les douanes et les services de l'immigration, à des fins de prévention de la criminalité.

Les avis relatifs au **marché intérieur** ont eux aussi gardé une place importante en 2012, avec une attention croissante accordée au marché numérique. Nous avons notamment adopté une série de quatre avis dans le domaine de la réglementation des marchés financiers[10].

3.2. Cadre d'action et priorités

3.2.1. Mise en œuvre de la politique de consultation

Même si nos méthodes de travail dans le domaine de la consultation ont évolué au fil des ans, les approches fondamentales des interventions n'ont pas changé. Notre document stratégique de mars 2005 intitulé «Le CEPD en tant que conseiller des institutions communautaires à l'égard des propositions de législation et documents connexes» reste pertinent, bien qu'il faille désormais le lire à la lumière du traité de Lisbonne.

Fondés sur l'article 28, paragraphe 2, ou l'article 41 du règlement (CE) n° 45/2001, les avis formels constituent le principal instrument de notre travail de consultation et contiennent une analyse complète de tous les éléments relatifs à la protection des données qui figurent dans une proposition de la Commission ou tout autre instrument pertinent.

Les consultations législatives fondées sur l'article 28, paragraphe 2, du règlement constituent l'élément central du rôle consultatif du CEPD. Selon cet article, la Commission nous consulte lorsqu'elle adopte une proposition législative ayant trait à la protection des droits et libertés des individus. Nos avis donnent une analyse complète des aspects liés à la protection des données d'une proposition ou d'un autre texte.

En règle générale, nous formulons des avis sur les textes non législatifs (comme les documents de travail de la Commission, les communications ou les recommandations) lorsque la protection des données en est un élément important. Il nous arrive de rédiger des commentaires par écrit à des fins plus limitées, afin de faire passer un message rapide et fondamental ou de nous concentrer sur un ou plusieurs aspects techniques. Ces commentaires sont également utilisés pour synthétiser ou répéter des observations antérieures.

Nous sommes à la disposition des institutions de l'UE pour les conseiller à tous les stades de l'élaboration des politiques et du processus législatif et utilisons toute une série d'autres instruments dans notre rôle consultatif. Bien que cette approche nécessite des contacts étroits avec les institutions, maintenir notre indépendance reste primordial.

Nous pouvons également recourir à d'autres outils tels que des présentations orales, des courriers explicatifs, des conférences de presse ou des communiqués de presse. Par exemple, les avis sont souvent suivis de présentations devant la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen ou devant les groupes de travail concernés du Conseil.

Les *avis prospectifs* ont été ajoutés récemment à ces instruments. Nous les utilisons pour expliquer l'importance et l'utilité de la mise en œuvre correcte des principes en matière de protection des données. Élaborés de notre propre initiative, ils ne sont pas liés à une proposition législative spécifique. Ils sont destinés à fournir des orientations et à devenir des points de référence pour les questions et thèmes fondamentaux en matière de protection des données.

Les contacts avec la Commission ont lieu aux différents stades de la préparation des propositions, et leur intensité dépend du sujet et de l'approche des services de la Commission. C'est le cas en particulier des projets à long terme, comme la réforme du cadre juridique de l'OLAF, à laquelle nous avons contribué à différents stades.

Les activités formelles de consultation sont assez souvent précédées d'observations informelles. Lorsque la Commission élabore une nouvelle mesure législative ayant des répercussions sur la protection des données, le projet nous est généralement envoyé au cours de la consultation interservices, c'est-à-dire

[7] Voir point 3.4.6.
[8] Voir point 3.4.4.
[9] Voir point 3.4.3.
[10] Voir point 3.5.3.

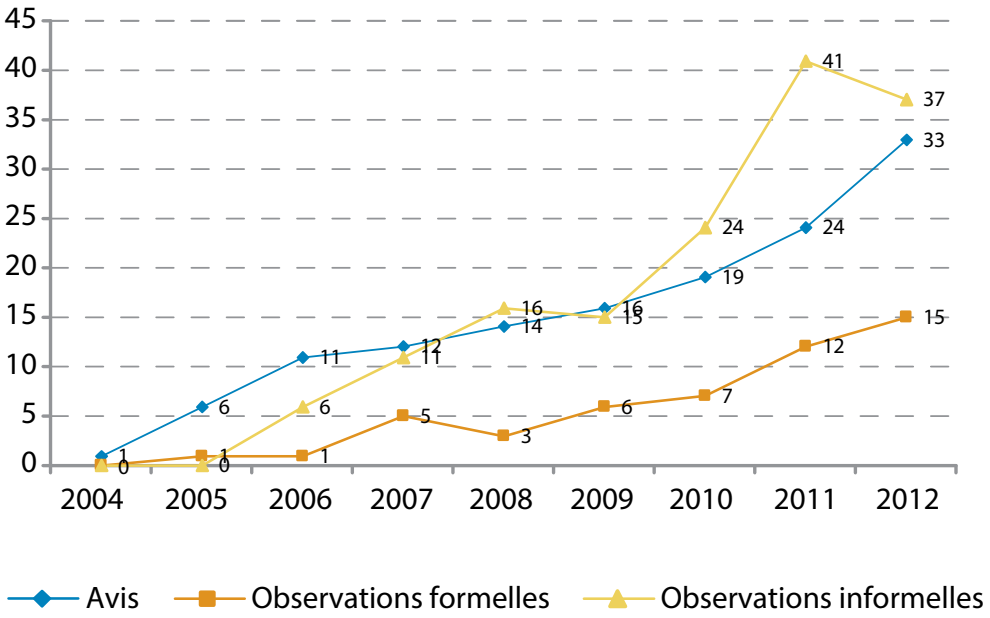
avant que la proposition ne soit finalisée et adoptée. Ces observations informelles, au nombre de 37 en 2012, permettent de traiter les questions de protection des données à un stade précoce où il est encore possible de modifier le texte d'une proposition relativement aisément. La présentation d'observations informelles à la Commission est un moyen précieux de garantir que les principes de protection des données sont dûment pris en considération au moment de la rédaction d'une proposition législative, et il est très souvent possible de résoudre des problèmes cruciaux à cette étape. En règle générale, ces observations informelles ne sont pas rendues publiques. Si elles sont suivies par un avis ou des observations formelles, nous faisons généralement référence aux observations informelles présentées antérieurement.

Des contacts réguliers avec les services de l'institution concernée auront lieu après la publication de nos observations ou avis. Dans certains cas, nous sommes largement impliqués dans les discussions et négociations qui se déroulent au Parlement et au Conseil. Dans d'autres cas, la Commission est le principal interlocuteur au cours de la phase de suivi.

3.2.2. Résultats en 2012

En 2012, le nombre d'avis rendus a augmenté de manière significative. Nous avons rendu 33 avis, 15 observations formelles et 37 observations informelles sur toute une série de sujets. Par ces interventions et d'autres, nous avons mis en œuvre nos priorités pour 2012 telles qu'elles sont décrites dans notre programme.

Évolution des avis législatifs entre 2004 et 2012



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

Pour le CEPD, il ne fait aucun doute que le paquet de réformes en matière de protection des données était le principal projet législatif de 2012. Nous avons souligné à de nombreuses reprises la nécessité d'avoir des règles européennes mises à jour et plus strictes en matière de protection des données. Le 25 janvier, la Commission a adopté son paquet de réformes, composé de deux propositions législatives: un règlement général sur la protection des données et une directive spécifique sur la protection des données dans le domaine de la police et de la justice.

Notre première réaction a été de saluer le règlement général comme un énorme pas en avant pour la protection des données en Europe, un excellent point de départ pour l'adoption de règles européennes en matière de protection des données suffisamment robustes pour faire face aux défis futurs des technologies de l'information.

Nous avons par contre vivement critiqué le contenu inadéquat de la directive. Nous avons fait remarquer que la Commission n'avait pas tenu sa promesse de mettre en place un système robuste de protection des données dans les domaines de la police et de la justice et demandé pourquoi la Commission avait exclus ces domaines de son intention originale de proposer un cadre législatif global.

Le 7 mars, nous avons adopté un avis présentant plus en détail notre position concernant ces deux

Peter Hustinx, CEPD, rencontre Sabine Leutheusser-Schnarrenberger, Ministre fédérale allemande de la Justice

propositions. Dans une déclaration publique, le CEPD a conclu qu'avec ces deux propositions législatives, l'Europe serait encore bien loin de posséder un ensemble complet de règles de protection des données, que ce soit au niveau national ou au niveau de l'Union, dans tous les domaines de politique de l'Union. C'est d'autant plus vrai que ces propositions laissent intacts de nombreux instruments européens de protection des données tels que les règles de protection des données applicables aux institutions et organes de l'UE et certains instruments particuliers dans le domaine répressif.

Nous avons salué une amélioration spécifique apportée par la directive, à savoir le fait que cette proposition couvre également le traitement dans un contexte domestique. Nous avons toutefois insisté sur le fait que cet élément n'aurait apporté une valeur ajoutée que si la directive avait renforcé de manière significative le niveau de protection des données dans ce domaine, ce qui n'est pas le cas.

Nous avons souligné que les règles proposées en matière de protection des données pour les services répressifs étaient bien trop faibles. Nous avons relevé de nombreux cas dans lesquels il n'était pas justifié de s'écarter des règles prévues par la proposition de règlement. Nous avons fait observer que, s'il est vrai que des règles précises sont nécessaires dans le domaine répressif, il n'est pas nécessaire de baisser globalement le niveau de protection des données.

Nous avons également exprimé des préoccupations particulières concernant:

- le manque de certitude juridique concernant l'utilisation ultérieure des informations personnelles par les autorités répressives;

Notre avis relatif à la révision du cadre européen en matière de protection des données souligne plusieurs points positifs du règlement:

- les règles seront directement applicables dans les États membres;
- elles élimineront de nombreuses complications et incohérences causées par les législations nationales de mise en œuvre actuelles;
- elles renforceront les droits des personnes;
- elles renforceront la responsabilité des responsables du traitement s'agissant de la façon dont ils traitent les informations personnelles;
- le rôle et les pouvoirs des autorités de contrôle nationales seront renforcés au niveau national, mais aussi au niveau de l'Union européenne, grâce au comité européen de la protection des données.

Le CEPD a notamment exprimé ses inquiétudes sur les points suivants:

- la possibilité de restriction des principes et droits fondamentaux;
- la possibilité de dérogation en vue du transfert de données vers des pays tiers;
- les pouvoirs excessifs octroyés à la Commission dans le mécanisme conçu pour garantir la cohérence entre les autorités de contrôle;
- les nouveaux motifs d'exception au principe de limitation de la finalité.

- l'absence d'obligation générale, dans le chef des autorités répressives, de démontrer leur respect des prescriptions en matière de protection des données;
- les conditions laxistes en matière de transfert vers des pays tiers;
- la restriction injustifiée des pouvoirs des autorités de contrôle.

Tout au long de l'année, le CEPD a prononcé divers discours précisant notre position sur le paquet de réformes et participé à des discussions thématiques. Nous sommes restés à la disposition du législateur de l'UE pour fournir des conseils ou des explications supplémentaires concernant notre position. Par ailleurs, par notre participation au groupe de travail de l'article 29, nous avons exprimé des commentaires sur plusieurs questions plus particulières.

Nous nous sommes également efforcés d'encourager les discussions. En septembre et en novembre, en étroite collaboration avec la Europäische Rechtsakademie (ERA), le CEPD a organisé deux séminaires consacrés aux propositions. Ces séminaires ont réuni de nombreux experts des administrations nationales, des autorités chargées de la protection des données, des institutions de l'Union européenne, du monde universitaire, des pays tiers et du secteur privé. Nous avons également lancé un site internet consacré au processus de réforme, contenant toute la documentation pertinente et accessible via un lien sur notre propre site.

Les deux propositions ont fait l'objet de débats approfondis au Parlement européen et au Conseil et ont attiré l'attention de bon nombre de parties prenantes publiques et privées. Ce processus législatif a fait l'objet d'un lobbying exceptionnel.

La commission LIBE du Parlement a été désignée pour mener les travaux relatifs au paquet de réformes. Deux rapporteurs ont été nommés, l'un pour le règlement et l'autre pour la directive, et ils ont travaillé en étroite collaboration. La commission a fourni des informations actualisées sur l'état d'avancement par des documents de travail soulignant les points de départ et les principaux éléments susceptibles de faire l'objet de discussions supplémentaires. La réunion annuelle de la commission parlementaire conjointe, organisée en octobre, a été consacrée aux deux propositions. Les deux projets de rapports ont été envoyés en traduction avant fin 2012 et ont été annoncés publiquement le 9 janvier 2013. Le Parlement compte organiser un vote en plénière au deuxième semestre 2013. Les projets de rapports de plusieurs autres commissions ont également été publiés vers la fin de l'année 2012.

Au Conseil, les travaux ont avancé à un rythme moins soutenu. Au cours d'une série de longues réunions de deux jours du groupe de travail DAPIX, sous la direction des Présidences danoise et chypriote, le Conseil a examiné les propositions article par article. Ces réunions ont généralement accordé une plus grande attention au règlement, la proposition de directive suscitant moins d'enthousiasme.

Parallèlement, le Conseil a discuté de plusieurs thèmes essentiels tels que la division possible du règlement entre secteur public et secteur privé, la diminution du fardeau administratif pour les responsables du traitement, et l'élargissement des pouvoirs de la Commission pour l'adoption d'actes délégués et d'actes d'exécution. Sous la Présidence irlandaise, le Conseil a annoncé son intention de travailler plus rapidement en 2013 et envisagé de finaliser la première lecture au début de l'année 2013.

3.4. Espace de liberté, de sécurité et de justice et coopération internationale

En 2012, nous avons adopté un ensemble de trois observations formelles et de trois avis concernant l'ELSJ et la coopération internationale.

3.4.1. EUROSUR

Le 8 février 2012, nous avons publié des observations relatives à une proposition de règlement du Parlement européen et du Conseil portant création du système européen de surveillance des frontières (EUROSUR). Cette proposition vise à assurer une meilleure coordination entre les autorités de contrôle aux frontières et une meilleure surveillance des frontières. À cette fin, il est prévu que les États membres créent des «centres de situation» nationaux dont les évaluations seront utilisées pour dresser le «tableau de situation européen» généré par FRONTEX.

Cette proposition n'a pas pour objectif le traitement d'informations personnelles, mais des traitements de ce type peuvent avoir lieu dans certaines circonstances. C'est pourquoi nous avons recommandé d'énumérer explicitement et de manière exhaustive les conditions dans lesquelles EUROSUR pourra traiter des informations personnelles et de clarifier les dispositions relatives aux échanges d'informations avec les pays tiers.

3.4.2. Gel et confiscation des produits du crime dans l'Union européenne

Le 18 juin 2012, nous avons envoyé une lettre à la Commission à propos de la proposition de directive concernant le gel et la confiscation des produits du crime dans l'Union européenne. Même si cette pro-

position ne concerne pas directement le traitement des informations personnelles, le CEPD a attiré l'attention de la Commission sur les conséquences en matière de protection des données que pourrait avoir la mise en œuvre de certaines dispositions au niveau national.

3.4.3. Centre européen de lutte contre la cybercriminalité

Le 29 juin 2012, nous avons adopté un avis sur la communication de la Commission relative à la création d'un Centre européen de lutte contre la cybercriminalité (EC3). Nous avons recommandé de clarifier la position et l'autorité de l'EC3 par rapport au cadre juridique actuel et à la mission d'Europol. Nous avons également mis en garde contre les risques en matière de protection des données inhérents à la communication directe envisagée entre l'EC3 et le secteur privé ainsi que contre les risques associés aux transferts internationaux de données.

3.4.4. Migration de SIS II

Le 9 juillet 2012, nous avons adopté un avis concernant la proposition par la Commission d'un règlement relatif à la migration du système d'information Schengen (SIS 1+) vers le système d'information Schengen de deuxième génération (SIS II) (refonte). Une fois opérationnel, SIS II offrira des fonctionnalités accrues comme la possibilité d'utiliser des données biométriques, de nouveaux types d'alertes, la possibilité de lier différentes alertes (par exemple des alertes concernant une personne et un véhicule) et une fonctionnalité de recherche directe à l'intérieur du système.

Nous avons accueilli favorablement la clarification, dans cette proposition, de l'étape de la migration à laquelle le règlement SIS II entrera en vigueur. Mais nous avons aussi mis en évidence les éléments susceptibles de poser des risques majeurs et les problèmes à régler pour permettre à la migration de se dérouler comme prévu.

Nous avons recommandé en particulier de mieux définir la portée de la migration dans la proposition, puisqu'il faut une clarté absolue quant aux catégories de données concernées par la migration; de préciser si la migration entraîne une transformation des données et, dans l'affirmative, quelles données sont touchées; d'analyser les risques liés à la migration et les mesures à prendre pour atténuer ces risques; de prévoir une obligation spécifique d'archivage des activités de traitement des données dans le cadre de la migration; de renforcer les obligations en matière de tests; de prendre des mesures de sécurité spécifiques à la lumière des risques liés à la migration.

3.4.5. Traite des êtres humains

Le 10 juillet 2012, nous avons publié nos observations concernant la communication de la Commission relative à une stratégie de l'Union européenne en vue de l'éradication de la traite des êtres humains (TEH) pour la période 2012-2016. Nous avons accueilli favorablement cette stratégie et l'importance qu'elle accorde à la protection des droits fondamentaux, mais souligné que la lutte contre la TEH est un domaine qui nécessite le traitement de données importantes, contenant souvent des informations personnelles, ce qui crée un risque d'intrusion dans la vie privée des personnes.

Nous avons insisté sur le fait que la protection des données est une condition indispensable pour instaurer une confiance réciproque entre les victimes et les autorités impliquées dans la lutte contre la TEH, mais aussi entre différentes autorités. Nous avons montré, par des suggestions pratiques et réalistes, comment la protection des données peut contribuer à une coopération plus efficace et efficiente entre toutes les parties prenantes.

3.4.6. Règlement EURODAC

Le 5 septembre 2012, nous avons adopté un avis concernant la proposition modifiée de la Commission en vue d'un règlement du Parlement européen et du Conseil relatif à la création d'EURODAC aux fins de la comparaison des empreintes digitales des demandeurs d'asile. Cette proposition modifiée prévoit notamment l'accès aux données d'EURODAC par les autorités répressives.

Même si la disponibilité d'une base de données d'empreintes digitales peut être un outil supplémentaire précieux dans la lutte contre la criminalité, nous avons estimé que l'accès à EURODAC à des fins répressives constituait une sérieuse atteinte contre les droits d'un groupe vulnérable, et avons demandé si cet accès était réellement nécessaire et proportionné.

Même si des preuves solides et des statistiques fiables devaient démontrer la nécessité et la proportionnalité de l'accès par les services répressifs aux données d'EURODAC, nous restons convaincus que la proposition devrait prévoir des garanties plus efficaces, comme par exemple une indication claire que l'auteur des faits a introduit une demande d'asile, une vérification réellement indépendante et des conditions d'accès pour Europol identiques à celles applicables aux États membres.

3.4.7. Commission CRIM du Parlement européen

Créée en 2012, la commission spéciale de la criminalité organisée, de la corruption et du blanchiment de capitaux (CRIM) du Parlement européen a pour objectif d'analyser et d'évaluer l'ampleur de ces activités et leur impact sur l'EU ainsi que l'état actuel de mise en œuvre de la législation de l'UE en la matière.

À la fin de son mandat, le 1er avril 2013, la commission CRIM doit présenter ses recommandations de politique concernant les mesures et initiatives à prendre dans ces domaines et dans les domaines politiques connexes liés à la sécurité. Ces questions ont des conséquences considérables pour la protection des données, et nous nous réjouissons donc d'avoir reçu une invitation permanente aux réunions de la commission CRIM. Nous avons suivi les travaux de la commission et apporté des contributions lorsque cela était utile.

3.5. Marché intérieur comprenant des données financières

En 2012, nous avons adopté une série d'avis portant sur les mesures relatives au marché intérieur. Certains de ces avis portent plus spécifiquement sur les marchés financiers.

3.5.1. Coopération administrative en matière d'accises

Le 27 janvier 2012, nous avons adopté un avis sur la proposition de la Commission portant sur un règlement du Conseil relatif à la coopération administrative en matière d'accises. Cette proposition vise notamment à réviser les dispositions relatives aux échanges d'informations automatiques et sur demande entre États membres.

Une coopération plus étroite entre les autorités fiscales pourrait contribuer à la lutte contre la fraude en matière d'accises, mais nous estimons que des garanties plus solides sont nécessaires concernant le traitement et l'échange des informations.

3.5.2. Révision de la directive sur les qualifications professionnelles

Le 8 mars 2012, nous avons adopté un avis sur la proposition de la Commission visant à moderniser et à modifier le texte existant de la directive sur les qualifications professionnelles. Les deux principaux aspects de cette proposition sont la mise en place d'un système d'alerte et l'introduction d'une carte professionnelle volontaire européenne. Le traitement des informations personnelles se fera via le système d'information du marché intérieur (IMI). Nous avons insisté pour que le système d'alerte proposé reste proportionné et demandé des garanties supplémentaires en matière de protection des données. Compte tenu du principe de proportionnalité et de l'équilibre entre les droits et les intérêts, y compris en ce qui concerne la présomption d'innocence, nous avons notamment recommandé que la proposition: précise que des alertes peuvent être envoyées uniquement après une décision prise par une autorité compétente ou un tribunal d'un État membre interdisant à une personne d'exercer ses activités professionnelles sur son territoire; précise que l'alerte ne doit pas contenir d'informations concernant les circonstances ou les raisons de cette interdiction; clarifie et limite au strict minimum la période de conservation des alertes; veille à ce que l'autorité destinataire préserve le caractère confidentiel des informations d'alerte reçues, et ne les distribue ni ne les publie, sauf si ces informations ont été rendues publiques en vertu de la législation de l'État membre qui les envoie.

3.5.3. Propositions de réforme des marchés financiers

Plusieurs propositions dans le domaine financier ont suscité les mêmes préoccupations en matière de protection des données, ce qui montre qu'un effort concerté est nécessaire pour intégrer des garanties en matière de protection des données aux propositions dans ce domaine.

Le 10 février 2012, nous avons publié une série de quatre avis sur des propositions de réforme de la législation européenne relative aux marchés financiers présentées par la Commission. Les quatre propositions portent toutes sur le contrôle des données financières, ce qui a une incidence considérable sur le droit fondamental à la protection des informations personnelles. Ces avis concernent la révision de la législation bancaire, la directive et le règlement sur les abus de marché (RAM et DAM), le règlement et la directive sur les marchés des instruments financiers (MIFID/MIFIR), et la révision du règlement relatif aux agences de notation de crédit (ANC).

Tous ces avis soulèvent des préoccupations similaires en matière de protection des données. C'est pourquoi nous avons émis les recommandations globales suivantes: l'inclusion de dispositions de fond soulignant l'applicabilité de la législation existante en matière de protection des données; l'ajout de garanties spécifiques aux dispositions permettant le transfert de données vers des pays tiers; la restriction de l'accès aux locaux privés; la limitation des enregistrement téléphoniques et des données relatives au trafic aux cas où des infractions graves à la législation proposée ont été identifiées; la définition claire des catégories de données concernant les appels téléphoniques et les données relatives au trafic qui doivent être conservées par les établissements financiers et/ou communiquées aux autorités de contrôle; l'évaluation de la nécessité et de la proportionnalité des dispositions proposées concernant la publication des sanctions, accompagnée de garanties adéquates; la garantie de la protection de

l'identité des personnes qui dénoncent des abus; la garantie du droit de toute personne accusée d'être défendue et entendue, ainsi que son droit à un recours judiciaire effectif contre toute décision ou mesure la concernant.

3.5.4. Contrôles légaux

Le 13 avril 2012, nous avons publié un avis sur deux propositions de la Commission concernant le contrôle légal des comptes annuels et des comptes consolidés. Ces propositions ont suscité des préoccupations en matière de protection des données dans divers domaines, parmi lesquels l'échange d'information, l'archivage, la publication de sanctions et le signalement des infractions.

3.5.5. Fonds européens de capital-risque et fonds d'entreprenariat social

Le 14 juin 2012, nous avons publié un avis sur la proposition de règlement relatif aux fonds européens de capital-risque et la proposition de règlement relatif aux fonds européens d'entreprenariat social. Notre principale préoccupation était que les règlements proposés sont trop généraux en ce qui concerne la protection des données. Dans certains cas, il était difficile de savoir si le traitement des informations personnelles aura lieu en vertu de certaines dispositions des règlements proposés, par exemple en ce qui concerne les échanges d'informations, les pouvoirs d'enquête des autorités compétentes, et la création de bases de données par l'Autorité européenne des marchés financiers (AEMF).

3.5.6. Amélioration du règlement des opérations sur titres dans l'Union européenne

Le 9 juillet 2012, nous avons publié un avis concernant une proposition de la Commission concernant l'amélioration du règlement des opérations sur titres dans l'Union européenne et chez les dépositaires centraux de titres. Cette proposition posait le problème des pouvoirs d'enquête des autorités concernées et de l'échange ou du transfert d'informations, ce qui nécessite la mise en place de garanties particulières.

3.5.7. Détachement de travailleurs effectué dans le cadre d'une prestation de services

Le 19 juillet 2012, nous avons rendu un avis concernant la proposition de la Commission portant sur une directive du Parlement européen et du Conseil relative à l'application de la Directive 96/71/CE concernant le détachement de travailleurs effectué dans le cadre d'une fourniture de services et sur la proposition de la Commission portant sur un règlement du Conseil relatif à l'exercice du droit de mener des actions collectives dans le contexte de la liberté d'établissement et de la libre prestation des services, également présentée par la Commission.

Nous nous sommes réjouis des efforts consentis dans cette proposition pour répondre aux préoccupations de protection des données et du fait qu'elle propose d'utiliser un système d'information existant,

le système d'information du marché intérieur (IMI), pour la coopération administrative. Du point de vue pratique, l'IMI offre déjà des garanties en matière de protection des données. Il subsiste néanmoins certaines inquiétudes concernant principalement les échanges bilatéraux, l'accès aux registres et le «système d'alerte». Nous avons recommandé des clarifications et des garanties supplémentaires pour répondre à ces préoccupations.

3.5.8. Intermédiation en assurance, organismes de placement collectif en valeurs mobilières et produits de placement

Le 23 novembre 2012, nous avons publié un avis sur trois propositions de la Commission concernant des documents d'information essentiels pour les produits d'investissement de détail, la médiation en assurance et pour les personnes qui achètent des fonds d'investissement. Nos principales préoccupations en matière de protection des données concernaient la nécessité de clarifier les pouvoirs d'enquête des autorités compétentes, la création d'une base de données par l'Autorité européenne des assurances et des pensions professionnelles (AEAPP), la publication des sanctions administratives, y compris l'identité des personnes responsables, et le signalement des infractions (système dits de «dénonciation des abus»).

3.6. Stratégie numérique et technologie

En 2012, la Commission a consacré des efforts importants à la mise en œuvre de la stratégie numérique et du programme UE 2020. Plusieurs de ces initiatives étaient extrêmement pertinentes pour la protection des données et ont donc été suivies de près par le CEPD.

Outre les initiatives mentionnées ci-dessous, le CEPD a également donné des conseils sur d'autres propositions figurant dans le plan d'action de la stratégie numérique, à savoir le cadre législatif en matière de gestion collective des droits d'auteurs et des droits voisins, et en matière de licences multi-territoriales, la proposition de système de règlement en ligne des litiges à l'échelle de l'UE[11], la communication relative à un Agenda du consommateur européen[12] et la communication relative à un centre européen de lutte contre la cybercriminalité[13].

3.6.1. Informatique en nuage

Le 16 novembre 2012, nous avons adopté un avis concernant la communication de la Commission intitulée «Exploiter le potentiel de l'informatique en

[11] Voir point 3.7.1.

[12] Voir point 3.7.3.

[13] Voir point 3.4.3.

nuage en Europe» afin de mettre en exergue les défis en matière de protection des données inhérents à l'informatique en nuage. Avec l'accès aux données dans le nuage, la responsabilité et l'obligation de rendre des comptes restent au cœur de la plupart de ces problèmes. C'est pourquoi nous avons insisté sur l'importance de définir des bases juridiques pour ces principes de protection des données et pour d'autres afin d'éviter toute ambiguïté dans leur applicabilité et leur mise en oeuvre pratique.

En plus de réagir à la communication, notre avis a mis en évidence les défis en matière de protection des données suscités par l'informatique en nuage et montré comment le règlement proposé relatif à la protection des données permettra de s'attaquer à ces problèmes une fois les règles réformées en vigueur.

Dans notre avis relatif à l'informatique en nuage, nous avons souligné la nécessité pour les prestataires de services en nuage d'assumer la responsabilité des services qu'ils proposent afin de leur permettre, ainsi qu'à leurs clients, de respecter leurs obligations en matière de protection des données.

Nous avons également montré que le règlement proposé relatif à la protection des données définit des règles claires qui, une fois adoptées, permettront d'éviter que les responsabilités en matière de protection des données ne disparaissent dans le nuage. Nous avons également précisé que la complexité de la technologie utilisée pour l'informatique en nuage ne justifie aucun relâchement des normes de protection des données.

Parmi nos recommandations, nous avons conseillé aux décideurs politiques responsables:

- d'élaborer des conditions commerciales standardisées respectant les obligations de protection des données pour les contrats commerciaux, les marchés publics et les transferts internationaux de données;
- d'apporter des précisions et des orientations supplémentaires sur la façon de garantir l'efficacité des mesures de protection des données dans la pratique et l'utilisation de règles d'entreprise contraignantes;
- de contribuer à l'élaboration de bonnes pratiques dans des domaines tels que la responsabilité du responsable du traitement et du sous-traitant, la portabilité des données, et l'exercice des droits des personnes concernées;
- d'élaborer des normes et des systèmes de certification qui intègrent pleinement les critères de protection des données et qui définissent sur le plan juridique la notion de transfert et les critères permettant aux organismes répressifs des pays non membres de l'EEE d'accéder aux données dans le nuage.

3.6.2. Paquet «Ouverture des données»

Le 18 avril 2012, nous avons adopté un avis sur le paquet de mesures «ouverture des données» dans lequel nous mettons en évidence la nécessité de garanties spécifiques de protection des données dans tous les cas où les informations du secteur public (ISP) contiennent des informations personnelles. Nous recommandons aux organismes du secteur public d'adopter une approche proactive lorsqu'ils mettent des informations personnelles à disposition en vue d'une réutilisation, et nous recommandons également que l'organisme du secteur public concerné procède à une évaluation de la protection des données avant la mise à disposition de toute ISP contenant des données personnelles.

La proposition devrait comporter une clause de protection des données dans les termes de la licence de réutilisation des ISP. Le cas échéant, il convient également de rendre les données entièrement ou partiellement anonymes, de définir des conditions de licence interdisant spécifiquement la ré-identification de personnes et la réutilisation d'informations personnelles à des fins susceptibles d'avoir des conséquences pour les personnes concernées.

La Commission devrait en outre élaborer des orientations supplémentaires en matière d'anonymisation et d'octroi de licence, et consulter le groupe de travail de l'article 29 sur la protection des données, un organe consultatif composé des autorités chargées de la protection des données des États membres de l'UE et du CEPD.

3.6.3. Compteurs intelligents

Le 8 juin 2012, nous avons adopté un avis sur la recommandation de la Commission relative à la préparation de l'introduction des réseaux électriques intelligents.

Dans notre avis, nous avons rappelé que, si l'introduction des réseaux électriques intelligents à l'échelle européenne est susceptible d'apporter des avantages importants, elle permettra également la collecte massive d'informations personnelles permettant de suivre les actions des membres d'un

ménage au sein de leur propre foyer. Nous avons donc prévenu qu'en l'absence de garanties adéquates, le profilage des consommateurs permettrait de suivre bien plus que la consommation d'énergie.

À la lumière de ces risques, nous avons invité la Commission à examiner la nécessité éventuelle d'actions législatives supplémentaires au niveau de l'Union. Nous avons également fourni des recommandations pragmatiques en vue d'actions législatives de ce type et indiqué que certaines de ces actions pourraient déjà être mises en œuvre par une modification de la directive sur l'efficacité énergétique, qui faisait l'objet de discussions au Conseil et au Parlement à l'époque. Cette modification devrait au moins inclure l'obligation, pour les responsables du traitement, de procéder à une évaluation de l'impact sur la protection des données et de notifier les violations de données à caractère personnel.

Dans l'attente de nouvelles mesures législatives ou en complément de ces mesures, nous avons proposé que le modèle d'évaluation de l'impact sur la protection des données (EIPD) soit préparé par le groupe de travail «réseaux intelligents» de la Commission et fournisse des orientations supplémentaires concernant la base juridique du traitement et les choix proposés aux personnes concernées (y compris la fréquence de relevé des compteurs), sur l'utilisation de technologies renforçant le respect de la vie privée et d'autres techniques disponibles pour réduire au minimum les données collectées, et sur les périodes de conservation et la manière de fournir aux consommateurs un accès direct à leurs données de consommation énergétique. Nous avons également recommandé de communiquer aux consommateurs leurs profils personnels, la logique des algorithmes éventuels utilisés pour l'exploration des données ainsi que les informations concernant la fonctionnalité d'activation/désactivation à distance.

3.6.4. Règlement sur les services de confiance électronique

Le 27 septembre 2012, nous avons adopté un avis concernant la proposition de la Commission de règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, qui remplacera le cadre juridique actuel sur les signatures électroniques (défini par la directive 1999/93/CE). Cette proposition a pour objectif de renforcer la confiance dans les transactions électroniques à l'échelle européenne et de garantir la reconnaissance juridique transfrontalière des services d'identification, d'authentification et de signature électronique et des services de confiance y afférents.

Nous avons insisté sur l'obligation de respecter la législation relative à la protection des données pour toutes les activités de traitement régies par cette proposition. Nous avons recommandé, en particulier de fournir aux utilisateurs des services de confiance électroniques des informations adéquates concernant le traitement de leurs données à caractère personnel, de spécifier les types d'informations personnelles traitées aux fins d'identification transfrontalière, de promouvoir, dans les services électroniques, l'utilisation de techniques de prise en compte du respect de la vie privée dès la conception permettant de ne pas divulguer d'informations personnelles, ou en tout cas d'en divulguer le moins possible (par ex. utilisation de pseudonymes), de définir un ensemble commun d'obligations de sécurité en matière de services de confiance et de systèmes d'identification, de faire en sorte que les obligations en cas d'infraction aux règles de protection des données introduites dans la proposition soient conformes à celles prévues par les autres instruments législatifs sur la protection des données (directive sur la vie privée dans les communications électroniques et proposition de règlement sur la protection des données).

3.6.5. Un internet mieux adapté aux enfants

Le 17 juillet 2012, nous avons rendu un avis sur la stratégie européenne pour un internet mieux adapté aux enfants, présentée par la Commission. Cette stratégie énumère différentes mesures à prendre par l'industrie, les États membres et la Commission. Ces mesures incluent la promotion des contrôles parentaux, des paramètres de sécurité, des indications relatives à l'âge, des outils de signalement, des lignes d'assistance téléphonique, et une coopération entre l'industrie, les services d'assistance téléphonique et les organismes répressifs.

Nous avons salué la reconnaissance de la protection des données en tant qu'élément essentiel et montré par des exemples précis comment renforcer la protection et la sécurité des enfants en ligne du point de vue de la protection des données. Nous avons notamment recommandé d'inclure des références aux risques pour la protection des données et aux outils de prévention dans les campagnes de sensibilisation, d'appliquer des paramètres de confidentialité par défaut plus protectifs pour les enfants, y compris par une modification des paramètres par défaut, de mettre en place des outils adéquats de vérification de l'âge qui ne soient pas intrusifs du point de vue de la protection des données, d'éviter les actions ciblant spécifiquement les mineurs à des fins de marketing direct ou de publicité basée sur le comportement. Nous avons invité la Commission à encourager les mesures d'autorégulation en faveur du respect de la vie privée et à examiner la possibilité de mesures législatives supplémentaires au niveau de l'UE.

Nous avons également exprimé des préoccupations concernant les initiatives de lutte contre les abus sexuels et l'exploitation sexuelle d'enfants sur l'inter-

net, et recommandé notamment une base juridique adéquate pour les outils de signalement, avec une définition claire du type d'activité illégale susceptible de faire l'objet d'un signalement; une meilleure définition et l'harmonisation des procédures de signalement par les services d'assistance téléphonique, par exemple par l'adoption d'un code de pratique européen définissant des procédures communes de signalement et un modèle de signalement intégrant des garanties en matière de protection des données; des conditions plus claires et mieux définies pour la coopération entre l'industrie et les services répressifs.

Il convient de trouver un juste équilibre entre l'objectif légitime de lutte contre les contenus illégaux et la nature des moyens mis en œuvre. Certaines tâches, comme la surveillance des réseaux de télécommunications, devraient rester principalement du ressort des services répressifs.

3.6.6. Sécurité des réseaux et de l'information dans l'UE

Dans nos observations du 10 octobre 2012 concernant une stratégie pour la sécurité des réseaux et de l'information (SRI) dans l'UE, nous avons souligné l'importance de tenir compte de la protection des données au moment de l'élaboration d'une telle stratégie. Nous nous sommes concentrés sur la définition claire des menaces de cybersécurité et leur signalement ainsi que les conditions et garanties applicables à l'échange d'informations entre les acteurs privés et les organismes publics. Nous avons également insisté sur le fait que cette initiative constitue une occasion de mettre en œuvre le principe de respect de la vie privée dès la conception.

3.6.7. Internet ouvert et neutralité du réseau

Le 15 octobre 2012, en réponse à la consultation publique de la Commission, nous avons indiqué que les pratiques en matière de gestion du trafic sur l'internet suscitaient des préoccupations en matière de protection des données, comme le souligne notre avis sur la neutralité du réseau (7 octobre 2011).

Différents principes de protection des données, comme les principes de limitation de la finalité, de proportionnalité et de responsabilité, devraient notamment guider la mise en place de méthodes alternatives moins susceptibles de porter atteinte à la vie privée. Nous avons également suggéré diverses mesures que les prestataires de services internet pourraient prendre pour accroître la transparence de leurs pratiques de gestion du trafic pour les utilisateurs finaux, notamment en fournissant des informations sur les formes de traitement plus intrusives et sur la façon dont les utilisateurs finaux peuvent retirer leur consentement lorsque celui-ci sert de base juridique au traitement.

3.7. Santé publique et consommateurs

En 2012, nous avons adopté un ensemble d'observations formelles et trois avis concernant la santé publique et les consommateurs en réponse à différentes propositions de la Commission.

3.7.1. Règlement transfrontalier alternatif des litiges de consommation et règlement relatif à une plate-forme de règlement en ligne des litiges

Le 12 janvier 2012, nous avons adopté un avis sur la proposition de directive sur le règlement transfrontalier alternatif des litiges de consommation et sur la proposition de règlement instituant une plate-forme de règlement en ligne des litiges.

Ces propositions tenaient déjà compte des principes de protection des données, mais nous avons recommandé de préciser les responsabilités des responsables du traitement, d'en informer les personnes concernées et de clarifier la limitation des droits d'accès.

3.7.2. Système d'alerte précoce et de réaction et menaces transfrontalières contre la santé

Le 28 mars 2012, nous avons adopté un avis sur la proposition de la Commission d'étendre le système existant d'alerte précoce et de réaction (SAPR) de manière à inclure les nouvelles menaces transfrontalières pour la santé, comme les risques d'origine biologique, chimique ou environnementale.

Nous avons recommandé de clarifier les règles relatives au traçage des contacts ainsi que la relation entre le SAPR et les réseaux de surveillance ad hoc proposés. Nous avons également recommandé de préciser les prescriptions en matière de sécurité des données et de confidentialité.

3.7.3. Agenda du consommateur européen

Le 16 juillet 2012, nous avons publié des observations sur l'agenda du consommateur européen – *Favoriser la confiance et la croissance* -, qui proposait la création de synergies entre les initiatives relatives aux consommateurs et celles visant à renforcer la protection des informations personnelles, en particulier dans l'environnement numérique.

Les campagnes de sensibilisation, les programmes de formation et les codes de conduite tels que ceux proposés par l'agenda du consommateur européen

peuvent être encore plus efficaces s'ils intègrent des éléments liés au respect de la vie privée et à la protection des données.

3.7.4. Essais cliniques

Le 19 décembre 2012, nous avons adopté un avis sur la proposition de la Commission relative aux médicaments à usage humain. Nous avons salué l'attention accordée spécifiquement à la protection des données dans cette proposition de règlement, mais nous avons également identifié des possibilités d'amélioration.

Nous recommandons que le règlement proposé fasse explicitement référence au traitement des informations personnelles concernant la santé, qu'il indique clairement s'il est prévu de traiter des informations personnelles concernant la santé dans les bases de données européennes utilisées pour les essais cliniques et, dans l'affirmative, à quelles fins, qu'il mentionne le droit des personnes concernées de bloquer leurs informations personnelles, et qu'il prévoie une période maximale de conservation des informations personnelles stockées.

3.8. Publication d'informations personnelles

La création d'un équilibre entre la transparence et la protection des données est un thème récurrent de notre travail. En 2012, nous avons adopté plusieurs avis portant principalement sur la publication des informations personnelles.

Il y a eu tout d'abord la série d'avis publiée le 10 février sur différentes propositions relatives aux marchés financiers[14]. Ces propositions concernaient notamment la dénonciation publique («naming and shaming») d'entreprises et de personnes. Des questions similaires ont été abordées dans les avis relatifs à l'amélioration du règlement des opérations sur titres dans l'Union européenne[15] (9 juillet), à l'intermédiation en assurances, aux OPCVM, et aux documents d'information essentiels pour les produits de placement[16] (23 novembre).

Dans tous ces avis, nous avons insisté sur la nécessité de trouver un équilibre entre le principe de transparence, le droit au respect de la vie privée et à la protection des données, et la nécessité de garanties précises. Nous avons insisté sur le fait que le respect de la vie privée et la protection des données n'ont pas pour fonction d'empêcher l'accès public à l'information dès lors que des informations personnelles sont concernées, ni de limiter la transparence de manière injustifiée. Le respect de la vie privée et la protection des données doivent permettre de publier des informations personnelles uniquement lorsque cette publication se justifie et d'une façon qui tienne compte des différents intérêts en jeu.

La portée de la divulgation publique d'informations personnelles devrait faire l'objet d'une analyse proactive dès les premières étapes, et il convient d'informer les personnes impliquées en conséquence afin de leur permettre de faire valoir leurs droits.

Le 18 avril 2012, nous avons adopté un avis relatif au paquet «ouverture des données»[17]. Comme cette proposition comportait des mesures visant à faciliter une réutilisation publique plus large des informations du secteur public (ISP), nous avons demandé plus de détails concernant les situations possibles dans lesquelles des informations person-

[14] Voir point 3.5.3.

[15] Voir point 3.5.6.

[16] Voir point 3.5.8.

[17] Voir point 3.6.2.

nelles peuvent être mises à disposition en vue d'une réutilisation et sous quelles conditions.

Nous avons analysé les différents propositions à la lumière des arrêts de la Cour de justice dans les affaires *Bavarian Lager* (C-28/08P) et *Schecke* (C-92/09 et C-93/09). La modification de la proposition relative au financement, à la gestion et au suivi de la politique agricole commune (PAC), à propos de laquelle nous avons adopté un avis le 9 octobre 2012, faisait suite à l'arrêt *Schecke*, qui annule la législation européenne relative à la divulgation des informations personnelles des agriculteurs recevant des fonds européens parce que des méthodes moins intrusives pour la vie privée n'avaient pas été envisagées.

Dans différentes propositions, la Commission s'est clairement efforcée de trouver un équilibre entre la transparence et la protection des données dans la législation proposée. Nos principales observations concernaient l'absence de définition claire de la finalité de la divulgation.

Ces propositions n'indiquaient pas non plus que les méthodes, modalités et niveaux de détail adéquats pour la publication d'informations personnelles avaient été examinés minutieusement dans le but de définir l'approche la moins intrusive. Nous avons souvent dû rappeler le caractère sensible des informations concernées (par ex. les données personnelles révélatrices d'opinions politiques ou relatives à des délits), qu'il convient de prendre en considération pour déterminer et justifier leur publication et pour définir les garanties adéquates.

Il en va de même pour la proposition relative au statut et au financement des partis et fondations politiques européens, à propos de laquelle nous avons adopté un avis le 13 décembre 2012. Dans nos recommandations, nous avons abordé un certain nombre de détails pertinents concernant la publication des données relatives aux membres, donateurs et contributeurs de ces organes.

3.9. Autres questions

En 2012, nous avons également rendu des avis sur des dossiers pour lesquels la protection des données n'était pas une question centrale, mais plutôt connexe: la proposition de règlement instituant le Corps volontaire européen d'aide humanitaire et la proposition par la Commission de règlement du Conseil en ce qui concerne le dépôt des archives historiques des institutions à l'Institut universitaire européen de Florence.

3.10. Politique du CEPD en matière d'accès aux documents

En tant qu'institution européenne, le CEPD est soumis au règlement de 2001 relatif à l'accès public aux documents. Le nombre de demandes d'accès public à des documents détenus par le CEPD a augmenté par rapport aux deux années précédentes. En 2012, nous avons reçu **10** demandes d'accès à des documents et nous avons été consultés à **deux reprises** par d'autres institutions à propos de demandes qui leur avaient été soumises. L'accès aux documents ou à l'information a été accordé dans ces 12 cas.

Afin de consolider notre pratique existante et de garantir une application uniforme des règles, nous avons adopté un manuel destiné à guider le personnel du CEPD dans le traitement des demandes d'accès public. Un assistant a été spécifiquement

chargé de cette mission afin de garantir la mise en œuvre correcte de ce manuel.

Nous prévoyons également de consacrer une rubrique de notre site Web à notre politique de transparence, ce qui illustre l'importance que nous accordons à cette question. Cette rubrique présentera notre politique et contiendra un outil convivial de demande d'accès aux documents. Il est prévu de lancer cette page Web spéciale en 2013.

3.11. Affaires judiciaires

Aucune décision du CEPD n'a été contestée devant la Cour de justice de l'Union européenne en 2012, et nous n'avons intenté aucune action contre d'autres institutions ou organes de l'UE. La Cour a statué dans deux affaires dans lesquelles nous étions intervenus. Nous avons également demandé l'autorisation d'intervenir dans deux autres affaires encore pendantes.

Le premier arrêt portait sur le manque d'indépendance allégué de l'autorité autrichienne chargée de la protection des données, la *Datenschutzkommission* (DSK). Dans l'affaire *Commission c. Autriche* (affaire C-614/10), nous sommes intervenus pour le compte de la Commission.

Dans son arrêt du 16 octobre 2012, la Cour a conclu que la DSK autrichienne ne répondait pas aux normes d'indépendance définies par la directive sur la protection des données. La Cour a notamment jugé que l'indépendance fonctionnelle de la DSK par rapport au gouvernement, prévue par le droit autrichien, ne suffisait pas, et que ses liens étroits avec la Chancellerie fédérale l'empêchaient de se placer au-dessus de tout soupçon de partialité.

Il s'agissait de la deuxième affaire devant la Cour portant sur l'indépendance des autorités chargées de la protection des données, après *Commission c. Allemagne* (affaire C-518/07), dans laquelle nous étions également intervenus pour le compte de la Commission. Nous avons accueilli avec beaucoup de satisfaction l'arrêt de la Cour du 9 mars 2009, qui était largement conforme avec les arguments avancés dans notre intervention et lors de l'audience au tribunal du mois d'avril.

Avec l'arrêt dans l'affaire *Commission c. Autriche*, nous estimons que la Cour a une fois de plus souligné l'obligation légale d'indépendance complète des autorités chargées de la protection des données. Cet arrêt confirme l'importance de la protection des données en tant que droit fondamental et la nécessité de garantir l'impartialité pour protéger efficacement ce droit dans la législation nationale. La décision de la Cour est importante également pour la révision du cadre en matière de protection des données, qui doit renforcer le rôle des autorités de protection des données.

Nous sommes également intervenus dans l'affaire *Egan et Hackett c. Parlement européen* (affaire T-190/10). Il s'agit de la dernière de trois affaires dans lesquelles le Tribunal général a dû se prononcer sur la relation entre le règlement sur l'accès public aux documents et le règlement relatif à la protection des données depuis l'arrêt dans l'affaire Bavarian lager c. Commission du 29 juin 2010 (affaire C-28/08 P). Nous étions également intervenus dans les deux autres affaires, à savoir *Valero Jordana c. Commission* (affaire T-161/04) et *Dennekamp c. Parlement européen* (affaire T-82/09), tranchées en 2011.

Dans cette dernière affaire, les deux demandeurs avaient demandé l'accès public à deux documents concernant les demandes d'indemnité d'assistance parlementaire de deux députés européens et dans lesquels le nom d'assistants parlementaires étaient mentionnés. Le Parlement a refusé cet accès, arguant que ces noms constituaient des informations personnelles dont la divulgation porterait atteinte à la vie privée des personnes concernées.

Le CEPD est intervenu pour le compte du demandeur et a fait valoir que le Parlement n'avait pas procédé à une analyse concrète et individuelle au titre du règlement sur l'accès aux documents et qu'il n'avait pas envisagé les possibilités d'accès au titre du règlement sur la protection des données. Dans son arrêt du 28 mars 2012, la Cour a annulé ce refus, le Parlement n'ayant pas démontré dans quelle mesure la divulgation de documents contenant les noms d'anciens assistants d'un député européen porterait spécifiquement et effectivement préjudice au droit à la vie privée de ces personnes.

La première affaire encore pendante au moment de la rédaction du présent rapport est une autre procédure d'infraction concernant l'indépendance des autorités chargées de la protection des données, cette fois contre la Hongrie (affaire C-288/12). Le CEPD a demandé l'autorisation d'intervenir.

La deuxième affaire pendante est *ZZ* c. *BEI*, devant le Tribunal de la fonction publique (affaire F-103/11).

Au cours d'une enquête interne pour harcèlement menée par la BEI, la plainte complète concernant le harcèlement allégué, y compris les documents associés (parmi lesquels des déclarations médicales), a été envoyée aux personnes accusées du harcèlement. Le demandeur considérait que la communication de ces documents était contraire au règlement sur la protection des données. Le CEPD est intervenu en soutien du demandeur dans la mesure où sa demande reposait sur une violation des règles en matière de protection des données.

En 2012, le CEPD a suivi de près plusieurs autres affaires sans toutefois intervenir. Dans l'affaire Google en Espagne (affaire C-313/12), des questions ont été soumises à la Cour de justice concernant l'applicabilité de la législation espagnole mettant en œuvre la directive européenne sur la protection des données aux activités de Google, qui sont pour la plupart effectuées physiquement en dehors de l'UE.

Deux autres affaires ont concerné la validité de la directive européenne sur la conservation des données. Cette directive impose aux États membres d'obliger les prestataires de services de télécommunications à conserver les données d'appel de leurs clients (à l'exception du contenu des conversations) pendant une période allant de 6 à 12 mois. En Allemagne, après l'annulation de la mesure de mise en œuvre par le Tribunal constitutionnel, aucune nouvelle législation n'a été adoptée. La Commission européenne a intenté une action contre l'Allemagne pour non-respect de la législation de l'Union, puisqu'elle n'avait pas mis en œuvre la directive (affaire C-329/12). L'Allemagne a justifié son inaction en arguant que la directive était contraire à la Charte des droits fondamentaux. La même question relative au respect des droits fondamentaux par la directive sur la conservation des données a été soulevée dans une décision préjudicielle demandée par un tribunal irlandais (affaire C-293/12). La Cour de justice n'a statué dans aucune de ces trois affaires en 2012.

3.12. Priorités pour 2013

En janvier 2013, le CEPD publiera son septième inventaire public en tant que conseiller sur les propositions législatives européennes, définissant nos priorités dans le domaine de la consultation pour l'année à venir. Nous devrons relever le défi de remplir un rôle sans cesse croissant dans la procédure législative, tout en garantissant une contribution qualitative élevée et appréciée, à partir de ressources limitées.

Plusieurs tendances qui se sont dégagées ces dernières années méritent une attention particulière du point de vue de la protection des données:

1. La nécessité de prendre en compte les implications sur la protection des données et la vie privée des propositions législatives devient essentielle dans tous les domaines de la politique de l'UE. Il est de plus en plus évident que le droit fondamental à la protection des données ne peut être réglé que par la seule législation en matière de protection des données, et que de nombreuses autres politiques doivent prendre en compte la protection des données.
2. Il existe une tendance croissante à doter les autorités administratives, à la fois au niveau de l'UE et au niveau national, de puissants outils d'enquête et de collecte d'information. Cela concerne particulièrement l'espace de liberté, de sécurité et de justice et la révision du cadre législatif concernant la surveillance financière.
3. Dans ce contexte, l'importance croissante du contrôle de l'internet par les autorités publiques et par des parties privées doit être envisagée par rapport aux irrégularités commises sur l'internet, qu'il s'agisse de lutter contre la pédopornographie, la cybercriminalité ou les atteintes aux droits de propriété intellectuelle.
4. La législation de l'UE facilite de plus en plus d'importants échanges d'informations entre les autorités nationales, impliquant souvent des organes de l'UE et des bases de données à grande échelle (avec ou sans unité centrale) d'une taille et d'une puissance de traitement croissantes. Cela nécessite un examen minutieux de la part des décideurs et des acteurs lors de la définition des exigences de protection des données lors de la procédure législative, en raison des conséquences que ces échanges peuvent avoir sur la protection de la vie privée des citoyens, par exemple en facilitant la surveillance des citoyens.
5. Ces dernières années ont été caractérisées par des développements technologiques impressionnants, essentiellement en raison de l'utilisation généralisée de l'internet et des technologies de positionnement par satellite. De tels développements ont des répercussions importantes sur les droits des citoyens en matière de protection de la vie privée et des données.

Ces développements stratégiques et technologiques soulignent que la protection des données et de la vie privée est vraiment devenue une question horizontale. Cela signifie également que nous allons recevoir un nombre croissant de demandes de conseils concernant des propositions de mesures législatives à un moment où les ressources sont limitées.

C'est pourquoi l'un des principes généraux de notre stratégie pour 2013-2014 est que nous allons agir de façon sélective et proportionnée et concentrer notre attention et nos efforts sur les domaines de politique qui ont l'impact le plus important sur le respect de la vie privée.

Moyennant ces considérations, nous nous engageons à consacrer des ressources considérables en 2013 à l'analyse des propositions d'importance stratégique.

Nous avons également recensé plusieurs initiatives de moindre importance stratégique qui peuvent néanmoins être pertinentes pour la protection des données. Le fait que ces initiatives figurent dans notre inventaire implique qu'elles seront régulièrement surveillées, mais pas qu'elles feront systématiquement l'objet d'un avis ou d'observations formelles de notre part.

Nos principales priorités, telles qu'elles sont définies dans notre programme, sont les suivantes:

a. Vers un nouveau cadre juridique de la protection des données
   - Propositions du 25 janvier en vue d'un règlement général sur la protection des données et d'une directive dans le domaine de la justice pénale
   - Propositions à venir, en particulier concernant la protection des données dans les institutions et organes de l'Union européenne

b. Développements technologiques et agenda numérique, droits de propriété intellectuelle et internet
   - Surveillance sur l'internet (par ex. lutte contre la pédopornographie et mise en application des droits de propriété intellectuelle)
   - Cybersécurité
   - Informatique en nuage

c. Développement de l'espace de liberté, de sécurité et de justice
   - Réforme d'Eurojust
   - Réforme d'Europol
   - Cybercriminalité
   - Paquet «frontières intelligentes»
   - Négociations sur les accords avec les pays tiers en matière de protection des données

d. Secteur financier
   - Réglementation et supervision des marchés et acteurs financiers
   - Surveillance bancaire
   - Lutte contre le blanchiment de capitaux

e. «Santé électronique»
   - Propositions relatives aux essais cliniques et aux dispositifs médicaux
   - Plan d'action «santé électronique»

4 COOPÉRATION

Notre objectif stratégique

Améliorer la coopération avec les autorités chargées de la protection des données, notamment le groupe de travail «Article 29», afin de garantir une cohérence accrue dans le domaine de la protection des données au sein de l'UE.

Nos principes directeurs

- Nous nous appuyons sur notre expertise et notre expérience concernant la législation et les pratiques européennes en matière de protection des données.
- Nous cherchons à améliorer la cohérence de la législation relative à la protection des données au sein de l'UE.

4.1. Groupe de travail «Article 29»

Le groupe de travail «Article 29» sur la protection des données (le Groupe de travail) est un organe consultatif indépendant institué par l'article 29 de la directive 95/46/CE. Il fournit à la Commission européenne des avis indépendants sur des questions concernant la protection des données et contribue à l'élaboration de politiques harmonisées dans ce domaine au niveau des États membres de l'UE.

Le Groupe de travail se compose de représentants des autorités nationales chargées de la protection des données, du CEPD et de la Commission (cette dernière assure également son secrétariat). Il joue un rôle essentiel pour garantir l'application homogène de la directive 95/46/CE.

En 2012, nous avons continué de contribuer activement aux activités du Groupe de travail, en particulier par notre participation aux sous-groupes thématiques Frontières, Voyages et domaine répressif, Gouvernement en ligne, Questions financières, Futur du respect de la vie privée, Transferts internationaux, Dispositions-clés et Technologie.

Nous avons également rempli les fonctions de rapporteur ou co-rapporteur pour l'avis sur la limitation des finalités et l'utilisation compatible (sous-groupe Dispositions-clés), pour l'avis sur les modèles d'évaluation des incidences des réseaux électriques intelligents sur la protection des données (sous-groupe Technologie), et pour l'avis sur l'ouverture des données (sous-groupe Gouvernement en ligne). L'adoption de ces trois avis est prévue pour 2013.

Nous avons également contribué de façon significative aux avis adoptés en 2012 concernant, notamment les débats sur la réforme de la protection des données (deux avis)[18], l'informatique en nuage[19], l'exemption de consentement en matière de cookies[20] et les évolutions des technologies biométriques[21].

Nous avons également contribué à d'autres activités du Groupe de travail dans les cas où ce dernier a fait

[18] Avis 08/12 apportant une contribution supplémentaire aux débats relatifs à la réforme de la protection des données - WP 199, 05.10.2012 ; avis 01/2012 sur les propositions de réforme de la protection des données – WP 191, 23.03.2012

[19] Avis 05/2012 sur l'informatique en nuage – WP 196, 01.07.2012

[20] Avis 04/2012 sur l'exemption de consentement en matière de cookies - WP 194, 07.06.2012

[21] Avis 03/2012 sur les évolutions des technologies biométriques - WP 193, 27.04.2012

état de sa position sous forme de lettres. On citera notamment la lettre sur les modifications apportées à la politique de respect de la vie privée de Google.

Nous coopérons également avec les autorités nationales chargées de la protection des données dans la mesure nécessaire à l'accomplissement de ses devoirs, notamment en échangeant toutes informations utiles et en leur demandant ou en leur fournissant une aide à l'accomplissement de leurs fonctions (article 46, point f), tiret i, du règlement (CE) n° 45/2001). Cette coopération se fait au cas par cas.

La coopération directe avec les autorités nationales est un aspect de plus en plus important dans le contexte du développement de grands systèmes internationaux tels EURODAC, qui requièrent une approche coordonnée du contrôle (voir point 4.2).

4.2. Supervision coordonnée

4.2.1. EURODAC

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

EURODAC est un système d'information à grande échelle consacré au stockage des empreintes digitales des demandeurs d'asile et des personnes arrêtées alors qu'elles franchissaient de manière irrégulière les frontières extérieures de l'Union européenne et de plusieurs pays associés[22].

Le groupe de coordination du contrôle d'EURODAC est composé de représentants des autorités nationales chargées de la protection des données et du CEPD. Nous assurons également le secrétariat du groupe et, à ce titre, nous avons organisé deux réunions à Bruxelles en 2012, l'une en juin et l'autre en novembre. Le groupe a basé ses activités de 2012 sur le programme de travail 2010-2012 et plusieurs initiatives ont été lancées en 2012:

[22] Islande, Norvège, Suisse et Liechtenstein.

Méthodologie pour les inspections nationales

L'une des principales réalisations du groupe cette année a été le plan d'inspection normalisé pour les points d'accès nationaux (PAN) d'EURODAC, adopté lors de la réunion de novembre. Le questionnaire a pour objet de faciliter les inspections nationales, sans toutefois être prescriptif. Il couvre les procédures formelles et informelles en place pour garantir la sécurité et la licéité, ainsi que la conformité aux autorisations de la collecte, du stockage, de la manipulation, de la transmission et de tout autre traitement d'informations d'EURODAC au niveau des PAN et de l'unité centrale, ainsi qu'entre les PAN et l'unité centrale.

Exercice sur les empreintes digitales illisibles

Au cours des deux réunions d'EURODAC de 2012, les préparatifs en cours en vue de l'exercice sur les empreintes digitales illisibles ont été examinés. Le consensus au sein du groupe est que l'adoption d'une pratique uniforme au sein de l'UE profiterait aussi bien aux demandeurs d'asile qu'aux autorités chargées de l'asile. Les travaux se poursuivent et l'adoption du rapport définitif est prévue pour le milieu de l'année 2013.

La prochaine réunion du groupe EURODAC aura lieu au printemps 2013.

4.2.2. VIS

Le système d'information sur les visas (VIS) est une base de données, incluant des données biométriques, sur les demandes de visas par les ressortissants des pays tiers. Ces informations sont collectées lorsqu'une demande de visa est introduite auprès d'un consulat de l'UE et servent à empêcher la fraude en matière de visas ainsi que les demandes de visas multiples dans les divers États membres (*visa shopping*), à faciliter l'identification des détenteurs de visas au sein de l'Union européenne et à vérifier que le demandeur et l'utilisateur du visa sont la même personne. Le VIS a été déployé sur une base régionale et est devenu opérationnel en Afrique du Nord en octobre 2011. Le VIS a ensuite été mis en service dans deux autres régions, au Proche-Orient en mai 2012 et dans la région du Golfe en octobre 2012.

En novembre 2012, nous avons accueilli la première réunion du groupe de coordination de la supervision du VIS. Ce groupe, composé des autorités nationales chargées de la protection des données et du CEPD, est chargé de superviser le déploiement progressif du système, d'examiner les problèmes éventuels, par exemple les questions liées à l'externalisation de certaines tâches par les États membres, et de partager les expériences nationales.

Le groupe VIS a discuté de son premier projet de programme de travail et échangé des informations

concernant les activités du CEPD et les inspections nationales dans les divers États membres. La prochaine réunion sera organisée au printemps 2013.

4.2.3. SID

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

Le SID enregistre des informations relatives aux produits de base, aux moyens de transport, aux personnes et aux entreprises, aux marchandises et aux liquidités détenues, saisies ou confisquées. Ces informations peuvent aider à prévenir, à rechercher et à poursuivre les opérations qui sont contraires aux réglementations douanières ou agricoles (ancien premier pilier de l'UE) ou les infractions graves aux lois nationales (ancien troisième pilier de l'UE). Du fait de sa base juridique, ce dernier aspect est contrôlé par une autorité de contrôle commune composée de représentants des autorités nationales chargées de la protection des données.

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

Ce groupe de coordination:

- analyse les problèmes de mise en œuvre liés aux activités du SID;
- analyse les difficultés rencontrées lors des vérifications par les autorités de contrôle;
- analyse les difficultés d'interprétation ou d'application du règlement SID;
- formule des recommandations en vue d'apporter des solutions communes aux problèmes existants;
- s'efforce d'améliorer la coopération entre les autorités de contrôle.

[23] Règlement (CE) n° 766/2008 du Parlement européen et du Conseil du 9 juillet 2008 modifiant le règlement (CE) n° 515/97 du Conseil relatif à l'assistance mutuelle entre les autorités administratives des États membres et à la collaboration entre celles-ci et la Commission en vue d'assurer la bonne application des réglementations douanière et agricole

Nous assurons le secrétariat du groupe SID et, à ce titre, nous avons organisé deux réunions à Bruxelles en 2012, l'une en juin et l'autre en décembre. Lors de la réunion du mois de juin, le groupe a adopté, en collaboration avec l'ACC Douane, un avis conjoint relatif au manuel FIDE ainsi que le rapport d'activité pour les deux années précédentes. À l'issue de discussions concernant l'état d'avancement de la refonte du règlement (CE) n° 515/1997, deux documents de travail ont été distribués au groupe. Ces deux documents vont être étoffés pour en faire des rapports à part entière d'ici à la prochaine réunion.

Lors de la réunion de décembre, le CEPD a présenté les points essentiels du suivi des contrôles préalables de l'OLAF. Cette présentation a été suivie d'une présentation par la Commission (OLAF) sur les développements récents dans l'évaluation des incidences de la modification du règlement n° 515/97 du Conseil et sur les développements techniques du SID. Le secrétariat a présenté deux projets de rapports qui, sous réserve de réponses encore à recevoir et de clarifications supplémentaires, exposaient les grandes lignes des activités possibles du groupe pour 2013, notamment l'évaluation du caractère approprié de l'accès au SID et à FIDE et l'analyse des possibilités de sensibilisation aux droits des personnes concernées.

4.3. Conférence européenne

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

La **Conférence européenne des commissaires à la protection des données** s'est tenue à Luxembourg les 3 et 4 mai 2012. Elle a été consacrée principalement aux développements récents dans la modernisation des cadres de protection des données de l'UE, du Conseil de l'Europe et de l'OCDE. La Conférence a reconnu les efforts actuels visant à renforcer les droits des citoyens et des consommateurs et à permettre l'exercice effectif de ces droits, tout en tenant compte de l'évolution technologique et de la mondialisation.

La conférence a accordé une attention importante à la réforme européenne de la protection des données. Les commissaires à la protection des données ont adopté une résolution saluant de nombreux aspects des propositions de la Commission visant à renforcer les droits des personnes et à assurer une plus grande homogénéité. Mais ils ont aussi relevé la nécessité d'améliorations supplémentaires, notamment pour faire en sorte que la directive proposée dans les domaines de la police et de la justice respecte les principes fondamentaux du règlement général proposé en matière de protection des données.

4.4. Conférence internationale

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

La 34e **Conférence annuelle des commissaires à la protection de la vie privée et à la protection des données** s'est déroulée en Uruguay les 25 et 26 octobre 2012, avec plus de 90 orateurs représentant 40 pays. Le thème général de cette conférence était *l'équilibre entre la technologie et le respect de la vie privée*, et elle s'est concentrée principalement sur le phénomène de la circulation massive des données («big data»). Peter Hustinx, contrôleur, et Giovanni Buttarelli, contrôleur adjoint, faisaient partie des orateurs et ont animé divers panels de discussion.

La conférence a adopté deux résolutions, l'une sur l'informatique en nuage, l'autre sur l'avenir du respect de la vie privée. La conférence a également mis l'accent sur la nécessité d'une coopération renforcée pour garantir un niveau élevé de respect de la vie privée, de protection des données, et de sécurité informatique, afin de réduire les risques associés à l'utilisation des services d'informatique en nuage et de faire face plus efficacement aux défis communs et aux problèmes futurs en matière de respect de la vie privée.

La Déclaration de l'Uruguay sur le profilage a été adoptée à la suite des discussions qui se sont tenues à Mexico en 2011 sur le volume croissant d'informations personnelles collectées et traitées par des entités du secteur privé et du secteur public dans le monde entier (circulation massive de données). Cette déclaration souligne que les principes généraux en matière de protection des données et de respect de la vie privée, et notamment le principe de limitation de la finalité, resteront le fondement de l'évaluation des opérations de traitement.

De nombreuses manifestations connexes ont été organisées avant ou parallèlement à cette conférence, comme par exemple la conférence Public Voice, avec la participation de la société civile et une réception organisée par le Conseil de l'Europe pour célébrer l'adhésion prochaine de l'Uruguay à la Convention 108 en tant que premier membre non européen.

La 35e Conférence internationale aura lieu à Varsovie en septembre 2013.

4.5. Pays tiers et organisations internationales

4.5.1. Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Ouverte à la signature en 1981, la Convention 108 du Conseil de l'Europe définit une série de garanties en matière de protection des données pour les individus à la lumière de la communication transfrontalière croissante de données dans le cadre des processus automatisés. Cette convention a servi de base à la directive 95/46/CE et fait aujourd'hui elle-même l'objet d'un processus de révision distinct. En sa qualité d'observateur habilité à intervenir, le CEPD a assisté en 2012 à deux réunions du Comité consultatif de la convention 108, l'une en septembre et l'autre en novembre. Il était particulièrement important pour nous d'assister à ces réunions afin de suivre et d'influencer la modernisation en cours de la Convention.

Lors de la réunion de septembre, le Bureau du Comité consultatif a discuté des modifications proposées au texte de la Convention. Nous avons proposé diverses façons de renforcer la protection des données, par exemple en harmonisant le texte proposé de façon à assurer la cohérence interne de la Convention, en conservant l'exigence *de consentement explicite*, et en clarifiant la différence entre *traitement* et *fichier*. À l'issue de cette réunion, une version modifiée a été distribuée en vue de recevoir des commentaires écrits.

Le nouveau projet provisoire de Convention, qui tient compte d'un grand nombre de nos recommandations, a été adopté lors de la réunion de novembre. À la fin de cette réunion, il a été décidé d'envoyer un projet de Convention actualisée au Conseil des ministres au début de l'année 2013.

4.5.2. Atelier international sur la protection des données dans les organisations internationales

WORLD CUSTOMS ORGANIZATION
ORGANISATION MONDIALE DES DOUANES

Les 8 et 9 novembre 2012, l'Organisation mondiale des douanes (OMD), avec le soutien du CEPD, a organisé à Bruxelles le 4e Atelier international sur la protection des données dans les organisations internationales. Cet atelier a été l'occasion d'un forum de discussion sur la protection des données dans les organisations internationales. Il a réuni des professionnels des institutions et des organes de l'UE, ainsi que des organisations internationales pour des discussions et un échange de bonnes pratiques.

Au cours de ces deux journées, plusieurs panels de discussion animés par des représentants du CEPD et de l'OMD ont été organisés. Les participants ont reçu des informations actualisées concernant les évolutions récentes présentant un intérêt pour les organisations internationales, notamment celles qui concernent la protection des données (Conseil de l'Europe et OCDE), le paquet de réformes de la protection des données en Europe, la conformité et le transfert de données à des parties tierces, le traitement des données des membres du personnel, la notification des failles de sécurité et l'informatique en nuage. Une fois de plus, cet atelier a permis de faciliter les échanges entre les participants et a ainsi contribué à une coopération et à un partage d'expériences encore plus poussés entre les DPD des institutions et des organes de l'UE et les représentants concernés des autres organisations internationales.

5 SUIVI DE LA TECHNOLOGIE

5.1. Évolution technologique et protection des données

Les développements technologiques ont souvent été la cause de défis pour le respect de la vie privée. Les nouvelles technologies de l'information et de la communication ont, à leur tour, également suscité des réactions législatives et réglementaires. Les avancées rapides des technologies informatiques concernent une grande partie de la société, avec les risques que cela entraîne du point de vue du traitement des informations personnelles, ce qui confère une importance plus grande encore au respect de la vie privée et à la protection des données.

Pour pouvoir travailler de façon utile dans ce domaine, les autorités chargées de la protection des données, en ce compris le CEPD, doivent fournir des analyses tenant compte des possibilités et des menaces engendrées par la technologie actuelle. C'est pourquoi, dans le cadre de notre processus de révision stratégique évoqué au chapitre 1.2, nous avons ajusté notre structure organisationnelle interne et créé un secteur «Politique IT» afin de disposer des connaissances et de l'expertise nécessaires et de renforcer notre aptitude à suivre les évolutions technologiques. Ce chapitre s'inscrit dans cette perspective et illustre l'analyse prospective de nos experts en informatique dans les différentes matières abordées.

Ce nouveau secteur analyse en permanence les évolutions technologiques et leur incidence potentielle sur la protection des données et soutient ainsi notre mission de supervision et de mise en application ainsi que nos activités de politique législative et de coopération.

- Nous participons activement à divers groupes de travail, sous-groupes technologiques du groupe de travail «Article 29», groupes de travail de la Commission et initiatives de normalisation, ainsi qu'à des conférences sélectionnées pour nous permettre de rester au fait des évolutions pertinentes pour la protection des données et des meilleures pratiques technologiques.
- Nous nous efforçons d'améliorer nos capacités de supervision technique et de fournir des orientations sur les aspects techniques du respect des règles de protection des données par les responsables du traitement. Nous offrons également des conseils techniques dans le cadre de lignes directrices particulières.
- Nous conseillons le législateur européen sur la façon de tenir compte des effets des initiatives et mesures politiques et législatives liées à la technologie sur le respect de la vie privée.
- Nous appliquons les principes de protection des données à nos propres activités informatiques en interne, par exemple pour l'hébergement du futur système de gestion des dossiers.

5.2. Développements technologiques futurs

5.2.1. Les principes de la protection des données doivent s'appliquer aux nouvelles technologies

Depuis ses débuts dans les années 1970, le potentiel du traitement automatique des données a été une force motrice des efforts de la société visant à protéger les droits fondamentaux des personnes. Même à l'époque, avec de gros ordinateurs moins puissants que les smartphones actuels, les partisans de la protection des données avaient conscience du potentiel de la technologie d'exercer un contrôle sur les personnes et de restreindre les libertés individuelles.

Les principes de base que sont la transparence, la limitation de la finalité, la réduction au minimum des données collectées, et la supervision indépendante ont constitué le fondement de la protection des données et se sont développés parallèlement aux changements sociétaux, économiques et technologiques. Ces principes ont été définis avec une incroyable prescience et restent valide dans le monde actuel. Ayant surmonté les restrictions techniques du passé, nous nous trouvons confrontés aujourd'hui à des modes de traitement entièrement nouveaux. Il est donc d'autant plus nécessaire de contrôler et d'évaluer ces développements technologiques afin de garantir leur efficacité pour la protection des données. Le règlement sur la protection des données qui a institué le CEPD nous charge d'effectuer ce suivi et d'informer le public et le législateur européen de la pertinence de ces développements.

5.2.2. Développement des activités

Les données massives (*big data*) seront l'un des moteurs du développement des technologies de l'information et de la communication.

Il est généralement admis que les évolutions désignées par le terme «données massives» sont le résultat direct des progrès de la technologie de l'information, qui permettent la création d'entrepôts de données de plusieurs pétaoctets et le traitement d'énormes quantités d'information à un coût abordable. Certains affirment que la production quotidienne de données a atteint 2,5 milliards de milliards d'octets[24], ce qui signifie que 90 % du contenu numérique existant a été produit au cours des deux dernières années. Le rythme de cette production ne peut qu'augmenter à l'avenir.

Les quantités sont impressionnantes, mais il reste à en définir la qualité. La notion de *données massives* n'a pas encore de définition universelle claire. On parle actuellement de données massives pour désigner les quantités massives de données de différents types utilisées pour améliorer l'expérience du consommateur et, en bout de course, augmenter le retour sur investissement[25]. Les développements futurs permettront de définir plus précisément le concept de *données massives* et de différencier les différentes catégories et les champs d'application.

Les mesures actuelles de mise en œuvre de politique d'ouverture des données, qui permettent une exploitation dans le secteur privé de données provenant du secteur public, devraient devenir un élément important des initiatives de traitement des données massives. Parallèlement, le nombre des applications d'analyse gérant différentes formes de données produites par des utilisations individuelles (par exemples des données textuelles, vidéo et audio) va augmenter considérablement.

La clarification du concept sera accompagnée d'efforts visant à surmonter les difficultés techniques causées par le traitement de volumes aussi importants de données. Le secteur public comme le secteur privé a intérêt à produire des *informations utilisables*[26], permettant d'améliorer l'efficacité, la productivité, la prise de décisions et les performances de façon générale.

Avec une meilleure compréhension des méthodes et des outils utilisés pour l'analyse des données massives et la différenciation des domaines d'application, il apparaîtra clairement que toutes les données massives ne sont pas nécessairement des données *personnelles*. Néanmoins, il ne fait aucun doute que le traitement des données massives créera des défis pour la protection des informations personnelles. Ce problème est déjà visible dans le domaine des *données sociales* produites par l'utilisation active des réseaux sociaux.

Les services de réseaux sociaux ont mûri et sont devenus utilisables par toutes les générations et les professions.

Les services de réseaux sociaux doivent continuer d'attirer de nouveaux utilisateurs pour survivre, quand ne serait-ce que pour rajeunir leur population, et on peut s'attendre à ce que la quantité de *données sociales* produites par chaque utilisateur augmente. Cette augmentation sera provoquée dans une cer-

[24] <http://www-01.ibm.com/software/data/bigdata/>

[25] M. Schroeck, R. Shockley, J.t Smart, D. Romero-Morales and P. Tufan ' Analytics: The real-world use of big data. How innovative enterprises extract value from uncertain data' <http://public.dhe.ibm.com/common/ssi/ecm/en/gbe03519usen/GBE03519USEN.PDF>

[26] Voir note de bas de page 25

taine mesure par le développement de nouvelles fonctionnalités et par une utilisation plus intensive d'applications dans les services de médias sociaux, sur les diagrammes sociaux de leurs utilisateurs.

L'augmentation de l'activité entraînera une augmentation des flux constants d'actualité et du temps d'utilisation. Mais surtout, pour tirer un avantage financier de leur travail, les services de réseaux sociaux s'efforcent d'enrichir leurs bases d'informations personnelles en travaillant en partenariat avec des services externes. Les utilisateurs des réseaux sociaux ont déjà accès, sur la base des coordonnées de leur profil social, à divers services et plates-formes en ligne, comme du contenu (musique, vidéo), des jeux, des services sociaux spéciaux (rencontres, voyages) ou des sites d'achats. Grâce à ces connexions, un service de réseau social peut collecter des informations concernant les transactions effectuées par ses utilisateurs sur ces services liés et peut accroître la valeur commerciale de sa collection de données, par exemple à des fins de marketing et de publicité.

En outre, on peut s'attendre à ce que les médias sociaux proposent de nouveaux services plus ciblés pour les entreprises comme pour les consommateurs sur la base d'une analyse et d'un profilage de plus en plus sophistiqués. Les diagrammes sociaux, c'est-à-dire la représentation des relations entre les personnes qui utilisent un service de réseau social, vont probablement fournir des informations plus détaillées concernant certains groupes d'utilisateurs (exploitation de préférences pour certaines marques ou célébrités par l'adhésion à des pages de «fans», etc.). Des services basés sur ces techniques sont également proposés aux consommateurs et permettent d'effectuer des recherches plus exhaustives sur la base de leur profil personnel afin d'intensifier les relations sur la base d'intérêts communs.

L'intérêt des entreprises pour l'utilisation commerciale des données de localisation va entraîner le développement de techniques avancées d'anonymisation.

Les capacités de collecte de données des dispositifs de communication dépassent désormais les simples données de communication. Les *services mobiles basés sur la localisation* joueront un rôle essentiel dans l'utilisation croissante des données de localisation. Les données de localisation sont très sensibles pour le respect de la vie privée, c'est pourquoi le législateur européen a imposé des limites strictes à leur utilisation, par exemple dans la législation relative aux communications électroniques et à la conservation des données de communication à des fins répressives.

Les données de localisation provenant d'autres sources, par exemple de l'utilisation de puces RFID ou de l'internet des objets en général, ont fait l'objet d'un débat politique et scientifique visant à réduire les conséquences de ces technologies pour le respect de la vie privée. En quête de moyens d'augmenter leurs revenus, les entreprises vont s'intéresser naturellement aux énormes quantités de données de localisation produites par les systèmes d'informations géographiques et les systèmes de positionnement par satellite, qui font partie intégrante de la plupart des appareils de communication intelligents. Mais pour tirer profit de l'utilisation des services basés sur la localisation, l'industrie doit gagner la confiance des consommateurs et veiller à ce que ceux-ci aient conscience de la collecte et de l'utilisation de leurs données.

L'utilisation d'algorithmes d'anonymisation est un moyen possible d'atténuer l'impact des données de localisation sur le respect de la vie privée. L'efficacité de l'«anonymisation des données de localisation» pour protéger la vie privée est un sujet controversé parmi les spécialistes de l'informatique. Il y a de fortes raisons de penser que la suppression de toutes les caractéristiques permettant d'identifier les données n'est pas effective. D'autres techniques comme le «floutage» (réduire la précision de la localisation) et l'exclusion de certaines zones (sphère privée) du suivi de la localisation, ou encore la restriction des périodes de suivi, sont des options complémentaires possibles.

Il ne fait aucun doute que ces techniques vont attirer l'attention de l'industrie[27]. L'expérience des pratiques actuelles sur certains marchés comme la Chine, le Japon et la Corée du Sud sera adaptée aux cadres africain, européen et nord-américain.

On prévoit une augmentation de la demande de dispositifs intégrés de sécurité et de protection de la vie privée dans les appareils de communication intelligents.

Les dispositifs de communication intelligents, comme les smartphones, ordinateurs, tablettes et autres services connectés, étendent et transforment nos possibilités d'interaction. La collecte, la communication et le traitement de données en temps réel offrent des services à valeur ajoutée sans précédent aux utilisateurs. Il peut s'agir de services contextuels liés aux données de localisation, aux capteurs de proximité et à l'ajustement automatique aux préférences des consommateurs, mais aussi de services mobiles de santé par lesquels des informations médicales sont traitées et communiquées aux praticiens et aux centres de santé, ou encore l'utilisation de smartcards pour les paiements au moyen de smartphones, rendue possible par la technologie NFC[28].

[27] Pour de plus amples informations, voir J. Wood, «Preserving Location Privacy by Distinguishing between Public and Private Spaces» http://locationanonymization.com/PrivateSpaces.pdf

[28] Near Field Communication

Dans cet environnement, les utilisateurs doivent faire face à des défis de contrôle et de gestion des données. Les informations sont souvent collectées par défaut et d'une façon non transparente. Des volumes considérables d'informations sont transférés aux propriétaires des applications et à des entreprises qui conçoivent des publicités basées sur le comportement sans obtenir un consentement donné librement et en connaissance de cause, en donnant des informations inadéquates, voire sans donner d'informations sur le mode de collecte de ces données, les raisons de la collecte, et l'utilisation prévue des informations personnelles. La sécurité mobile n'est pas encore suffisamment mûre pour gérer le caractère critique des informations traitées.

L'adoption de dispositifs intelligents et de services connexes et leur utilisation en toute sécurité nécessiteront donc absolument des environnements mobiles sécurisés, dignes de confiance et propices au respect de la vie privée, offrant aux utilisateurs une expérience d'utilisation sans accrocs. Tous les acteurs de la chaîne de valeur, en ce compris les développeurs de plates-formes, les développeurs d'applications, les sites de distribution d'applications et les opérateurs de réseaux, doivent contribuer à cette évolution.

L'utilisation de réseaux électriques intelligents sera un avantage, une fois surmontés les problèmes de sécurité et de respect de la vie privée.

La production, la distribution et l'utilisation intelligentes et rationnalisées d'énergie, et en particulier d'électricité et de gaz, sont indispensables à une économie durable. Les réseaux électriques intelligents sont considérés comme des éléments essentiels pour garantir la disponibilité de l'approvisionnement énergétique et pour permettre aux clients (particuliers et industrie) de réduire leurs coûts et d'adopter un comportement écologique. À cet effet, des informations relatives aux utilisateurs sont collectées, principalement des données de consommation, par le biais des relevés périodiques, et peut-être, à l'avenir, d'autres informations plus détaillées.

L'industrie, les associations de consommateurs et les autres parties prenantes collaborent avec la Commission afin de coordonner les actions en vue du déploiement de réseaux électriques intelligents. Des efforts de normalisation et d'autres activités sont en cours pour garantir l'interopérabilité, la sécurité de fonctionnement et l'acceptation des utilisateurs, en montrant les avantages de cette approche et en garantissant le respect de la vie privée et la protection des informations personnelles des consommateurs.

La mise en place de réseaux électriques intelligents aura pour effet d'accroître les risques pesant sur la sécurité et la confidentialité. L'utilisation de différents réseaux de communication et la réorientation des activités de sabotage informatique vers les infrastructures critiques, l'industrie et l'internet des objets augmenteront les risques en matière de cybersécurité. La collecte d'informations relatives au comportement des consommateurs pourrait pousser les fournisseurs d'énergie à exploiter financièrement les informations personnelles.

Il faudra protéger la vie privée des clients en garantissant le respect de principes fondamentaux tels que la réduction des données au minimum, l'évitement de la collecte de données, la nécessité et la limitation de la finalité. Le respect de la vie privée dès la conception et l'utilisation des meilleures techniques disponibles sont des principes de respect de la vie privée dont il faut assurer le respect, par exemple par le recours à des techniques d'anonymisation, de pseudonymisation et de regroupe-

ment. Les analyses d'impact relatives à la protection des données (AIPD) permettent d'évaluer les risques pour le respect de la vie privée.

Afin d'accroître le nombre des utilisateurs, les prestataires de services en nuage devront respecter leurs obligations en matière de protection des données.

L'*informatique en nuage* devrait bouleverser fondamentalement le secteur informatique. Par rapport au modèle traditionnel de services informatiques, elle peut offrir des avantages considérables aux particuliers comme aux organisations, par exemple grâce à des coûts réduits, à une flexibilité accrue, à une mise en œuvre plus rapide et à des prix calculés en fonction de l'utilisation et non des capacités. On s'attend à ce que le marché des services en nuage connaisse une croissance extrême.

Jusqu'à présent, son développement n'a pas encore tout à fait confirmé les attentes. De nombreuses entreprises craignent de perdre le contrôle de leur infrastructure d'information en passant au nuage, d'où le manque de confiance dans ce service. Certaines solutions d'informatique en nuage présentent un risque élevé d'attachement forcé à long terme à un même fournisseur. Les inquiétudes relatives à la sécurité sont également perçues comme un réel problème. Les technologies permettant de résoudre ces problèmes n'en sont encore qu'à leurs débuts et sont conçues pour des fournisseurs spécifiques ou pour des solutions spécifiques de «logiciel en tant que service». Des efforts considérables de développement et de normalisation sont nécessaires pour assurer des niveaux de sécurité largement acceptés.

L'informatique en nuage est une tendance que les institutions européennes ne peuvent clairement pas ignorer. Il va donc falloir élaborer des lignes directrices pour l'utilisation de l'informatique en nuage par les administrations publiques. Comme nous l'indiquions dans notre avis récent à ce sujet, l'un des principaux défis est que les clients de l'informatique en nuage n'ont généralement que très peu d'influence sur les conditions proposées par les fournisseurs. Et pourtant, ces clients doivent s'assurer que ceux-ci respectent leurs obligations en matière de protection des données.

5.2.3. Répression et sécurité

Des méthodes innovantes vont être développées pour recueillir des preuves à partir de l'environnement en nuage.

À mesure que l'informatique en nuage deviendra plus répandue, on peut s'attendre à ce qu'elle attire des applications criminelles, que ce soit en tant que ressource à l'appui d'activités criminelles ou en tant que cible de ces activités. Face à cette évolution, les autorités répressives devront trouver de nouvelles façons de mener des enquêtes et de rassembler et de préserver des preuves.

La criminalistique du nuage est une discipline nouvelle consistant à utiliser des moyens scientifiques pour recenser, recueillir, examiner et analyser les données du nuage, tout en préservant l'intégrité des informations et en maintenant une stricte chaîne de surveillance des données. L'environnement en nuage accroît la complexité en ce que les preuves peuvent être recueillies à distance depuis des machines disponibles sur le réseau et à grande échelle.

Ce processus est rendu plus complexe par la nécessité d'impliquer de nombreux acteurs du nuage comme les fournisseurs de services, les consommateurs, les intermédiaires, les opérateurs de réseaux et les contrôleurs, mais aussi par la présence d'«occupants» multiples et la répartition du nuage sur plusieurs juridictions. Dans ce contexte, les acteurs de la criminalistique du nuage pourraient facilement perdre de vue les considérations liées au respect de la vie privée. Il est indispensable de développer des solutions créatives pour faire en sorte que les activités criminalistiques ne portent pas atteinte à la vie privée des personnes qui partagent l'informatique en nuage.

Les autorités chargées du contrôle de la protection des données seront confrontées aux mêmes difficultés.

Les contrôles automatisés aux frontières vont améliorer le contrôle des frontières.

Le nombre des voyageurs continue d'augmenter, et les infrastructures existantes aux points de passage des frontières vont subir une pression extrême pour faire face à l'augmentation des flux. De nouvelles approches et solutions sont actuellement en développement afin de maintenir un service à un prix raisonnable. Les *contrôles automatisés aux frontières* (CAF) visent à automatiser le contrôle des passagers aux points de passage des frontières par l'utilisation de nouvelles technologies sous le contrôle des gardes-frontières. Les gardes-frontières qui utilisent les CAF pourront se focaliser sur les personnes jugées à risques et permettre à la majorité des passagers d'utiliser le système automatisé.

Il existe un large consensus en faveur de l'utilisation des CAF, mais le calendrier et les méthodes restent à définir. En ce qui concerne le *calendrier*, les principaux défis consistent à garantir l'interopérabilité entre les systèmes au niveau global, à préparer les voyageurs à l'utilisation des CAF, et à former les gardes-frontières afin qu'ils puissent préserver un équilibre entre la sécurité et la facilité. Le *comment* reste à définir, mais il est évident que les données biométriques, qui restent préoccupantes du point de vue de la protection des don-

nées, joueront un rôle essentiel dans les CAF. À l'heure actuelle, les méthodes les plus couramment utilisées sont les empreintes digitales et la reconnaissance faciale. On s'attend toutefois à ce que d'autres techniques, comme la reconnaissance d'iris, soient introduites prochainement.

De plus, à mesure que les systèmes de contrôle aux frontières deviennent de plus en plus automatisés, on peut s'attendre à une demande d'intégration de ces systèmes avec des bases de données centrales (SIS, VIS, bases de données de criminels connus, etc.), ce qui suscitera aussi des préoccupations en matière de protection des données.

L'utilisation de scanners corporels portables va modifier l'approche des opérations de police.

Les scanners corporels sont utilisés dans les aéroports européens depuis environ 2007 et leur utilisation s'est étendue au monde entier. En 2010, la police néerlandaise envisageait l'utilisation de cette technologie sous forme portable dans les rues, afin de détecter les armes dissimulées à distance et d'éviter ainsi les fouilles corporelles individuelles. Des programmes similaires ont été lancés aux États-Unis. Au début de l'année 2012, la police de New York (NYPD) a lancé des tests de ces appareils montés sur des voitures de police. Le NYPD a reçu ces scanners corporels portables au début de l'année 2013.

On peut s'attendre à ce que l'utilisation des scanners corporels portables se répande aux États-Unis en 2013. Nous allons suivre de près les évolutions dans ce domaine en nous focalisant sur les projets d'utilisation de cette nouvelle technologie par les organismes européens chargés des missions de police. Dans un premier temps, ces scanners auront une portée et une résolution limitées. Mais la technologie va s'améliorer, la portée va augmenter de façon à permettre le contrôle des personnes en rue à leur insu et la résolution va progresser de façon à donner une image plus détaillée.

Les images de vidéo-surveillance seront analysées automatiquement en permanence.

Nous suivons l'utilisation des techniques de vidéo-surveillance depuis plusieurs années et, en 2012, nous avons publié des lignes directrices pour l'utilisation de la vidéo-surveillance dans les institutions et organes de l'UE. À mesure que l'utilisation de la vidéo-surveillance augmente, il en va de même pour le volume des informations à traiter. Les flux vidéo générés par les caméras de vidéo-surveillance contiennent des informations précieuses pour autant que le responsable du traitement dispose des ressources nécessaires pour en analyser le contenu.

Pour résoudre ce problème, les agences répressives recherchent des méthodes qui permettraient d'automatiser l'analyse des flux d'images de vidéo-surveillance. L'un des objectifs du projet INDECT financé par l'UE, par exemple, est de créer une solution d'observation intelligente des flux de vidéo-surveillance et de détecter automatiquement les comportements suspects ou les actes de violence dans les environnements urbains, avec à la clef un avertissement automatique des forces de l'ordre.

Les chercheurs travaillant sur des projets tels qu'INDECT doivent, entre autres, réfléchir à l'impact potentiel de ces outils et systèmes sur les droits fondamentaux au respect de la vie privée et à la protection des données en cas d'utilisation plus poussée des données. Pour trouver un juste équilibre dans un projet où la sécurité le dispute aux droits tels que le droit au respect de la vie privée, il est recommandé de tenir compte de cet équilibre dès le début du projet.

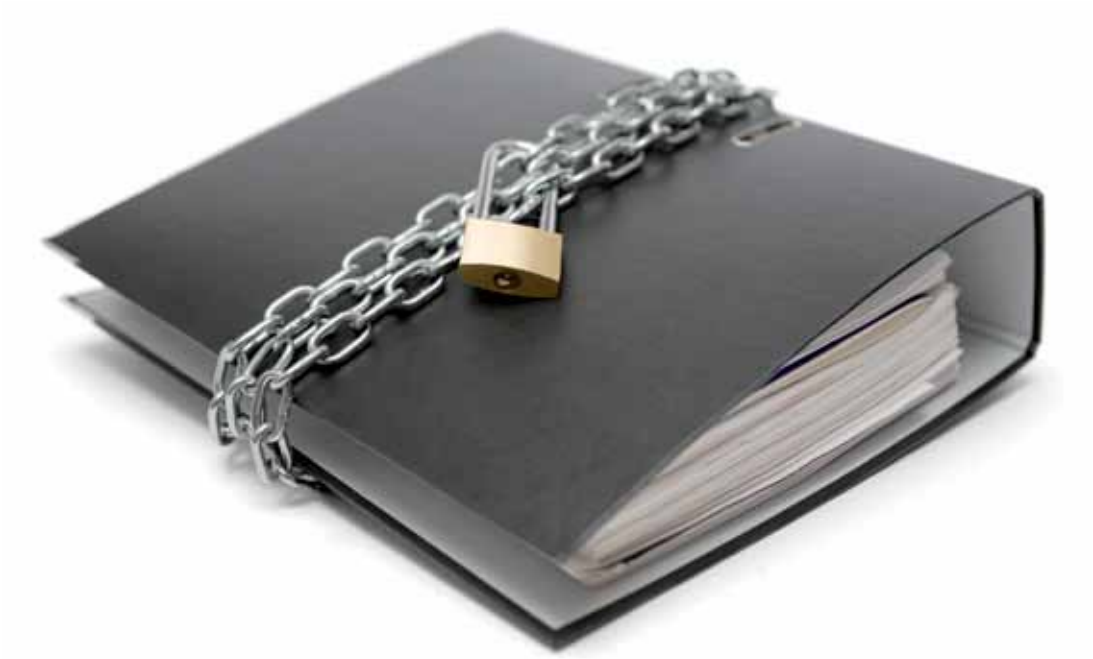
Des possibilités techniques comme l'anonymisation des données, les périodes de conservation limitées, etc. pourraient être intégrées dès le stade de la définition des objectifs du projet. Une technologie développée sans tenir compte de ces critères pourrait être difficile ou impossible à exploiter dans le respect des droits civils.

L'utilisation des drones ou avions sans pilote va retenir l'attention du public.

Les systèmes d'aéronefs pilotés à distance (*Remotely piloted aircraft systems*, RPAS), aussi appelés véhicules aériens sans pilote (*unmanned aerial vehicles*, UAV), avions sans pilotes ou encore drones, ont été développés à des fins militaires, et les forces armées restent leur principal domaine d'application. Récemment, des rapports publiés sur l'internet ont rapporté l'existence d'un drone équipé d'une caméra d'1,8 gigapixel volant à une altitude de 5,3 kilomètres et couvrant une superficie de 2,5 kilomètres carrés[29].

Des applications de recherches civiles et scientifiques présentant diverses caractéristiques sont aussi en fin de développement. Ces technologies utilisent généralement une forme de détection, de contrôle ou de surveillance à distance sur la base d'images enregistrées par une caméra haute défini-

[29] http://www.liveleak.com/view?i=e95_1359267780



tion. La technologie arrive à maturité et l'on peut s'attendre à ce qu'elle se répande largement dans le courant des prochaines années. À l'heure actuelle déjà, des drones ont été utilisés à des fins de surveillance lors de certains événements sportifs[30].

Afin d'examiner l'impact économique de cette technologie émergente, la DG Entreprise de la Commission a lancé une vaste consultation sur l'avenir des avions sans pilote en Europe. Les avions sans pilote peuvent assurer des services commerciaux précieux dans divers domaines, par exemple pour une gestion efficace de l'agriculture et des pêches, la surveillance des lignes électriques et des conduites de gaz, l'inspection des infrastructure, des services de communication et de télédiffusion, les systèmes de relais pour la communication sans fil et l'amplification des signaux satellitaires, le contrôle des ressources naturelles, les médias et le divertissement, la cartographie numérique, la gestion du territoire et de la faune ou encore le contrôle et la gestion de la qualité de l'air. La Commission prévoir un potentiel énorme pour cette technologie, et donc la nécessité d'adopter une législation afin d'intégrer les avions sans pilote en toute sécurité dans l'espace aérien européen.

Contrairement aux caméras de surveillance, les avions sans pilote volent. Ils ont donc la possibilité d'offrir une perspective unique en surveillant les espaces publics depuis les airs. Leur capacité de déplacement permet de suivre des objets ou des personnes en mouvement sans devoir regrouper différents flux vidéo issus d'un grand nombre de caméras fixes.

La surveillance par les avions sans pilote n'est pas toujours évidente et souvent quasi-anonyme. Même si les avions sans pilote n'emmènent pas d'équipage, ils sont pilotés manuellement et les images qu'ils enregistrent peuvent être introduites dans des systèmes d'analyse. En principe, ces images pourraient être conservées pour l'éternité. Les avions sans pilote sont une technologie en développement rapide qui va bouleverser notre conception de la surveillance et du contrôle.

5.2.4. Autres développements

La demande accrue de technologies de protection de la vie privée va susciter l'adoption de normes, de méthodes et d'outils de respect de la vie privée afin de garantir l'efficacité et la responsabilité.

La proposition de règlement général relatif à la protection des données impose aux responsables du traitement et aux sous-traitants de réaliser des études d'incidences pour les opérations de traitement de données présentant des risques spécifiques pour les droits et libertés des personnes concernées. Cette proposition impose également le *respect de la vie privée dès la conception* et *respect de la vie privée par défaut* afin de garantir une protection adéquate.

Les premiers efforts visant à définir un *cadre d'évaluation des incidences sur le respect de la vie privée* au niveau de l'UE ont été entrepris dans le contexte des applications RFID[31]. La seconde initiative est lancée par le secteur des réseaux électriques intelligents et par les parties intéressées. Le projet

[30] http://rt.com/news/london-olympics-security-drones-007/

[31] http://ec.europa.eu/information_society/policy/rfid/pia/index_en.htm

PIAF[32] cofinancé par la Commission, a publié ses objectifs fin 2012. Ces résultats comportent un certain nombre de recommandations concernant l'élaboration des politiques et les pratiques d'évaluation des incidences sur le respect de la vie privée. Le projet de normalisation de l'analyse des incidences sur le respect de la vie privée par l'Organisation internationale de normalisation (ISO) est attendu dans un avenir proche.

Des pratiques de mise en application du principe de respect de la vie privée dès la conception commencent à se développer d'élaboration dans les nombreux domaines où le respect de la vie privée est en jeu, comme la gestion de l'identité et de la confiance, les services d'informatique en nuage, les réseaux électriques intelligents, la biométrie, et bien d'autres. Il serait utile de tester et d'appliquer en production les connaissances accumulées dans le cadre de la recherche.

La gestion du respect de la vie privée et l'application du principe de respect de la vie privée dès la conception seront également soumises au processus de normalisation de l'ISO/CEI. La Commission compte examiner la possibilité de charger les organisations européennes de normalisation (CEN/CENELEC/ETSI) d'élaborer une norme de respect de la vie privée dès la conception dans le secteur de la sécurité.

Les fuites de données continueront de démontrer que personne n'est tout à fait à l'abri dans l'environnement en ligne.

Comme les années précédentes, toute une série d'entreprises et d'organisations ont connu des fuites de données en 2012. Les entreprises internationales en ligne et de grandes entreprises nationales dans lesquelles des informations concernant les clients avaient été compromises ont été impliquées dans un grand nombre d'affaires de violation de données à caractère personnel. Cela prouve une fois de plus qu'en ligne, personne n'est tout à fait à l'abri.

Lorsqu'une fuite de données est révélée publiquement, les conséquences sont généralement graves pour l'entité chargée de protéger les informations ainsi compromises. Il n'est pas rare d'entendre qu'une fuite de données a coûté des centaines de milliers d'euros (ou d'une autre devise) à corriger. On retiendra par exemple le cas de LinkedIn, un site bien connu de réseau social professionnel, qui a vu les mots de passe de ses utilisateurs publiés sur l'internet. LinkedIn dit avoir payé près d'un million de dollars (environ 740 000 euros) en frais d'analyses techniques et autres coûts de rétablissement pour cette seule fuite de données. Il n'existe pas d'informations concernant les coûts pour les utilisateurs, les véritables victimes de ces failles.

Selon le rapport 2012 de Verizon relatif aux enquêtes sur les fuites de données, 97 % des fuites «auraient pu être évitées par des contrôles de base ou intermédiaires». On peut s'attendre à ce que cette tendance malencontreuse se poursuive au cours des années à venir et à ce qu'il faille prendre plus de mesures pour assurer la sécurité de base et pour responsabiliser les responsables du traitement et les obliger à signaler les fuites de données aux personnes concernées. Des études publiées récemment aux États-Unis indiquent qu'une victime de fuite de données sur quatre est victime d'usurpation d'identité. Le préjudice qui en découle souligne la nécessité de suivre ces développements afin de garantir le plus possible le respect de la vie privée et la protection des données à caractère personnel.

[32] Le projet «A Privacy Impact Assessment Framework for data protection and privacy rights» (cadre d'évaluation des incidences sur le respect de la vie privée pour la protection des données et des droits liés à la vie privée), cofinancé par la Commission européenne, vise à encourager l'UE et ses États membres à adopter une politique progressive d'évaluation des incidences sur le respect de la vie privée afin de faire face aux besoins et aux défis en matière de respect de la vie privée et de traitement des données à caractère personnel.

6 INFORMATION ET COMMUNICATION

Notre objectif stratégique

Développer une stratégie de communication efficace.

6.1. Introduction

L'information et la communication sont importantes pour que notre voix soit entendue et comprise non seulement de l'administration européenne, mais aussi du grand public. Notre objectif est de sensibiliser l'opinion à la protection des données en tant que droit fondamental et élément essentiel d'une politique publique saine et de la bonne administration au sein des institutions de l'UE. À cette fin, nous avons adopté dans notre stratégie pour 2013-2014 l'objectif-clé de développer une stratégie de communication créative et efficace. Nous avons également inscrit à l'article 52 de notre règlement interne notre engagement de fournir des informations au public.

Grâce à cette stratégie, nous comptons faire du CEPD un point de référence au niveau de l'Union européenne pour toutes les questions relevant de

nos compétences, nous assurer une plus grande **visibilité** au niveau institutionnel, et **sensibiliser** toutes les parties concernées à nos activités principales (avis législatifs, avis de contrôle préalable, informations spécifiques aux personnes concernées, formation des délégués à la protection des données de l'UE) et à la protection des données en général.

Même si des progrès significatifs ont déjà été accomplis, il faut attirer encore plus l'attention sur notre rôle et notre mission au niveau de l'UE. Nos activités de communication sont essentielles pour y parvenir.

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

Les indicateurs comme le nombre de demandes d'information soumises par les citoyens, le nombre de demandes d'information et d'interview des médias, le nombre d'abonnés à notre newsletter, le nombre de personnes suivant le CEPD sur Twitter ainsi que le nombre d'invitations à venir s'exprimer à des conférences et le trafic sur le site internet montrent bien que nous sommes devenus un point de référence pour les questions de protection des données au niveau de l'Union européenne.

6.2. Caractéristiques de la communication

L'évolution de notre politique de communication est adaptée à notre public-cible. Tout en restant adaptable, elle repose sur les caractéristiques particulières de notre organisation en termes d'âge, de taille, de compétences et de besoins de nos parties prenantes.

6.2.1. Principaux publics et groupes cibles

Les politiques et les activités de communication de la plupart des autres institutions et organes de l'UE s'adressent généralement à l'ensemble des citoyens de l'Union. Notre champ d'action direct est plus restreint. Nous nous adressons avant tout aux parties prenantes du CEPD - aux institutions et organes de l'UE, aux personnes concernées en général, et au personnel de l'UE en particulier, aux acteurs politiques de l'UE, ainsi qu'aux personnes actives dans le secteur de la protection des données. Il n'est donc pas nécessaire que notre politique de communication recoure à une «communication de masse». Au contraire, la sensibilisation des citoyens de l'UE aux questions de protection des données, au niveau des États membres, repose sur une approche plus indirecte passant par exemple par les autorités nationales chargées de la protection des données.

Nous communiquons malgré tout avec le grand public, notamment grâce à un certain nombre d'outils de communication (site internet, Twitter, newsletter et événements de sensibilisation), en entretenant des contacts réguliers avec les parties intéressées (par des visites d'étude, par exemple) et en participant à des événements publics, réunions et autres conférences.

6.2.2. Politique linguistique

Notre politique de communication doit aussi tenir compte de la nature particulière du champ d'activité de notre organisation. Les questions de protection des données sont souvent perçues comme relativement techniques et obscures pour les non-spécialistes, et le langage utilisé dans notre communication doit être adapté de façon à déjouer cette impression. Pour que nos activités d'information et de communication attirent un public varié, il convient de communiquer dans un style clair et intelligible qui évite tout jargon inutile. En 2012, comme les années précédentes, nous avons poursuivi nos efforts dans cette direction, notamment dans notre communication avec le grand public et la presse généraliste. Notre objectif global dans ce contexte a été de corriger l'image de la protection des données, qui passe pour une préoccupation excessivement juridique et technique. C'est pourquoi notre stratégie pour 2013-2014 nous engage à communiquer de façon à ce que le public comprenne plus facilement le message.

Si le public visé est plus informé (par exemple les experts de la protection des données ou les acteurs de l'UE), un langage plus spécialisé se justifie naturellement. Nous sommes bien conscients qu'il est important d'utiliser différents styles et différentes approches linguistiques pour communiquer des faits identiques en fonction du public ciblé.

Nos activités de presse et de communication sont proposées dans au moins trois langues – anglais, français et allemand - et ce depuis 2010. Notre objectif global est de toucher un public aussi large que possible.

6.3. Relations avec les médias

Nous nous sommes fixé pour objectif de continuer à développer et maintenir les contacts avec les médias afin d'entretenir l'image d'un partenaire réactif et fiable et de promouvoir le CEPD en tant que point de référence indépendant pour la protection des données au niveau de l'UE.

Nous souhaitons être aussi accessibles que possible aux journalistes, afin que le public puisse suivre notre travail. Nous interagissons régulièrement avec les médias au moyen de communiqués de presse, d'interviews et de rencontres avec la presse. La gestion des demandes formulées par les médias permet d'entretenir des contacts supplémentaires avec ceux-ci.

6.3.1. Communiqués de presse

En 2012, notre service de presse a publié 17 communiqués de presse. Bon nombre de ces communiqués concernaient nos travaux de **supervision** et de **consultation**, et en particulier de **nouveaux avis législatifs** présentant un intérêt immédiat pour le grand public. Les sujets abordés par ces communiqués de presse ont notamment été la stratégie de réforme de la protection des données dans l'UE, le rapport de notre enquête générale sur la conformité, les marchés financiers, l'ACAC, les compteurs électriques intelligents, les cartes de conducteur pour les chauffeurs professionnels, la vidéo-surveillance, le paquet «ouverture des données», la modification du règlement EURODAC, l'affaire *Commission c. Autriche*, l'informatique en nuage et notre politique d'orientation à l'intention des DPD.

Les communiqués de presse sont publiés sur le site internet du CEPD et dans la base de données des communiqués de presse de la Commission (RAPID) en anglais, en français et en allemand. Ils sont distribués à notre réseau régulièrement mis à jour de journalistes et de parties intéressées. Les informations fournies dans nos communiqués de presse contribuent généralement à la production d'une couverture médiatique importante par la presse générale et spécialisée. De plus, nos communiqués de presse sont fréquemment publiés sur des sites internet institutionnels et non institutionnels, notamment ceux des institutions et organes de l'UE, des groupes de défense des libertés civiles, des institutions académiques et des entreprises de technologies de l'information et autres.

6.3.2. Interviews

En 2012, le CEPD et le Contrôleur adjoint ont accordé 40 interviews directes à des journalistes de la presse écrite, de la radiotélévision et des médias électroniques, en Europe et aux États-Unis.

Les articles résultant de ces interviews ont été publiés dans la presse internationale, nationale et de l'UE, généraliste ou spécialisée (dans l'informatique, les affaires européennes …). Certaines interviews ont également été diffusées à la radio et à la télévision.

Ces interviews ont abordé des questions horizontales comme les défis actuels et à venir dans le domaine de la protection de la vie privée et des données. Elles ont également abordé les thèmes particuliers qui ont fait la une des journaux en 2012, comme l'ACAC, les compteurs intelligents, l'informatique en nuage, EURODAC, la révision du cadre juridique européen de protection des données, les préoccupations de vie privée dans le contexte des réseaux sociaux, les droits numériques, ainsi que la conservation et la sécurité des données.

6.3.3. Conférences de presse

En 2012, nous avons organisé trois rencontres réussies avec la presse: un petit-déjeuner de presse le 7 mars sur le paquet de réforme de la protection des données dans l'UE, une conférence de presse le 20 juin pour présenter notre rapport annuel pour 2011, qui a également été l'occasion de discuter encore des propositions de la réforme, et un autre déjeuner de presse le 16 novembre sur l'informatique en nuage.

Ces événements ont été l'occasion pour les journalistes de poser des questions au CEPD, Peter Hustinx, ainsi qu'au Contrôleur adjoint, Giovanni Buttarelli, sur ces questions en particulier ainsi que sur la question plus large de la protection des données dans l'Union européenne et sur les défis à venir.

6.3.4. Demandes formulées par les médias

En 2012, le CEPD a reçu quelque 46 demandes écrites formulées par les médias qui comprenaient des demandes de commentaires et des demandes de clarification ou d'information. L'attention des médias s'est portée sur de nombreux sujets comme les cookies, la santé en ligne, les données de passagers, EURODAC, la vidéo-surveillance, mais nous avons aussi reçu des demandes répétées concernant la réforme de la protection des données en Europe, les compteurs intelligents, l'informatique en nuage et l'ACAC.

6.4. Demandes d'informations et de conseils

En 2012, nous avons répondu à 116 demandes d'informations ou d'assistance émanant du public ou des parties intéressées. Ce chiffre est inférieur à

celui de 2011, mais il reste considérable pour une petite organisation. La notoriété du CEPD dans le monde de la protection des données, renforcée par nos efforts de communication, par les améliorations importantes apportées à notre site internet, et par de nouveaux outils de communication comme les fiches d'information et l'utilisation de Twitter, montre que nous faisons passer notre message de façon plus efficace.

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

La majorité de ces demandes en 2012 étaient en fait des réclamations de citoyens de l'UE pour lesquelles le CEPD n'est pas compétent. Ces réclamations portaient pour la plupart sur des violations présumées de la protection des données par des autorités publiques, des entreprises publiques ou privées et des services et technologies en ligne. D'autres portaient sur la protection des données dans les États membres, les transferts de données, la collecte excessive de données et le temps de réaction excessif des autorités chargées de la protection des données.

Lorsque ces types de réclamations ne relèvent pas de la compétence du CEPD, nous envoyons une réponse au plaignant, précisant le mandat du CEPD et conseillant à la personne de s'adresser à l'autorité nationale compétente, en général l'autorité chargée de la protection des données de l'État membre concerné ou, le cas échéant, la Commission européenne ou l'institution, organe ou agence de l'UE concerné.

Les autres demandes d'informations ont porté notamment sur les activités, rôles et missions du CEPD, la législation européenne en matière de protection des données et sa révision, l'informatique en nuage, l'ACAC, la santé en ligne, les cookies, le respect de la vie privée en ligne, les données biométriques, le consentement, les grands systèmes informatiques tels que SIS et EURODAC, et les questions de protection des données dans l'administration de l'UE, comme les activités de traitement effectuées par les institutions, organes et agences de l'UE.

6.5. Visites d'étude

Dans le cadre de nos efforts visant à sensibiliser à la protection des données, nous recevons régulièrement la visite de divers groupes. L'année dernière, nous avons notamment accueilli des universitaires et des chercheurs ou des experts dans les domaines du droit européen, de la protection des données et de la sécurité informatique.

En 2012, nous avons reçu la visite de représentants des autorités de protection des données de Norvège et de l'ARYM. Le 17 avril, nous avons reçu la délégation de l'ARYM dans nos bureaux et nous avons discuté avec eux de vidéo-surveillance, de supervision coordonnée et de respect de la vie privée sur le lieu de travail. La délégation norvégienne, en visite le 3 décembre, a tenu à entendre notre point de vue sur la réforme de la protection des données dans l'UE, le groupe de travail «Article 29» et notre rôle de supervision dans le secteur public de l'UE.

6.6. Outils d'information en ligne

6.6.1. Site internet

Le site internet reste notre outil de communication et d'information le plus important et, à ce titre, il est mis à jour quotidiennement. Ce site permet aux visiteurs d'accéder aux documents élaborés dans le cadre des activités du CEPD (par exemple les avis relatifs aux contrôles préalables et aux propositions d'actes législatifs européens, les priorités de travail, les publications, les discours du contrôleur et du contrôleur adjoint, les communiqués de presse, les newsletters, les informations sur les événements, etc.).

Évolution du site internet

L'année 2012 a été particulièrement fructueuse pour nos activités de développement sur l'internet. La refonte des rubriques consacrées à la supervision et à la consultation a constitué le développement le plus important. Un système de filtrage a été mis en place afin d'améliorer la fonction de recherche et la navigation sur la base de catégories thématiques. Les visiteurs devraient désormais trouver plus facilement les documents se rapportant aux divers thèmes abordés.

Une nouvelle fonction de recherche a également été créée pour le registre du CEPD. Elle permet

désormais de rechercher des documents non seulement sur un thème donné, mais aussi en fonction de la date et des institutions concernées.

Comme nous l'avons signalé plus haut, nous avons lancé en 2012 un «Coin des DPD» sur notre site internet. Cette nouvelle fonctionnalité est un formulaire extranet avec accès par mot de passe et sert de plate-forme de communication pour tous les DPD des institutions et organes de l'Union européenne. Au cours des mois qui ont suivi son lancement, le Coin des DPD a bénéficié d'un retour très positif en tant que forum permettant de simplifier les contacts entre le CEPD et les DPD.

Parmi les autres développements du site internet, on peut également citer:

- la mise en place d'un flux RSS;
- de nouvelles améliorations apportées au formulaire électronique de dépôt de réclamation introduit pour la première fois en 2011;
- des modifications apportées au graphisme de la page d'accueil.

Nous poursuivrons nos efforts d'amélioration des performances du site internet en 2013.

Trafic et navigation

Une analyse des données sur le trafic et la navigation montre que le site internet a accueilli au total 83 618 nouveaux visiteurs en 2012, ce qui représente une augmentation significative par rapport à 2011 (+27,5 %). Le nombre total des visites en 2012 a été de 179 542, soit 40,4 % de plus qu'en 2011. En octobre et en novembre 2012, le nombre de visites a dépassé les 18 000 par mois.

À partir du 1er janvier 2013, ces chiffres seront l'un des indicateurs-clés des performances du CEPD (voir ci-dessus, point 1.2 sur la révision stratégique du CEPD, et le document «Stratégie 2013-2014» sur notre site internet).

Après la page d'accueil, les pages les plus fréquemment consultées sont les rubriques Consultation, Presse & Actualités, Publications et Supervision. Les statistiques indiquent que la plupart des visiteurs accèdent au site internet par l'intermédiaire d'un lien sur un autre site, par exemple le portail Europa ou le site internet d'une autorité nationale chargée de la protection des données. Environ 40 % des connexions se sont faites par une adresse directe, un onglet ou un lien contenu dans un courrier électronique. Quelques visiteurs seulement ont utilisé les liens proposés par un moteur de recherche.

6.6.2. Newsletter

La newsletter du CEPD est un outil précieux pour informer nos lecteurs de nos dernières activités et pour attirer l'attention sur les ajouts récents au site internet. Elle donne un aperçu de certains de nos avis récents concernant les propositions législatives européennes et les contrôles préalables opérés dans notre fonction de supervision qui mettent en évidence certaines conséquences particulières en matière de protection des données et de respect de la vie privée. Elle évoque également en détail les conférences et les autres événements récents et à venir, ainsi que les discours du contrôleur et du contrôleur adjoint. La newsletter est disponible en anglais, français et allemand sur notre site internet, et les lecteurs sont ajoutés à notre liste de diffusion via une fonctionnalité d'abonnement en ligne.

Cinq numéros de la newsletter du CEPD ont été publiés en 2012, soit en moyenne un tous les deux mois (juillet et septembre sont exclus). Le nombre d'abonnés est passé de 1 750 fin 2011 à environ 1 950 en 2012. Parmi les abonnés figurent notamment des membres du Parlement européen, du personnel des institutions de l'UE et des autorités nationales chargées de la protection des données, ainsi que des journalistes, des universitaires, des sociétés du secteur des télécommunications et des cabinets juridiques.

6.6.3. Twitter

Twitter est un réseau social en ligne jouissant d'une popularité mondiale. Il permet à ses utilisateurs d'envoyer et de lire des messages textuels d'un maximum de 140 caractères appelés «tweets». Il a été décrit comme le *service SMS de l'internet*, bien que les tweets soient en principe lisibles par tout le monde.

Le 1er juin 2012, le CEPD a rejoint la communauté Twitter (@EU_EDPS), notre premier pas vers une communication interactive en ligne. Avant cela, nous avions une présence passive sur Twitter, dans la mesure où le CEPD et les sujets liés à la protection des données apparaissent régulièrement dans des messages Twitter.

Notre politique d'utilisation de Twitter est publiée sur notre site internet. Elle reflète notre approche progressive visant à maintenir un outil contemporain d'information et de communication qui reste gérable avec des ressources limitées.

Conformément à notre politique, nos tweets sont axés sur:

- nos communiqués de presse;
- nos nouveaux avis;
- nos nouvelles publications;
- nos discours et articles;
- nos vidéos;
- des liens vers des articles intéressants consacrés au CEPD et à la protection des données;
- la participation à venir à des événements.

À la fin de l'année 2012, nous avions envoyé 83 tweets, nous suivions 150 autres utilisateurs de Twitter et comptions 312 suiveurs. En 2013, nous allons analyser la réussite de notre compte Twitter et réviser et actualiser notre politique le cas échéant.

6.7. Publications

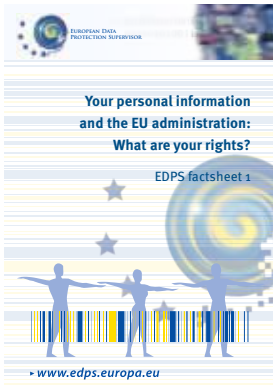
6.7.1. Rapport annuel

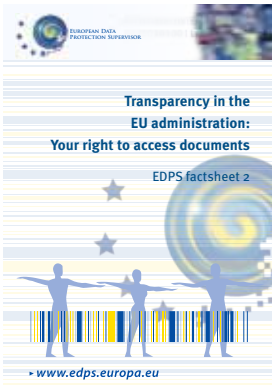
Le rapport annuel constitue une publication essentielle du CEPD. Il présente un aperçu de nos activités au cours de l'année concernée dans les principaux domaines opérationnels que sont la supervision, la consultation et la coopération et fixe les principales priorités pour l'année suivante. Il décrit en outre les réalisations en termes de communication externe et l'évolution de la situation en ce qui concerne l'administration, le budget et le personnel. Un chapitre particulier est également consacré aux activités du délégué à la protection des données du CEPD.

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

Le contrôleur et le contrôleur adjoint ont présenté le rapport annuel 2011 à la commission LIBE du Parlement européen, le 20 juin 2012. Les caractéristiques essentielles du rapport ont également été présentées lors de la conférence de presse qui a eu lieu le même jour.

6.7.2. Publications thématiques





En 2012, nous avons publié notre première fiche d'information thématique sur notre site internet: «*Vos informations personnelles et l'administration de l'UE: quels sont vos droits?*» Cette fiche d'information est disponible en anglais, en français, et en allemand.

En ce qui concerne les questions de protection des données présentant une importance stratégique pour le CEPD, nous comptons publier des informations ciblées à titre d'orientations pour le grand public et les autres parties intéressées. Parmi les autres thèmes actuels des fiches d'information, on peut citer notamment «*La transparence dans l'administration européenne: votre droit d'accès aux documents*», le respect de la vie privée en ligne, les compteurs intelligents, les violations de données, la vidéo-surveillance et le rôle de supervision du CEPD. Nous comptons publier le plus grand nombre possible de ces fiches sur notre site internet d'ici à la fin de l'année 2013 en anglais, en français et en allemand.

6.8. Actions de sensibilisation

Nous tenons à saisir toutes les occasions de mettre en lumière l'importance croissante de la protection de la vie privée et des données et de mieux faire connaître les droits des personnes concernées, ainsi que les obligations de l'administration européenne en la matière.

6.8.1. Journée de la protection des données 2012

Les pays du Conseil de l'Europe et les institutions et organes de l'Union européenne ont célébré le 28 janvier 2012 la cinquième Journée de la protection des données. Cette date marque l'anniversaire de l'adoption de la convention du Conseil de l'Europe pour la protection des données à caractère personnel (Convention 108), le premier instrument international juridiquement contraignant dans le domaine de la protection des données.

Cette journée a été l'occasion idéale de sensibiliser le personnel de l'UE et les autres personnes intéressées à leurs droits et obligations en matière de protection des données. Nous avons diffusé vers les parties prenantes institutionnelles et sur notre site internet un message vidéo du Contrôleur et du Contrôleur adjoint s'exprimant sur le respect de la vie privée et la protection des données en tant que droits fondamentaux. Ce message a également insisté sur le traitement des informations personnelles au quotidien et les risques qui y sont associés.

Comme chaque année, nous avons également apporté notre soutien aux efforts de sensibilisation des DPD des institutions et organes de l'UE.

Nous avons aussi participé aux manifestations organisées par la Commission et le Conseil. Le 25 janvier, le Contrôleur et le Contrôleur adjoint ont pris la parole lors d'un petit-déjeuner de travail avec le DPD et les CPD de la Commission.

Nous avons également participé à diverses autres manifestations, entre autres à la conférence internationale «Ordinateurs, vie privée et protection des données» organisée du 25 au 27 janvier à Bruxelles, qui sert de pont entre les décideurs politiques, les universitaires, les praticiens et les activistes afin de discuter des problèmes émergents en matière de respect de la vie privée, de protection des données et de technologies de l'information. Nous avons notamment participé à des panels de discussion sur le cadre européen de protection des données, le respect des droits d'auteur et de la vie privée, le respect de la vie privée et les flux transfrontaliers de données à caractère personnel. Comme à l'accoutumée, le Contrôleur a assuré le discours de clôture.

6.8.2. Journée portes ouvertes de l'UE 2012

Le 12 mai 2012, nous avons une fois de plus participé à la Journée portes ouvertes annuelle des institutions de l'UE. La Journée portes ouvertes de l'Union européenne nous offre une excellente occasion de sensibiliser le public à la nécessité de protéger la vie privée et les données à caractère personnel, ainsi qu'au rôle du CEPD.

Les membres du personnel du CEPD ont accueilli les visiteurs sur notre stand dans le bâtiment principal du Parlement européen à Bruxelles et répondu aux questions sur les droits des citoyens de l'UE en matière de protection des données et de respect de la vie privée. Les visiteurs ont également pu prendre part à notre quiz sur la protection des données et emmener de la documentation. La caméra à infra-rouges reliée à un grand écran a été l'une des principales attractions de notre stand. Bien que n'ayant pas de lien direct avec le traitement des données personnelles, elle a permis de montrer de manière ludique et provocante le risque potentiel que les nouvelles technologies représentent pour la vie privée.

7 ADMINISTRATION, BUDGET ET PERSONNEL

Notre objectif stratégique

Améliorer l'utilisation des ressources humaines, financières, techniques et organisationnelles.

Notre principe directeur

Nous cherchons à nous positionner en tant qu'organe faisant autorité en développant l'expertise et l'assurance de notre personnel pour pouvoir collaborer efficacement avec les différentes parties prenantes.

7.1. Introduction

Dans le climat actuel d'austérité économique, nous nous sommes imposé des réductions budgétaires considérables pour la deuxième fois en 2012. Afin d'en faire plus avec moins, nous avons mis en place de nouveaux mécanismes de contrôle, par exemple les examens trimestriels d'exécution du budget ainsi que trois niveaux de planification (mensuel, annuel et stratégique) permettant de mieux suivre les activités et de répartir plus efficacement les ressources.

La planification stratégique, l'amélioration de la planification et la répartition et l'utilisation plus efficace des ressources ont dominé nos réflexions en 2012 dans un sens nettement plus large également.

Fin 2012, nous avons déménagé du n° 63 au n° 30 de la Rue Montoyer. Comme précédemment, nous louons ces nouveaux bureaux au Parlement européen dans le cadre d'un accord interinstitutionnel. Les services du Parlement européen continuent de nous apporter une assistance dans tous les domaines liés à l'informatique, à l'infrastructure et à la logistique. Ce déménagement réussi et longtemps retardé a été le résultat des travaux de réflexion et du travail d'un groupe de travail s'inscrivant dans le cadre de notre révision stratégique globale.

Nous avons également amélioré considérablement l'efficacité de la fonction RH en 2012 par l'intégration de Sysper2 (système de gestion des dossiers du personnel) et de MIPs (système de gestion des missions), deux systèmes développés principalement en vue d'une utilisation par la Commission européenne.

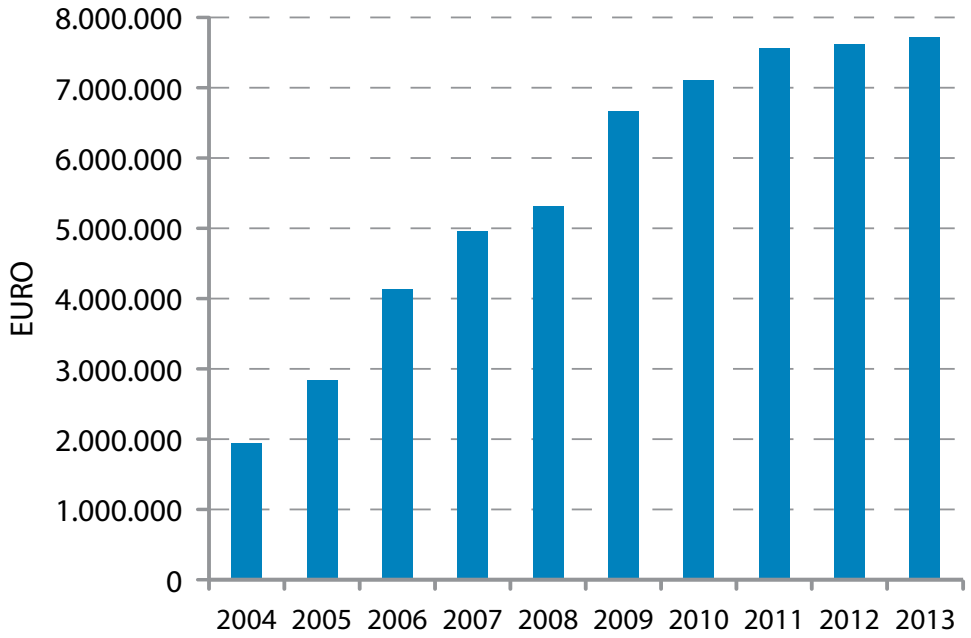
L'amélioration de la répartition et du contrôle des moyens financiers a également permis d'augmenter considérablement le taux d'exécution du budget, qui est actuellement d'environ 90 %.

Conformément au plan de gestion annuel 2012, nous avons créé une fonction de passation de marchés. Celle-ci nous a permis de lancer des procédures d'achats entièrement gérées par le CEPD.

7.2. Budget, finances et marchés publics

7.2.1. Budget

CEPD – Évolution du budget 2004-2013



Le budget du CEPD s'établissait à 7 624 090 EUR pour l'exercice 2012, soit une hausse de 0,79 % par rapport au budget 2011. Vu le taux d'inflation prévu de 1,9 % pour 2012, ce chiffre représente en fait une diminution nominale.

En période d'austérité économique, et tout comme les autres institutions de l'UE et les États membres, nous avons consenti des efforts considérables pour rationaliser notre budget. Cette tâche est particulièrement difficile dans le cas d'un budget modeste. Contrairement aux autres institutions de l'UE établies de longue date et dotées de moyens importants par comparaison, le CEPD est une institution de taille modeste en pleine croissance. Nous sommes parvenus à réduire notre budget grâce à un redéploiement fondamental des ressources et en identifiant les priorités négatives.

Pour faire face à un scénario marqué à la fois par une réduction budgétaire et une augmentation des responsabilités, nous avons adopté une culture d'optimisation accrue dans l'utilisation des ressources. En d'autres termes, il s'agit d'en faire plus avec moins. Nous avons amélioré l'examen trimestriel de l'exécution budgétaire mis en place en 2011, et cet examen s'est révélé essentiel pour l'utilisation efficace de nos ressources limitées.

Des suites de cet exercice, notre taux d'exécution du budget a progressé de manière significative, de 76 % en 2010 à 85 % en 2011, avec une prévision de 90 % pour 2012.

7.2.2. Finances

La déclaration d'assurance de la Cour des comptes européenne concernant l'exercice financier 2011 (DAS 2011) n'a pas fait état de préoccupations concernant le CEPD ni formulé de recommandations à son intention. Néanmoins, dans le cadre d'une gestion financière saine et en vue d'améliorer la fiabilité et la qualité de nos données financières:

a) une charte des missions et responsabilités des ordonnateurs délégués et subdélégués a été préparée pour adoption en janvier 2013;

b) une note explicative relative aux procédures de passation de marché pour des montants modestes, à compléter et à joindre à tout ordre d'achat ou contrat, a été préparée pour adoption en janvier 2013;

c) l'application de demande de mission MIPS a été mise en œuvre afin d'assurer un meilleur contrôle et une plus grande transparence;

d) à la lumière de la création possible d'un Comité européen de la protection des données associé sur le plan administratif au CEPD, un nouveau Titre III a été rédigé et ajouté au budget du CEPD (aucun crédit supplémentaire n'a été demandé à ce stade);

e) une procédure interne de remboursement des frais de représentation a été adoptée.

En 2012, la Commission a continué d'apporter une assistance dans le domaine financier, notamment en ce qui concerne les services comptables - le comptable de la Commission est également le comptable du CEPD.

7.2.3. Marchés publics

Afin d'acquérir une plus grande autonomie dans le domaine de la passation de marchés, nous avons adopté nos propres *lignes directrices pas à pas en matière de marchés publics pour* les contrats de faible valeur en juin 2012.[33]

En conséquence, deux procédures ont été lancées en 2012. La première, en juin, était une procédure négociée avec concurrence pour la production de séquences vidéo. La deuxième, en décembre, était une procédure négociée pour un contrat d'assistance informatique. Le montant total des contrats associés à signer était de 73 200 EUR.

7.3. Ressources humaines

7.3.1. Recrutement

Le CEPD est une institution de taille relativement modeste, et notre personnel se caractérise par une grande polyvalence et une charge de travail élevée. Le résultat est que tout départ de personnel est problématique parce qu'il n'est pas facile de trouver un remplacement, et jusqu'à l'arrivée d'un nouveau collègue la charge de travail déjà importante des autres travailleurs est encore augmentée. Recruter la bonne personne le plus rapidement possible est donc de la plus haute importance, et l'équipe HR accorde un grand soin à cette tâche afin de réduire le plus possible l'impact de ces départs.

Dans leurs perspectives financières pour 2007-2013, le Conseil et le Parlement européen ont prévu une politique de croissance modérée mais durable pour le CEPD. De nouveaux collègues ont immédiatement été désignés pour aider à la gestion de la lourde charge de travail entraînée par l'importance croissante de la protection des données et par la visibilité de notre institution, ainsi que par l'entrée en vigueur du traité de Lisbonne.

Après le concours général en matière de protection des données de 2009, nous avons recruté de manière extensive les années suivantes. Les listes de réserve du concours sur la protection des données sont maintenant pratiquement épuisées. Nous avons également reçu un nombre important de demandes de transfert de la part de fonctionnaires d'autres institutions européennes, ce qui démontre la visibilité croissante du CEPD en tant qu'employeur attractif.

En 2012, nous avons recruté sept fonctionnaires, dont trois destinés au nouveau secteur «Stratégie IT» (voir 7.3.5), deux pour l'unité HRBA à la suite d'un départ et d'une réorganisation interne de l'unité, et un pour chacune des deux unités existantes de protection des données.

Outre ces fonctionnaires européens, nous avons recruté un expert national détaché (équipe S&E) et trois agents contractuels (équipes S&E et P&C). Au total, que ce soit en raison de la rotation du personnel ou de nouvelles intégrations, l'unité HRBA a organisé le recrutement de 11 nouveaux membres du personnel en 2012.

Le diagramme ci-dessous illustre la croissance respectable de l'organisation ces trois dernières années à la suite de la création de trois nouveaux secteurs (I&C, OPS et PIT). Les unités (S&E, P&C et HRBA) n'ont pas connu de réductions significatives de leur personnel.

7.3.2. Professionnalisation de la fonction RH

À la suite de l'adoption de plusieurs manuels et décisions en 2011, l'équipe RH a publié son premier rapport décrivant ses métriques et ses activités passées et à venir. Ce rapport a été soumis à l'examen du Conseil d'administration du CEPD en 2012.

De plus, nos efforts de négociation considérables avec plusieurs départements de la Commission européenne ont finalement abouti à l'intégration de la famille de logiciels Sysper2. Il en découle une simplification et une professionnalisation de la fonction RH au sein de notre institution compacte.

En préparation d'une visite de l'auditeur interne, l'équipe RH a procédé à une analyse approfondie de toutes ses activités. De ce fait, les décisions, flux de travail, processus, pratiques de gestion des dossiers, etc. ont été analysés en détail pour chaque activité, mettant ainsi au jour les incohérences et les inefficacités apparues avec la croissance de l'institution au fil des années. Bon nombre de ces problèmes ont été résolus en 2012, les autres seront traités en 2013.

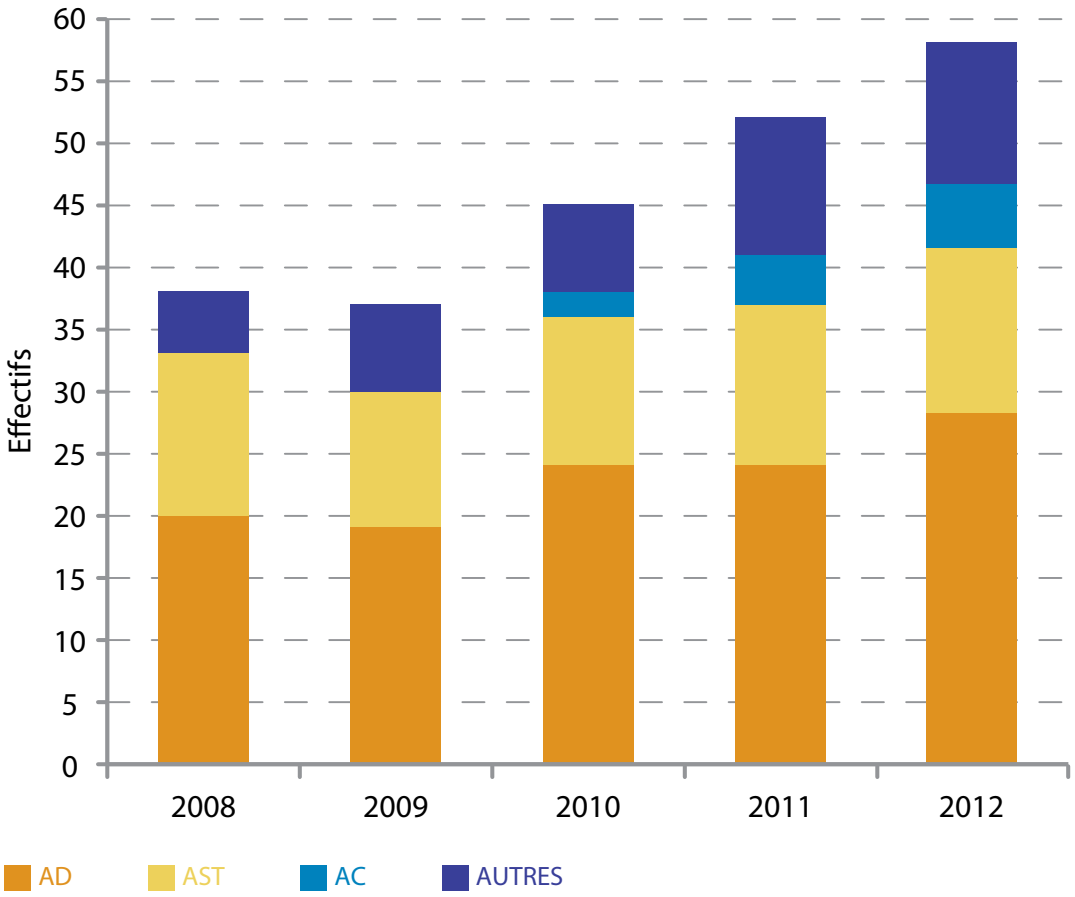
À la suite de cette analyse, plusieurs décisions d'exécution du CEPD ont été modifiées et 16 notifications en matière de protection des données ont été envoyées ou mises à jour.

7.3.3. Programme de stages

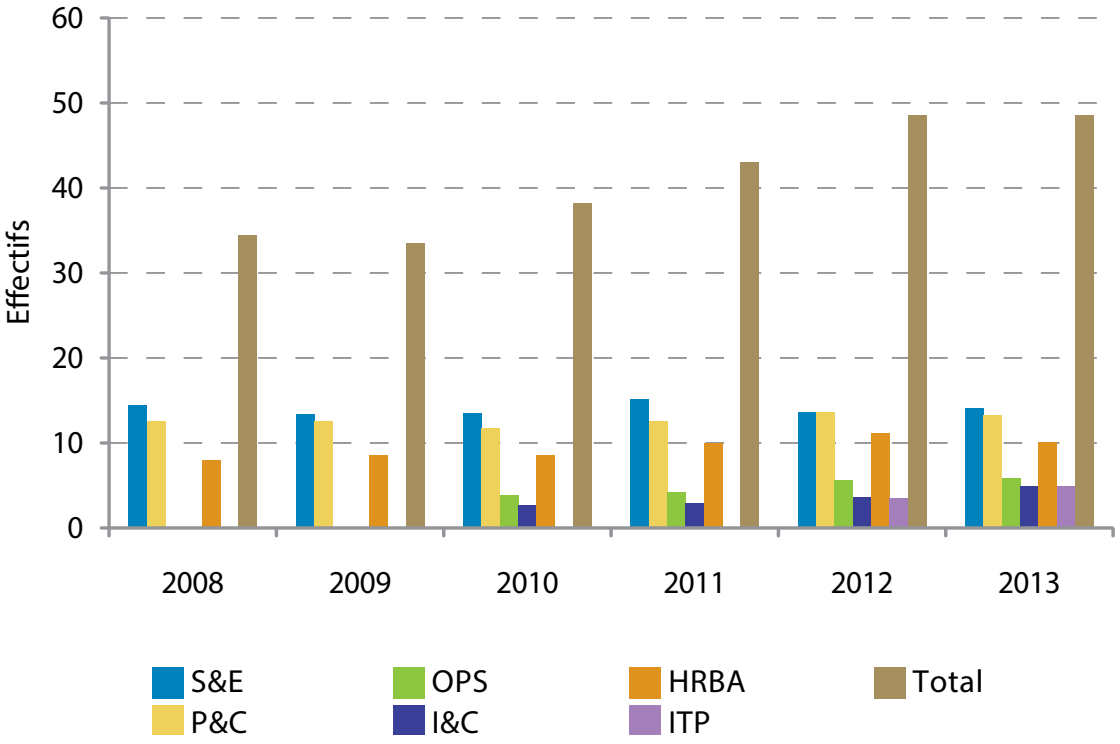
En 2012, notre organisation a continué d'investir dans le programme de stages créé en 2005. Ce programme

[33] À modifier en fonction du nouveau règlement financier entré en vigueur le 1er janvier 2013.

CEPD - ÉVOLUTION DU PERSONNEL PAR CATÉGORIE



Évolution du personnel du CEPD 2008-2013



donne aux diplômés universitaires récents l'occasion de mettre en pratique les connaissances acquises à l'université. Nous leur proposons la possibilité d'acquérir de l'expérience pratique dans nos activités au quotidien au sein des unités opérationnelles ainsi que dans l'unité HRBA et les secteurs I&C et ITP.

Le programme accueille en moyenne quatre stagiaires par session, avec deux sessions de cinq mois par an (de mars à juillet et d'octobre à février). Dans des circonstances exceptionnelles, et dans le respect de critères d'admission stricts, nous pouvons également accueillir des stagiaires non rémunérés souhaitant acquérir de l'expérience dans le cadre de leurs études ou de leur carrière professionnelle. Les critères d'admission et autres règles régissant le programme de stages sont décrits dans notre décision en matière de stages disponible sur notre site internet.

Tous les stagiaires, rémunérés ou non, contribuent à la fois au travail théorique et pratique, tout en acquérant une expérience directe utile. Historiquement, les stagiaires ont été recrutés pour les unités P&C, S&E et HRBA. En 2012, outre ces stagiaires, le CEPD a recruté des stagiaires dans le secteur de l'information et de la communication ainsi que dans le nouveau secteur «Politique IT».

Depuis octobre 2012, en raison de la place supplémentaire disponible dans le nouveau bâtiment, nous pouvons envisager l'adjonction de stagiaires supplémentaires non rémunérés.

7.3.4. Programme pour les experts nationaux détachés

Le programme destiné aux experts nationaux détachés (END) auprès du CEPD a été lancé en janvier 2006. En moyenne, deux experts nationaux des autorités chargées de la protection des données (APD) des États membres sont détachés chaque année. Le détachement d'experts nationaux nous a permis de bénéficier de leurs compétences et de leur expérience professionnelle et d'accroître notre visibilité dans les États membres. À son tour, ce programme permet aux END de se familiariser avec les questions de protection des données au niveau de l'UE.

En 2012, le détachement d'un expert national allemand est arrivé à son terme et un nouvel expert national a été recruté auprès de l'autorité britannique de protection des données (ICO).

7.3.5. Organigramme

L'organigramme du CEPD a été actualisé en 2012. Un nouveau secteur, «Politique IT», a été créé le 1er avril 2012. Ce secteur se compose de deux postes transférés de l'unité S&E, un poste transféré de l'unité P&C et un nouveau poste créé par l'autorité budgétaire pour 2012, qui a servi à recruter un chef de secteur. Un nouveau poste viendra renforcer ce secteur en 2013.

L'importance croissante du rôle joué par les coordinateurs a également été reconnue. Nous avons continué de développer cette fonction en 2012 en confirmant les coordinateurs existants, en désignant de nouveaux coordinateurs, et en clarifiant leurs fonctions et leurs responsabilités, ainsi qu'en utilisant la terminologie «chef d'activité». Il en a résulté la désignation de six chefs d'activité (trois dans l'unité S&E, deux dans l'unité P&C et un dans l'unité HRBA).

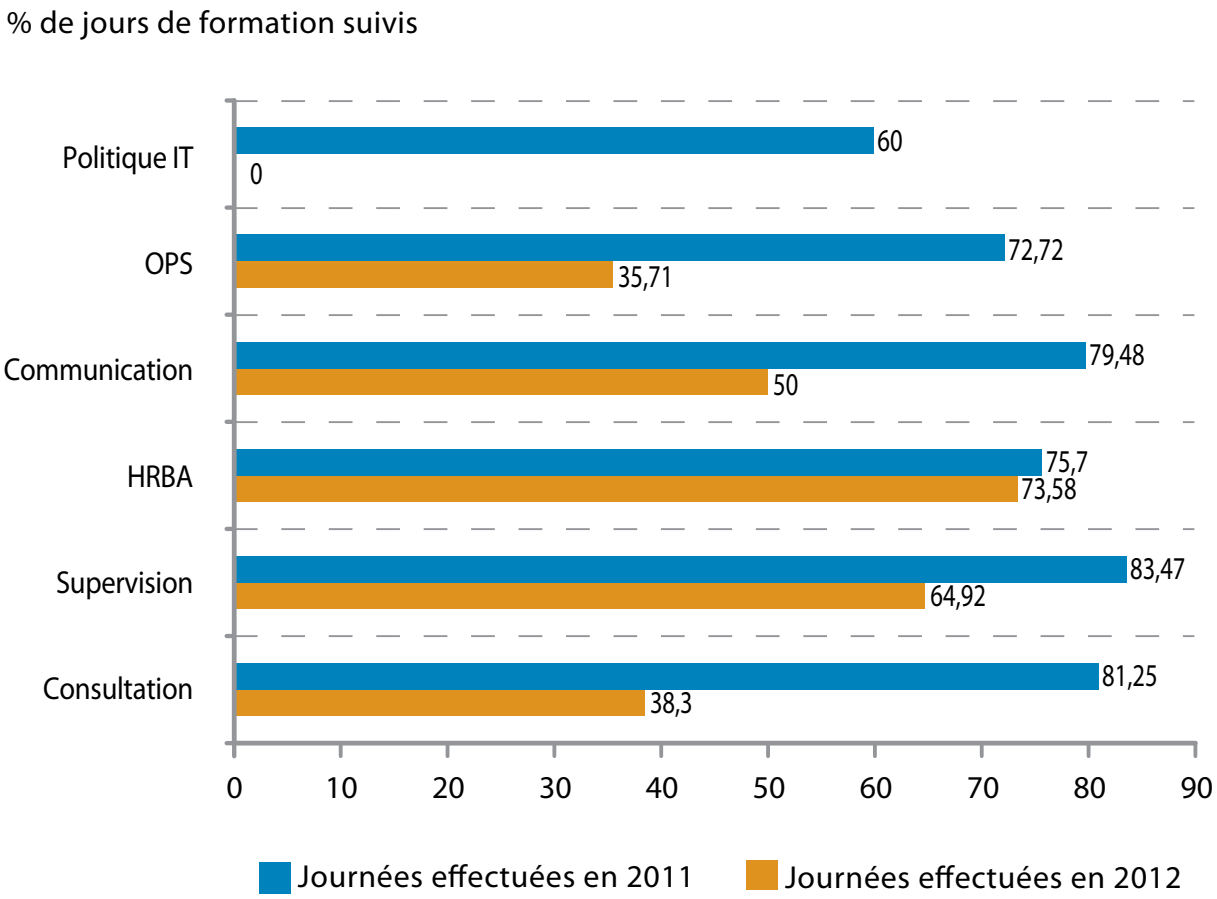
7.3.6. Conditions de travail

Comme pour les autres institutions de l'UE, les conditions de travail du CEPD sont définies dans le statut des fonctionnaires et le régime applicable aux autres agents des Communautés européennes. Dans le cadre de la flexibilité limitée prévue par ce cadre juridique, l'équipe RH s'efforce de rendre ces conditions aussi attrayantes et flexibles que possible pour notre personnel, et en particulier pour les personnes ayant des responsabilités familiales.

Le régime d'horaire flexible est fort apprécié par le personnel. À l'heure actuelle, 99,5 % de tous les membres du personnel introduisent leurs heures de travail dans Sysper2. Dix pour cent utilisent l'horaire flexible uniquement pour bénéficier d'heures de travail variables, tandis que le reste des utilisateurs s'en servent non seulement pour avoir des horaires flexibles, mais aussi pour récupérer les heures supplémentaires (en jours ou en demi-journées).

Depuis le mois de mai 2012, la procédure en matière d'horaire flexible est gérée par le module «gestion du temps» de Sysper2 et toutes les demandes et autorisations sont gérées à travers cette application.

Notre décision relative au télétravail, qui s'inspire dans une large mesure d'une décision similaire prise par la Commission, a été adoptée en juillet 2012 à la suite de nombreuses discussions entre la direction et le comité du personnel. Le système de télétravail a ensuite été lancé sous la forme d'un projet pilote en septembre 2012. La phase pilote se terminera en février 2013 et des ajustements seront apportés si nécessaire. Il y a un choix entre deux régimes de télétravail: structurel et occasionnel. Le télétravail structurel est récurrent (maximum un jour ou deux demi-journées par semaine), tandis que le télétravail occasionnel est conçu pour les situations dans lesquelles un membre du personnel n'est pas en mesure de se rendre au bureau pour l'une ou l'autre raison mais est malgré tout capable de travailler (maximum 12 jours par an).



Pendant la phase pilote, deux membres du personnel ont pratiqué le télétravail structurel, tandis que 19 demandes de télétravail occasionnel ont été accordées.

7.3.7. Formation

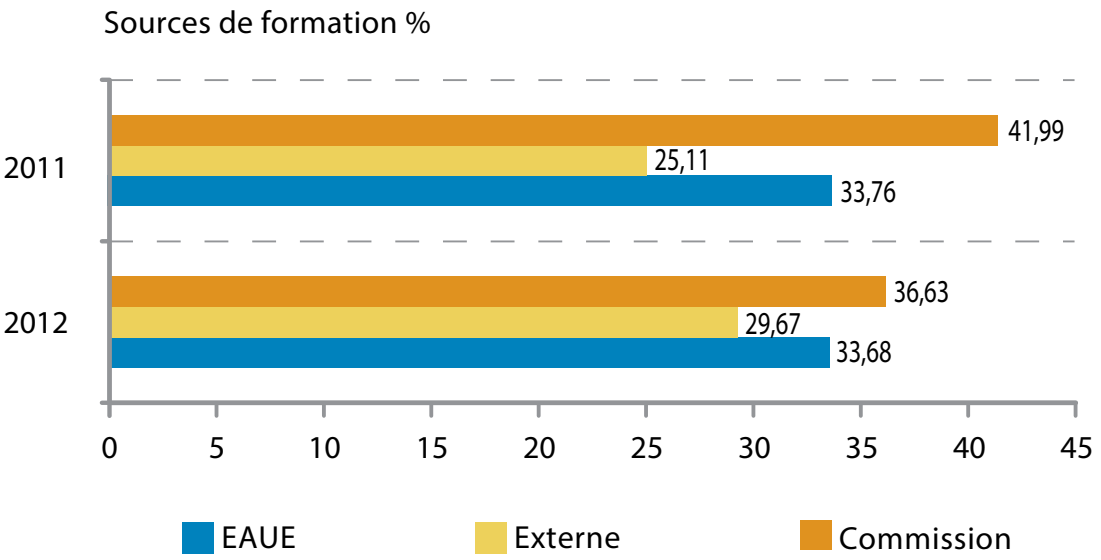
La formation et l'évolution des carrières au CEPD se sont considérablement améliorées en 2011, qu'il s'agisse du nombre des formations suivies ou de leur diversité. Cette tendance s'est poursuivie en 2012 à mesure que les membres du personnel se sont familiarisés avec les offres contenues dans Syslog 2 (un système de gestion du catalogue des formations de la Commission et des demandes de formation).

De ce fait, le nombre des journées de formation a augmenté de manière substantielle (+60,51 % par rapport à 2011). Le pourcentage des jours de formation effectifs par rapport au nombre de jours estimé dans les plans de formation au début de l'année a progressé également, de 56,82 % en 2011 à 77,59 % en 2012.

Les trois principaux fournisseurs de formations de notre institution sont la Commission, l'École européenne d'administration, qui représente un tiers des formations suivies par le personnel du CEPD, et d'autres prestataires de services externes tels que les Instituts européens de formation, qui assurent certaines formations spéciales particulièrement importantes pour les juristes. Le diagramme ci-dessous illustre l'évolution de ces formations.

En 2012, deux formations sur mesure ont été proposées à notre personnel: une deuxième session de la formation First steps in management (premiers pas dans l'encadrement), organisée par l'école européenne d'administration, et une formation spécialement destinée à l'unité de supervision et appelée Comment gérer les entretiens lors d'une inspection. Cette dernière formation, qui avait été suivie et recommandée par le personnel de l'APD française, la CNIL, était particulièrement pertinente dans le contexte de nos pouvoirs de supervision (article 47, paragraphe 1 du règlement n° 45/2001. Douze membres du personnel ont participé à chacune de ces formations.

La formation en encadrement pour les membres de la nouvelle équipe d'encadrement s'est poursuivie en 2012, ce qui a entraîné des améliorations tangibles au niveau de la planification, de la coordination, et de la mise en œuvre des politiques lors de la réunion de direction.



7.3.8. Activités sociales

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

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

En 2012, diverses activités sociales ont été organisées avec la participation du comité du personnel de l'institution.

Dans nos nouveaux locaux, une salle consacrée aux activités sociales, The Cloud, a été mise à la disposition des membres du personnel. Ils peuvent s'y retrouver pour boire un café, pour le déjeuner ou pour des activités sociales. C'est également dans cette salle qu'ont lieu les réunions du comité du personnel.

7.4. Fonctions de contrôle

7.4.1. Contrôle interne

Le système de contrôle interne, en vigueur depuis 2006, gère le risque de non-réalisation des objectifs. En 2012, nous avons élargi la liste des actions d'exécution afin de garantir un contrôle interne plus efficace des processus en place. À titre d'exemple, une version révisée de toutes les descriptions de fonctions, un règlement intérieur (article 46, point k) du règlement (CE) n° 45/2001), la présentation des activités de l'unité à tous les membres du personnel, un manuel relatif à l'accès aux documents et un nouveau registre des risques sont au nombre des mesures adoptées pour mettre en œuvre les normes de contrôle interne (NCI).

Une décision révisée des normes de contrôle interne sera adoptée en 2013 pour simplifier l'approche, augmenter l'appropriation et renforcer l'efficacité de ces normes.

À la suite de l'adoption d'un plan annuel de gestion au début de l'année 2012, nous avons adopté une décision sur la gestion des risques en juillet 2012, outils contemporains qui facilitent le recensement des risques et le choix des actions possibles. La gestion des risques ne se contente pas d'une évaluation des risques, encore faut-il mettre en place des contrôles et des actions qui feront ensuite l'objet d'un suivi. C'est pourquoi nous avons inclus la gestion des risques en tant qu'élément essentiel de notre stratégie globale de gestion de la qualité totale (GQT).

Nous avons pris acte du rapport annuel d'activité et de la déclaration d'assurance signée par l'ordonnateur délégué. D'une manière générale, nous esti-

mons que les systèmes de contrôle interne mis en place fournissent une assurance raisonnable quant à la légalité et à la régularité des opérations dont l'institution est responsable.

7.4.2. Audit interne

L'auditeur interne de la Commission, le Directeur général du Service d'Audit Interne (SAI), est également l'auditeur interne du CEPD.

À la suite du rapport d'audit de novembre 2011 portant sur les avis de contrôle préalable, les mesures administratives et les inspections, un rapport publié en avril 2012 formule un certain nombre de recommandations à suivre.

En juin 2012, à la suite de cet audit spécifique, le SAI a publié un rapport consultatif consacré au processus d'inspection du CEPD. Cette mission de conseil avait pour objectif de recommander des améliorations possibles du processus d'inspection du CEPD. Les domaines à améliorer ainsi recensé sont notamment: l'approche stratégique, les procédures d'inspection, la gestion des ressources et les mesures de contrôle mises en place par le CEPD afin d'assurer ce processus de manière efficace.

En mai 2012, le SAI a publié le Rapport annuel d'audit interne (RAAI – article 86, paragraphe 3 du règlement financier) pour 2011, qui résumait les activités d'audit effectuées en 2011 au CEPD.

Lors du suivi des six recommandations ouvertes pendantes d'audits antérieurs, deux ont été closes par le SAI et les quatre autres devraient être closes dans le courant de l'année 2013.

Comme le SAI et le CEPD ont un intérêt commun dans le domaine des audits, un protocole d'accord permettant aux deux organisations d'assumer leurs fonctions le plus efficacement possible a été signé en mai 2012. Ce protocole a été conclu dans le respect absolu des droits, des obligations et de l'indépendance des deux parties tels que définis dans leurs documents constitutifs.

Un accord de niveau de service (Service Level Agreement, SLA) entre le SAI et le CEPD a été signé au même moment. Depuis septembre 2004 et la désignation de l'auditeur interne de la Commission en tant qu'auditeur interne du CEPD, le SAI a assuré ses services d'audit dans le cadre de l'accord interinstitutionnel entre le Parlement européen, la Commission européenne et le CEPD. Comme l'accord interinstitutionnel avec la Commission arrive à expiration en décembre 2013, ce SLA deviendra un document autonome qui servira de base aux services d'audit futurs.

Enfin, la charte de mission du SAI a aussi été signée en mai 2012. Cette charte définit la mission, les objectifs, les comptes rendus et les modalités de travail essentiels pour permettre au SAI d'accomplir correctement sa mission en vers le CEPD.

7.4.3. Audit externe

En tant qu'institution de l'UE, le CEPD est audité par la Cour des comptes. Conformément à l'article 287 du traité sur le fonctionnement de l'Union européenne, la Cour réalise un audit annuel de nos recettes et dépenses afin de produire une déclaration d'assurance concernant la fiabilité des comptes et la légalité et la régularité des transactions sous-jacentes. Cela se déroule dans le cadre de ce que l'on appelle «l'exercice de décharge», avec des questions et des entretiens d'audit.

Pour la décharge relative à l'année 2011, le CEPD a répondu de façon satisfaisante aux questions posées par la Cour. En juin 2012, la Cour a envoyé au CEPD une lettre indiquant que «l'audit effectué n'a donné lieu à aucune observation».

La Cour des comptes (article 143 du règlement financier) a déclaré n'avoir repéré aucun point faible significatif dans les domaines audités et affirmé que les mesures mises en œuvre à la suite de son audit (allocations sociales) étaient effectives. Nous avons pris acte de l'analyse de la Cour et comptons continuer d'améliorer notre système en vue d'un suivi et d'un contrôle en temps utile.

En janvier 2012, le directeur du CEPD a participé à la réunion de décharge de la commission budgétaire du Parlement européen et répondu aux questions posées par les membres de cette commission. Le Parlement européen a accordé la décharge au CEPD pour la mise en œuvre de notre budget pour l'exercice 2010.

7.5. Infrastructure

Les bureaux du CEPD se situent dans l'un des bâtiments du Parlement européen. En vertu d'un accord interinstitutionnel de coopération, le Parlement nous

apporte également un soutien en matière d'informatique et d'infrastructure.

Après des préparatifs longs et minutieux en 2011 et pendant la majeure partie de 2012, nous avons enfin déménagé dans nos nouveaux bureaux, Rue Montoyer 30 à Bruxelles. Notre étroite collaboration avec les services du Parlement européen a permis une planification efficace et un déménagement sans accrocs en octobre 2012, avec le moins de perturbation possible de notre travail. Nous avons profité de notre déménagement pour investir et mettre à niveau certains équipements informatiques. Ainsi, nous avons acheté un système de vidéoconférence qui devrait nous permettre d'économiser sur les frais de mission, puisque cette technologie nous permet de participer à des réunions externes depuis nos locaux.

L'institution continue de gérer indépendamment l'inventaire de son mobilier. En vertu d'un accord forfaitaire avec le PE, l'inventaire informatique est géré par la DG ITEC du PE.

7.6. Environnement administratif

7.6.1. Assistance administrative et coopération interinstitutionnelle

Le CEPD bénéficie de la coopération interinstitutionnelle dans de nombreux domaines en vertu de l'accord conclu en 2004 avec les secrétaires généraux de la Commission, du Parlement et du Conseil, accord qui a été prorogé pour une durée de trois ans en 2006 et de deux ans en 2010 avec la Commission et le Parlement. Les secrétariats généraux de la Commission et du Parlement et le directeur du CEPD ont signé une prorogation de l'accord pour une durée de deux ans en décembre 2011.

En 2012 cependant, dans la perspective de notre déménagement imminent vers de nouveaux bureaux, le Parlement européen a préféré réviser l'accord administratif général signé avec nous ainsi que ses annexes relatives à l'infrastructure, à la sécurité, à l'informatique, etc. afin de mieux refléter les besoins et les obligations des deux parties et de simplifier et d'uniformiser ces textes. Conclus techniquement en 2012, l'accord administratif général et ses annexes seront signés au début de l'année 2013. Cette coopération administrative est essentielle pour nous dans la mesure où elle augmente l'efficacité et permet des économies d'échelle.

En 2012, nous avons poursuivi notre coopération interinstitutionnelle étroite avec diverses directions générales de la Commission (DG «Personnel et administration», DG «Budget», service d'audit interne, DG «Éducation et culture»), l'Office des paiements (PMO), l'École européenne d'administration (EEA), le Centre de traduction des organes de l'Union européenne et divers services du Parlement européen (services de l'information et des technologies, en ce qui concerne plus particulièrement la maintenance et le développement du site internet du CEPD, l'équipement des locaux, la sécurité des bâtiments, les travaux d'impression, le courrier, la téléphonie, les fournitures, etc.). Dans la plupart des cas, cette coopération se fait au moyen d'accords de niveau de service, qui sont régulièrement mis à jour. Nous avons également continué de participer aux appels d'offres interinstitutionnels, accroissant ainsi son efficacité dans de nombreux domaines administratifs et évoluant vers plus d'autonomie. Un bon exemple de résultat de cette coopération interinstitutionnelle est le travail avec la DG DIGIT et la DG HR de la Commission et avec la DG DIGIT et PMO, qui a permis l'intégration de Sysper2 et de la famille de logiciels MIPs en 2012.

Le CEPD est membre de plusieurs comités interinstitutionnels et groupes de travail, notamment le collège des chefs d'administration, le comité de gestion assurances maladies (CGAM), le comité de préparation pour les questions statutaires (CPQS), le comité du statut, le groupe de travail interinstitutionnel de l'EEA, le conseil de direction de l'EPSO, la commission paritaire commune et le comité de préparation pour les affaires sociales.

Le 22 octobre 2012, l'équipe HRBA a visité la Cour des comptes pour participer à une série d'ateliers sur les bonnes pratiques dans le domaine des ressources humaines, des affaires budgétaires/financières et de l'administration. À la suite de ces discussions, de nouvelles méthodes de travail et de nouvelles idées seront mises en pratique en 2013.

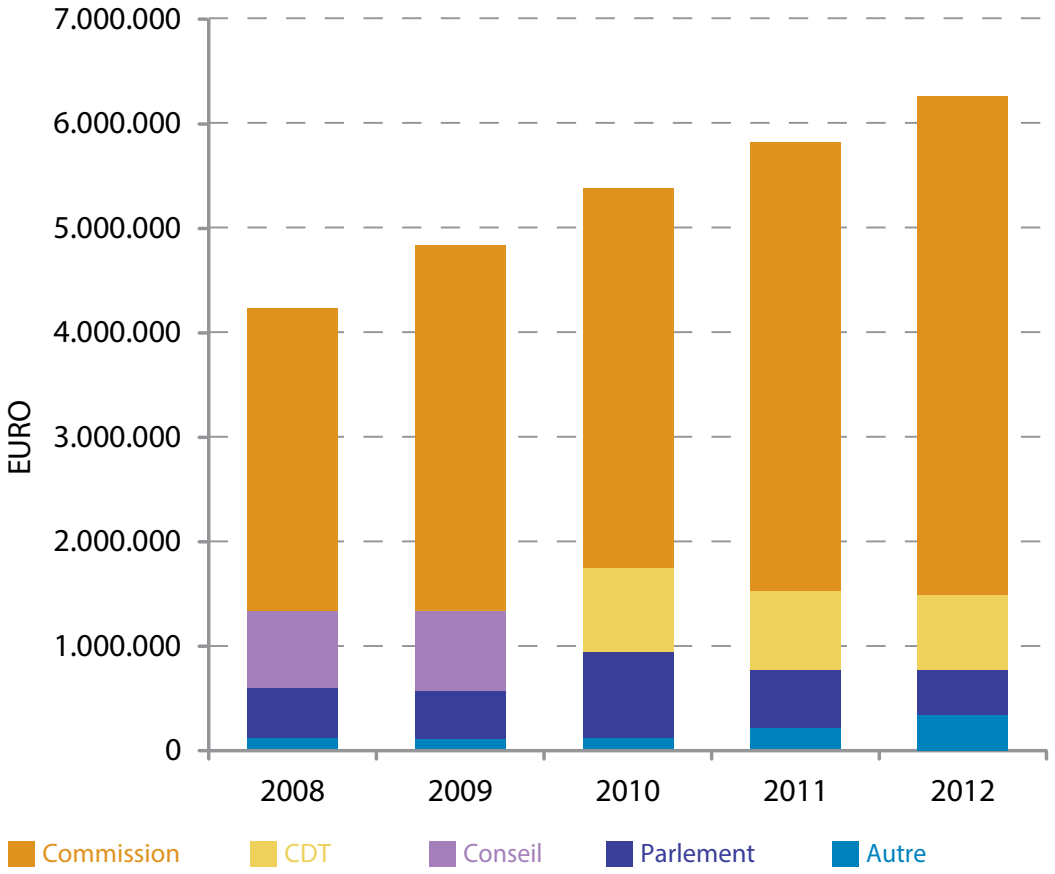
7.6.2. Gestion des documents

En 2012, nous avons personnalisé un système de gestion des documents et des dossiers intégrant la gestion des dossiers. Ce système de gestion des documents et des dossiers permet de stocker des documents et des dossiers regroupés dans des fichiers d'affaires pour toutes nos activités. Les fichiers d'affaires sont classés selon un plan de classement.

Le système présente des fonctionnalités comme un contrôle d'accès sophistiqué, l'enregistrement du courrier, des délais de conservation, la possibilité de mise en suspens pour des raisons juridiques, la gestion de différentes versions d'un document, l'indication du sujet, des recherches sur texte et sur toute la base de données, des pistes d'audit, des rapports et des flux de travail.

Ce système devrait être opérationnel en 2013.

Exécution budgétaire du CEPD par la coopération interinstitutionnelle



8 DÉLÉGUÉ À LA PROTECTION DES DONNÉES DU CEPD

8.1. Le DPD du CEPD

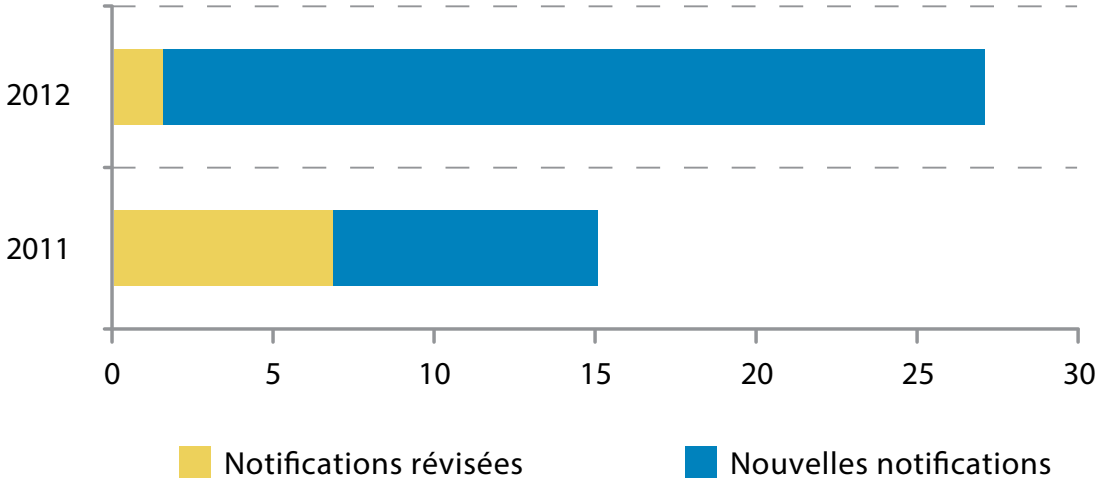
Le rôle de DPD au CEPD présente de nombreux défis : le DPD doit se montrer indépendant au sein d'une institution indépendante, répondre aux attentes élevées de collègues particulièrement attentifs et sensibles aux questions de protection des données et apporter des solutions qui pourront servir de références aux autres institutions.

Pour renforcer cette indépendance et approfondir son expertise, le DPD du CEPD suit la formation de l'IAPP (International Association of Privacy Professionals) recommandée dans le document des DPD sur les normes professionnelles publié par le réseau des DPD[34], et a obtenu le titre de Certified Information Privacy Professional/Europe (CIPP/E). Le DPD a également participé au congrès de l'IAPP en novembre 2012 afin de consolider plus encore son expertise.

8.2. Le registre des traitements

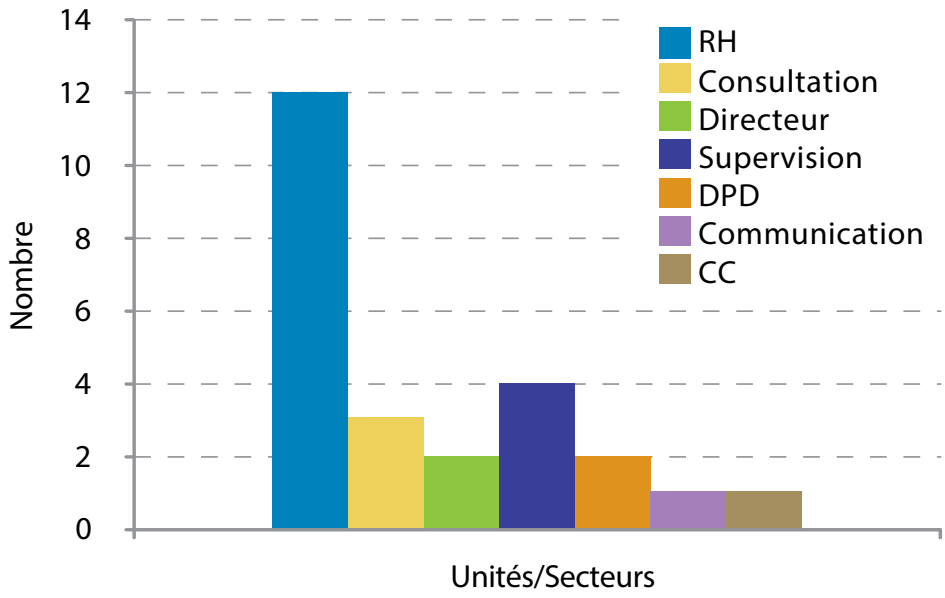
Après la révision de toutes les notifications en vue des opérations de traitement du CEPD en 2011, l'inventaire et sa mise en œuvre ont été actualisés en 2012. Par conséquent, il y a eu 25 nouvelles notifications et 2 révisions de notifications existantes.

Notifications Article 25



[34] *Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation* (EC) 45/2001 (Normes professionnelles des Délégués à la protection des données des institutions et organes européens travaillant en application du règlement (CE) n° 45/2001), 14 octobre 2010

Notifications Article 25 par unité/secteur du CEPD



De ce fait, 93,02 % de l'inventaire ont été notifiés et mis en œuvre.

Les 25 nouvelles notifications relatives à l'article 25 du règlement 45/2001 ont été distribuées parmi les unités et secteurs du CEPD comme présenté dans le schéma ci-dessus.

Les efforts considérables consentis par l'équipe RH ont permis de terminer toutes les notifications relatives aux traitements de données. Les autres unités, secteurs et fonctions (comme le Directeur, le DPD et le correspondant en comptabilité/CC) ont moins d'opérations de traitement à notifier. Au total toutefois, ces autres contrôleurs ont été responsables de 52 % des nouvelles notifications. Le diagramme ci-dessus donne un aperçu global de toutes les opérations de traitement au sein de l'institution.

Conformément aux lignes directrices du CEPD, le DPD s'est chargé des notifications soumises au CEPD au titre de l'article 27, paragraphe 2, du règlement 45/2001. En l'occurrence, très peu de notifications ont relevé de cette disposition en 2012.

Le principal objectif du DPD pour 2013 est de traiter les 3 notifications manquantes (une notification relative au système de gestion des dossiers, qui sera pleinement mis en œuvre dans le courant de l'année 2012, et deux autres du Comité du personnel) en plus des nouvelles opérations de traitement susceptibles de se présenter en cours d'année.

8.3. Enquête de 2012 du CEPD sur le statut des DPD

En mai 2012, le CEPD a lancé un questionnaire sur le statut des DPD afin de contrôler le respect, par les institutions et organes de l'Union européenne, de l'article 24 du règlement 45/2001. En juin, le directeur du CEPD a répondu à l'enquête avec une vue d'ensemble complète du statut et de l'évolution de la fonction de DPD au sein du CEPD lui-même. Les informations fournies concernent la désignation et le mandat, la formation, la position et les ressources du DPD.

8.4. Information et sensibilisation

Le DPD accorde une grande importance à la sensibilisation du personnel impliqué dans les différents traitements et à la communication du respect des règles de protection des données au sein du CEPD, en interne comme en externe.

En ce qui concerne la **communication externe**, la rubrique DPD du site internet du CEPD, qui fournit des informations sur le rôle et les activités du DPD, est actualisée régulièrement afin que le public puisse consulter le registre actualisé et toutes les notifications. En octobre 2012, la première demande d'accès public au registre a été reçue par le DPD. Une réponse a été envoyée sans retard le jour suivant avec un lien vers le registre sur le site internet du CEPD.

En 2012, le DPD a participé aux **réunions du réseau des DPD à Helsinki et à Francfort**. Ces réunions sont une occasion unique de créer des réseaux, d'évoquer les préoccupations communes et d'échanger les bonnes pratiques. Il a été décidé que le CEPD accueillerait la réunion du réseau des DPD au deuxième semestre 2013.

En ce qui concerne la **communication interne**, l'intranet du CEPD constitue une façon efficace de communiquer avec le personnel. La rubrique du DPD sur l'intranet contient des informations utiles pour les membres du personnel : les principaux aspects du rôle du DPD, les dispositions d'application, le plan d'action du DPD ainsi que des informations concernant les activités du DPD.

La rubrique du DPD sur l'intranet contient une liste très détaillée de déclarations de confidentialité (25 nouvelles notices légales) contenant toutes les informations pertinentes (en vertu des articles 11 et 12 du règlement 45/2001) à propos des opérations de traitement du CEPD, permettant à tous les membres du personnel de faire valoir leurs droits.

Le DPD a également été consulté à propos de l'utilisation possible de Twitter par le CEPD. Au vu de ses conseils, le conseil d'administration a décidé d'utiliser ce nouveau moyen de communication avec ses parties prenantes. La notice légale concernant l'utilisation de Twitter en tant que plate-forme d'information a été publiée sur le site internet du CEPD[35].

Dans le cadre de la sensibilisation, le DPD donne régulièrement une présentation intitulée «Initiation au règlement (CE) n° 45/2001», destinée aux nouveaux arrivants, aux stagiaires et aux fonctionnaires ne disposant pas d'expérience en matière de protection des données. Son objectif est de permettre aux membres du personnel de se familiariser avec notre mission de protection des données et nos valeurs.

[35] Voir http://www.edps.europa.eu/EDPSWEB/edps/EDPS/

9 PRINCIPAUX OBJECTIFS POUR 2013

Les objectifs suivants ont été sélectionnés pour 2013 dans le cadre de la stratégie générale pour 2013-2014. Les résultats obtenus figureront dans le rapport de 2013.

9.1. Supervision et mise en application

- **Contrôle préalables ex post**

Au début des activités du CEPD en 2004, il existait un arriéré de dossiers de contrôles préalables *ex post* concernant des opérations de traitement déjà en place. Il a donc été décidé d'accepter des notifications *ex post* malgré l'absence de base juridique pour cette pratique. Nous considérons que les institutions et organes de l'Union européenne ont eu suffisamment de temps pour nous notifier leurs activités de traitement existantes, et cette phase touche donc à sa fin. C'est pourquoi le CEPD a écrit aux institutions et organes de l'UE en juillet 2012 afin de fixer l'échéance de juin 2013 pour les notifications de tous les contrôles préalables ex post. Cela devrait provoquer une augmentation de notre charge de travail dans la première moitié de 2013.

- **Orientations et formation**

L'introduction du concept de responsabilité dans le cadre de protection des données implique que les administrations de l'UE vont devoir prendre toutes les mesures nécessaires pour garantir le respect des règles et tenir une documentation apportant la preuve que ces mesures sont effectives. Le CEPD est convaincu que DPD et CPD ont un rôle essentiel à jouer dans tout programme de responsabilisation. Afin de soutenir le travail des DPD et CPD et de contribuer à la promotion d'une culture de la protection des données au sein des institutions de l'UE, nous continuerons de proposer des orientations et des formations et nous encouragerons des contacts étroits avec le réseau des DPD.

- **Dialogue plus étroit avec les institutions de l'UE**

Lors du processus de consultation en vue de la révision stratégique, nos parties prenantes ont souligné la difficulté de garantir le respect des règles de protection des données tout en tenant compte des contraintes de l'administration de l'UE. Notre réussite dépendra d'une compréhension approfondie des exigences de protection des données par les responsables du traitement, les DPD et les CPD. Dans le cadre de l'objectif 1 de notre stratégie 2013-2014, nous allons entretenir des contacts et un dialogue étroits avec les institutions de l'UE afin d'encourager une meilleure compréhension du contexte institutionnel et de promouvoir une application pragmatique et pratique du règlement. Ce dialogue pourrait prendre différentes formes, notamment celle d'ateliers sur un thème particulier, de réunions ou de conférences téléphoniques.

- **États des lieux généraux**

Le CEPD compte lancer un nouvel exercice d'état des lieux dans toutes les institutions et tous les organes de l'UE. Cette initiative s'inscrit dans le cadre d'un exercice régulier dans lequel nous demandons un retour écrit concernant certains indicateurs de conformité aux différentes obligations. Les résultats de cette enquête permettront d'identifier les institutions ayant pris du retard dans leur programme de conformité et de compenser les lacunes éventuellement repérées.

- **Visites**

L'engagement de la direction est indispensable pour garantir le respect des règles de protection des données au sein de l'administration de l'UE. Nous allons poursuivre nos efforts de sensibilisation à tous les niveaux de direction et nous utiliserons si nécessaire nos pouvoirs d'exécution. Nous rendrons visite aux organes qui ne communiquent pas de manière adéquate avec nous ou qui montrent un manque d'engagement manifeste à respecter le règlement sur la protection des données.

- **Inspections**

Les inspections constituent un instrument essentiel qui nous permet de contrôler et d'assurer l'application du règlement. Nous comptons préciser encore notre politique en matière d'inspections et raffiner la procédure relative au processus d'inspection. Nous allons continuer de mener des inspections ciblées non seulement dans les domaines où nous avons fourni des orientations, mais aussi dans les cas où nous souhaitons vérifier la situation.

9.2. Politique et consultation

Le principal objectif de notre fonction consultative est de faire en sorte que le législateur européen ait conscience des normes applicables en matière de protection des données et qu'il intègre la protection des données dans les nouvelles législations. Ce point décrit les mesures conçues pour atteindre cet objectif. Nous devons relever le défi de remplir un rôle sans cesse plus important dans la procédure législative et de proposer en temps utile des conseils faisant autorité, le tout avec des moyens de plus en plus limités. Dans cette perspective, nous avons utilisé notre programme de questions politiques pour sélectionner les questions d'importance stratégique formant la pierre angulaire de notre travail consultatif pour 2013 (le programme et une note d'accompagnement sont publiés sur notre site internet).

- **Vers un nouveau cadre juridique de la protection des données**

Nous accorderons la priorité au processus d'examen en cours sur un cadre juridique de la protection des données dans l'UE. Nous avons rendu un avis sur les propositions législatives relatives à ce cadre et nous continuerons de contribuer aux débats aux prochaines étapes de la procédure législative chaque fois que cela sera nécessaire et indiqué.

- **Développements technologiques et agenda numérique, droits de propriété intellectuelle et internet**

Les développements technologiques, notamment les développements liés à l'internet et les réponses politiques correspondantes, constitueront un autre domaine d'intérêt du CEPD en 2013. Les thèmes vont des plans en vue d'un cadre paneuropéen pour l'identification, l'authentification et la signature électroniques à la question du contrôle de l'internet (par exemple, l'application des droits de propriété intellectuelle et les procédures de retrait), en passant par les services d'informatique dématérialisée. Nous renforcerons également notre savoir-faire technologique et participerons aux recherches sur les technologies permettant de renforcer la protection de la vie privée.

- **Développement de l'espace de liberté, de sécurité et de justice**

L'ELSJ demeurera l'un des domaines politiques clés traités par le CEPD. Parmi les propositions à venir en la matière, on peut citer la création d'un parquet européen chargé de lutter contre les crimes portant atteinte au budget de l'UE et la réforme d'EUROJUST. En outre, nous allons continuer de suivre les initiatives qui se poursuivent depuis l'année passée, comme la réforme d'EUROPOL et le paquet de mesures sur les frontières intelligentes. Nous allons également suivre de près les négociations avec les pays tiers en vue d'accords sur la protection des données.

- **Réformes du secteur financier**

Nous continuerons de suivre et d'examiner les nouvelles propositions pour la réglementation et la supervision des marchés et acteurs financiers, dans la mesure où ces propositions affectent le droit à la protection de la vie privée et des données. Cette démarche est d'autant plus importante qu'un nombre croissant de propositions sont avancées dans le but d'harmoniser le secteur financier et de le soumettre à une supervision centrale.

- **«Santé électronique»**

Vu la tendance croissante à intégrer les technologies numériques dans le cadre des services de santé, il est essentiel de définir des règles claires concernant l'utilisation des informations personnelles dans ce cadre, surtout au regard de la nature sensible des données relatives à la santé. Nous allons suivre les évolutions dans ce domaine et intervenir lorsque cela semblera nécessaire pour faire en sorte que les principes de la protection des données soient respectés et appliqués.

- **Autres initiatives**

Nous envisageons de publier des avis prospectifs visant à contribuer à la diffusion future des principes fondamentaux de la protection des données dans d'autres domaines de politique de l'UE comme la compétition et le commerce.

9.3. Coopération

Nous accorderons une attention particulière à la réalisation de la stratégie 2013-2014 concernant la coopération avec les autres autorités chargées de la protection des données, avec les organisations internationales, et concernant nos responsabilités en matière de supervision coordonnée.

- **Supervision coordonnée**

Nous allons continuer de jouer notre rôle dans la supervision coordonnée d'EURODAC, de CIS et de VIS. À ce titre, nous avons supervisé la mise en place du groupe de coordination de la supervision de VIS en novembre 2012. Le système d'information Schengen de deuxième génération (SIS II) fera également l'objet d'une supervision coordonnée. Son lancement est prévu pour 2013, et les préparatifs seront suivis de près, puisque la nouvelle agence chargée des grands systèmes informatiques ne deviendra opérationnelle qu'en décembre 2012. Nous effectuerons également des inspections des unités centrales de ces systèmes lorsque ces inspections seront nécessaires ou requises par la loi.

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

Nous allons continuer de contribuer activement aux activités et au succès du groupe de travail «Article 29», en assurant cohérence et synergie entre le groupe de travail et les positions du CEPD, conformément à leurs priorités respectives. Nous allons également maintenir nos bonnes relations avec les APD nationales. En tant que rapporteur de certains dossiers particuliers, le CEPD dirigera et préparera l'adoption des avis du groupe «Article 29».

- **Protection des données au sein des organisations internationales**

Les organisations internationales ne sont souvent pas soumises à la législation relative à la protection des données dans leur pays d'accueil. Cependant, elles ne disposent pas toutes leurs propres règles appropriées en matière de protection des données. Le CEPD continuera donc de se rapprocher des organisations internationales par un atelier annuel visant à sensibiliser et à encourager l'échange des bonnes pratiques.

9.4. Autres domaines

- **Information et communication**

Conformément à notre stratégie 2013-2014, le CEPD continuera de sensibiliser à la protection des données dans l'administration de l'UE. Nous poursuivrons également nos efforts pour informer les personnes de leurs droits fondamentaux en matière de vie privée et de protection des données.

Pour ce faire, nous allons développer notre stratégie de communication créative afin de gagner la confiance du public et l'engagement des institutions de l'UE. Cette initiative comportera:

- la mise à jour et la poursuite du développement de notre site internet;
- le développement de nouveaux outils de communication pour rendre les activités principales du CEPD plus visibles;

- l'utilisation d'un langage clair pour rendre les questions techniques plus accessibles, avec des exemples auxquels le grand public peut facilement s'identifier.

• Gestion des ressources et professionnalisation de la fonction RH

Dans ce contexte d'austérité économique, et avec la nécessité d'en faire plus avec moins, la stratégie de gestion de la qualité va être développée de façon à permettre à l'institution de jouer son rôle de la façon la plus efficace. Elle comprendra:

- une attention particulière accordée à une nouvelle politique de formation afin de renforcer les compétences professionnelles, de favoriser l'évolution des carrières et d'améliorer les performances;
- des efforts renouvelés visant à améliorer la planification, les performances et le suivi des dépenses des ressources financières;
- une approche plus stratégique de la gestion des ressources humaines; et
- un système de gestion de la qualité totale qui sera développé et mis en œuvre avec des liens clairs entre les normes de contrôle interne, la gestion des risques et le cadre commun d'évaluation.

Nous allons également lancer une réflexion stratégique sur les besoins de ressources à moyen et à long terme, en particulier dans le contexte du futur Comité européen de la protection des données.

• Infrastructure des technologies de l'information

Dans le courant de l'année, nous comptons lancer notre nouveau système de gestion des dossiers, afin de délivrer des résultats dans le respect du calendrier prévu, tout en respectant les garanties nécessaires en matière de sécurité et de protection des données.

Annexe A — Cadre juridique

Le Contrôleur européen de la protection des données a été créé par le règlement (CE) n° 45/2001 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données. Le règlement se fondait sur l'article 286 du traité CE, maintenant remplacé par l'article 16 du traité sur le fonctionnement de l'Union européenne (TFUE). Le règlement décrivait également les règles appropriées pour les institutions et les organes conformément à la législation relative à la protection des données qui existait alors dans l'UE. Le règlement est entré en vigueur en 2001[36].

Depuis l'entrée en vigueur du traité de Lisbonne, le 1er décembre 2009, l'article 16 du TFUE doit être considéré comme le fondement juridique du CEPD. L'article 16 souligne l'importance de la protection des données à caractère personnel d'une manière plus générale. L'article 16 du TFUE et l'article 8 de la charte européenne des droits fondamentaux, désormais contraignante, prévoient que le respect des règles relatives à la protection des données doit être soumis à un contrôle exercé par une autorité indépendante. Au niveau de l'UE, cette autorité est le CEPD.

Les autres actes de l'UE relatifs à la protection des données sont la directive 95/46/CE, qui définit le cadre général de la législation en matière de protection des données dans les États membres, la directive 2002/58/CE concernant la protection de la vie privée dans le secteur des communications électroniques (telle que modifiée par la directive 2009/136), et la décision-cadre 2008/977/JAI du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Ces trois instruments peuvent être considérés comme le résultat d'une évolution du cadre juridique qui a commencé au début des années 70 au sein du Conseil de l'Europe.

Contexte

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

La directive 95/46/CE a repris les principes de la Convention 108, en les précisant et en les développant de diverses manières. L'objectif était d'assurer un niveau élevé de protection et de permettre la libre circulation des données à caractère personnel au sein de l'UE. Quand la Commission a présenté la proposition de directive au début des années 90, elle a indiqué que les institutions et les organes de la Communauté devraient être couverts par des garanties légales similaires qui leur permettraient ainsi de participer à la libre circulation des données à caractère personnel soumises à des règles équivalentes de protection. Toutefois il n'existait, jusqu'à l'adoption de l'article 286 du TCE, aucune base juridique pour un tel instrument.

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

Règlement (CE) n° 45/2001

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

[36] JO L 8, 12.1.2001, p. 1.

législatifs de l'Union. Les conséquences précises de ces changements pourraient nécessiter une clarification supplémentaire.

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

Une des caractéristiques intéressantes du règlement est l'obligation qui est faite aux institutions et organes de l'Union de désigner au moins un délégué à la protection des données (DPD). Ces délégués sont chargés d'assurer, d'une manière indépendante, l'application interne des dispositions du règlement, y compris la notification appropriée des traitements. Des délégués sont désormais en place dans toutes les institutions et dans la plupart des organes, pour certains depuis plusieurs années. Ces délégués sont souvent 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 le point 2.2).

Tâches et compétences du CEPD

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

Cette présentation des attributions, fonctions et compétences suit, pour l'essentiel, le même schéma que pour les autorités nationales de contrôle: entendre et examiner les réclamations, effectuer d'autres enquêtes, informer le responsable du traitement et les personnes concernées, effectuer des contrôles préalables lorsque les opérations de traitement présentent des risques particuliers, etc. Le règlement habilite le CEPD à obtenir accès à toutes les informations utiles et aux locaux pertinents lorsque cela est nécessaire pour ses enquêtes. Le CEPD peut aussi imposer des sanctions et saisir la Cour de justice. Ces activités de supervision sont examinées de façon plus approfondie au chapitre 2 du présent rapport.

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

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

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

Article 41 — Le Contrôleur européen de la protection des données

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

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

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

Article 46 — Fonctions

Le Contrôleur européen de la protection des données:

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

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

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

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

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

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

ii) coopère également avec les organes de contrôle de la protection des données institués en vertu du titre VI du traité sur l'Union européenne en vue notamment d'améliorer la cohérence dans l'application des règles et procédures dont ils sont respectivement chargés d'assurer le respect;

g) participe aux activités du groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive 95/46/CE;

h) détermine, motive et rend publiques les exceptions, garanties, autorisations et conditions mentionnées à l'article 10, paragraphe 2, point b), à l'article 10, paragraphes 4, 5 et 6, à l'article 12, paragraphe 2, à l'article 19 et à l'article 37, paragraphe 2;

i) tient un registre des traitements qui lui ont été notifiés en vertu de l'article 27, paragraphe 2, et enregistrés conformément à l'article 27, paragraphe 5, et fournit les moyens d'accéder aux registres tenus par les délégués à la protection des données en application de l'article 26;

j) effectue un contrôle préalable des traitements qui lui ont été notifiés;

k) établit son règlement intérieur.

Article 47 — Compétences

1. Le Contrôleur européen de la protection des données :

(a) conseiller les personnes concernées dans l'exercice de leurs droits;

(b) saisir le responsable du traitement en cas de violation alléguée des dispositions régissant le traitement des données à caractère personnel et, le cas échéant, formuler des propositions tendant à remédier à cette violation et à améliorer la protection des personnes concernées;

(c) ordonner que les demandes d'exercice de certains droits à l'égard des données soient satisfaites lorsque de telles demandes ont été rejetées en violation des articles 13 à 19;

(d) adresser un avertissement ou une admonestation au responsable du traitement;

(e) ordonner la rectification, le verrouillage, l'effacement ou la destruction de toutes les données lorsqu'elles ont été traitées en violation des dispositions régissant le traitement de données à caractère personnel et la notification de ces mesures aux tiers auxquels les données ont été divulguées;

(f) interdire temporairement ou définitivement un traitement;

(g) saisir l'institution ou l'organe concerné et, si nécessaire, le Parlement européen, le Conseil et la Commission;

(h) saisir la Cour de justice des Communautés européennes dans les conditions prévues par le traité;

(i) intervenir dans les affaires portées devant la Cour de justice des Communautés européennes.

2. Le Contrôleur européen de la protection des données est habilité à:

(a) obtenir d'un responsable du traitement ou d'une institution ou d'un organe communautaire l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires à ses enquêtes;

(b) obtenir l'accès à tous les locaux dans lesquels un responsable du traitement ou une institution ou un organe communautaire exerce ses activités s'il existe un motif raisonnable de supposer que s'y exerce une activité visée par le présent règlement.

Annexe C — Liste des abréviations

ACAC	Accord commercial anti-contrefaçon
ACC	Autorité de contrôle commune
AECER	Agence exécutive du Conseil européen de la recherche
AEE	Agence européenne pour l'environnement
AESA	Agence européenne de la sécurité aérienne
APD	Autorité chargée de la protection des données
BCE	Banque centrale européenne
BEI	Banque européenne d'investissement
CC	Cour des Comptes
CCR	Centre commun de recherche
CdR	Comité des régions
CE	Communautés européennes
CEDH	Convention européenne des droits de l'homme
CEPCM	Centre européen de prévention et de contrôle des maladies
CEPD	Contrôleur européen de la protection des données
CGAM	Comité de gestion du régime commun d'assurance maladie
CJE	Cour de justice européenne
CPAS	Comité de Préparation pour les Affaires Sociales
CPD	Coordinateur de la protection des données
CSO	Centre de service et d'opération
DAS	Déclaration d'assurance
DEE	Décision d'enquête européenne
DG INFSO	Direction générale de la société de l'information et des médias
DG MARKT	Direction générale du marché intérieur et des services
DIGIT	Direction générale de l'informatique
DPD	Délégué à la protection des données
DPE	Décision de protection européenne
EEA	École européenne d'administration
EFSA	Autorité européenne de sécurité des aliments
END	Expert national détaché
ENISA	Agence européenne chargée de la sécurité des réseaux et de l'information
EPSO	Office européen de sélection du personnel
FRA	Agence des droits fondamentaux de l'Union européenne
GTPJ	Groupe de travail sur la police et la justice
HCRNU	Haut Commissariat des Nations Unies pour les réfugiés
IMI	Système d'information du marché intérieur
LIBE	Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen
OCC	Organe de contrôle commun
OCR	Opération conjointe de retour
OHMI	Office de l'harmonisation dans le marché intérieur
OIM	Organisation internationale pour les migrations
OLAF	Office européen de lutte antifraude
OMD	Organisation mondiale des douanes
PNR	Données des dossiers passagers
RFID	Identification par radiofréquence
RH	Ressources humaines
RLS	Responsable local de la sécurité
RLSI	Responsable local de la sécurité informatique
SAI	Service d'audit interne
SAPR	Système d'alerte précoce et de réaction
SID	Système d'information douanier
SIS	Système d'information Schengen
SSI	Stratégie de sécurité intérieure

s-TESTA	Services télématiques transeuropéens sécurisés entre administrations
SWIFT	Société de télécommunications interbancaires mondiales
TFTP	Programme de surveillance du financement du terrorisme
TFTS	Système de surveillance du financement du terrorisme
TFUE	Traité sur le fonctionnement de l'Union européenne
TI	Technologies de l'information
TIC	Technologies de l'information et de la communication
TURBINE	TrUsted Revocable Biometrics IdeNtitiEs
UE	Union européenne
VIS	Système d'information sur les visas
WP 29	Groupe travail de l'article 29 sur la protection des données

Annexe D — Liste des délégués à la protection des données

ORGANISATION	NOM	E-MAIL
Parlement européen (PE)	Secondo SABBIONI	Data-Protection@europarl.europa.eu
Conseil de l'Union européenne (Consilium)	Carmen LOPEZ RUIZ	Data.Protection@consilium.europa.eu
Commission européenne (CE)	Philippe RENAUDIÈRE	Data-Protection-officer@ec.europa.eu
Cour de justice de l'Union européenne (CURIA)	Valerio Agostino PLACCO	Dataprotectionofficer@curia.europa.eu
Cour des comptes européenne (ECA)	Johan VAN DAMME	Data-Protection@eca.europa.eu
Comité économique et social européen (CESE)	Maria ARSENE	Data.Protection@eesc.europa.eu
Comité des régions (CdR)	Rastislav SPÁC	Data.Protection@cor.europa.eu
Banque européenne d'investissement (BEI)	Alberto SOUTO DE MIRANDA	Dataprotectionofficer@eib.org
Service européen pour l'action extérieure (SEAE)	Ingrid HVASS. a.i Carine CLAEYS	Ingrid.HVASS@eeas.europa.eu Carine.CLAEYS@eeas.europa.eu
Médiateur européen	Rosita AGNEW	DPO-euro-ombudsman@ombudsman.europa.eu
Contrôleur européen de la protection des données (CEPD)	Sylvie PICARD	Sylvie.picard@edps.europa.eu
Banque centrale européenne (BCE)	Frederik MALFRÈRE	DPO@ecb.int
Office européen de lutte antifraude (OLAF)	Laraine LAUDATI	Laraine.Laudati@ec.europa.eu
Centre de traduction des organes de l'Union européenne (CdT)	Edina TELESSY	Data-Protection@cdt.europa.eu
Office de l'harmonisation dans le marché intérieur (OHMI)	Gregor SCHNEIDER	DataProtectionOfficer@oami.europa.eu
Agence des droits fondamentaux de l'Union européenne (FRA)	Nikolaos FIKATAS	Nikolaos.Fikatas@fra.europa.eu
Agence européenne des médicaments (EMEA)	Alessandro SPINA	Data.Protection@emea.europa.eu
Office communautaire des variétés végétales (CPVO)	Véronique DOREAU	Doreau@cpvo.europa.eu
Fondation européenne pour la formation (ETF)	Tiziana CICCARONE	Tiziana.Ciccarone@etf.europa.eu
Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)	Ulrike LECHNER	Dataprotection@enisa.europa.eu
Fondation européenne pour l'amélioration des conditions de vie et de travail (Eurofound)	Markus GRIMMEISEN	mgr@eurofound.europa.eu

>>>

ORGANISATION	NOM	E-MAIL
Observatoire européen des drogues et des toxicomanies (EMCDDA)	Ignacio Vázquez MOLINÍ	Ignacio.Vazquez-Molini@emcdda.europa.eu
Autorité européenne de sécurité des aliments (EFSA)	Claus RÉUNIS	Dataprotectionofficer@efsa.europa.eu
Agence européenne pour la sécurité maritime (EMSA)	Malgorzata NESTEROWICZ	Malgorzata.Nesterowicz@emsa.europa.eu
Centre européen pour le développement de la formation professionnelle (Cedefop)	Spyros ANTONIOU	Spyros.Antoniou@cedefop.europa.eu
Agence exécutive «Éducation, Audiovisuel et Culture» (EACEA)	Hubert MONET	eacea-data-protection@ec.europa.eu
Agence européenne pour la sécurité et la santé au travail (OSHA)	Emmanuelle BRUN	brun@osha.europa.eu
Agence communautaire de contrôle des pêches (CFCA)	Rieke ARNDT	cfca-dpo@cfca.europa.eu
Centre satellitaire de l'Union européenne (CSUE)	Jean-Baptiste TAUPIN	j.taupin@eusc.europa.eu
Institut européen pour l'égalité entre les hommes et les femmes (EIGE)	Ramunas LUNSKUS	Ramunas.Lunskus@eige.europa.eu
Autorité de surveillance du GNSS européen (GSA)	Triinu VOLMER	Triinu.Volmer@gsa.europa.eu
Agence ferroviaire européenne (ERA)	Zografia PYLORIDOU	Dataprotectionofficer@era.europa.eu
Agence exécutive pour la santé et les consommateurs (EAHC)	Beata HARTWIG	Beata.Hartwig@ec.europa.eu
Centre européen de prévention et de contrôle des maladies (CEPCM)	Rebecca TROTT	Rebecca.trott@ecdc.europa.eu
Agence européenne pour l'environnement (AEE)	Olivier CORNU	Olivier.Cornu@eea.europa.eu
Fonds européen d'investissement (FEI)	Jobst NEUSS	J.Neuss@eif.org
Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures (Frontex)	Sakari VUORENSOLA	Sakari.Vuorensola@frontex.europa.eu
Agence européenne de la sécurité aérienne (EASA)	Francesca PAVESI a.i. Frank Manuhutu	Francesca.Pavesi@easa.europa.eu
Agence exécutive pour la compétitivité et l'innovation (EACI)	Elena FIERRO SEDANO	Elena.Fierro-Sedano@ec.europa.eu
Agence exécutive du réseau transeuropéen de transport (TEN-T EA)	Zsófia SZILVÁSSY	Zsofia.Szilvassy@ec.europa.eu
Autorité bancaire européenne (ABE)	Joseph MIFSUD	Joseph.MIFSUD@eba.europa.eu

>>>

ORGANISATION	NOM	E-MAIL
Agence européenne des produits chimiques (ECHA)	Bo BALDUYCK	data-protection-officer@echa.europa.eu
Agence exécutive du Conseil européen de la recherche (ERCEA)	Nadine KOLLOCZEK	Nadine.Kolloczek@ec.europa.eu
Agence exécutive pour la recherche (REA)	Evangelos TSAVALOPOULOS	Evangelos.Tsavalopoulos@ec.europa.eu
Comité européen du risque systémique (CERS)	Frederik MALFRÈRE	DPO@ecb.int
Fusion à des fins énergétiques – F4E	Angela BARDENEWER-RATING	Angela.Bardenhewer@f4e.europa.eu
Entreprise commune SESAR	Daniella PAVKOVIC	Daniella.Pavkovic@sesarju.eu
Entreprise commune ARTEMIS	Anne SALAÜN	Anne.Salaun@artemis-ju.europa.eu
Entreprise commune Clean Sky	Bruno MASTANTUONO	Bruno.Mastantuono@cleansky.eu
Initiative Médicaments innovants (IMI)	Estefania RIBEIRO	Estefania.Ribeiro@imi.europa.eu
Entreprise commune Piles à combustible et hydrogène	Nicolas BRAHY	Nicolas.Brahy@fch.europa.eu
Autorité européenne des assurances et des pensions professionnelles (AEAPP)	Catherine COUCKE	catherine.coucke@eiopa.europa.eu
Collège européen de police (CEPOL)	Leelo KILG-THORNLEY	leelo.kilg-thornley@cepol.europa.eu
Institut européen d'innovation et de technologie (EIT)	Roberta MAGGIO a.i. Francesca LOMBARDO	roberta.maggio@eit.europa.eu
Agence européenne de défense (EDA)	Alain-Pierre LOUIS	alain-pierre.louis@eda.europa.eu
Entreprise commune ENIAC	Marc JEUNIAUX	Marc.Jeuniaux@eniac.europa.eu
Organe des régulateurs européens des communications électroniques (ORECE)	Michele Marco CHIODI	Michele-Marco.CHIODI@berec.europa.eu
Agence de coopération des régulateurs de l'énergie (ACER)	Paul MARTINET	Paul.MARTINET@acer.europa.eu
Bureau européen d'appui en matière d'asile EASO)	Paula McCLURE	paula-mello.mcclure@ext.ec.europa.eu

Annexe E — Liste des avis de contrôle préalable et des avis sur l'absence de contrôle préalable

Système de contrôle électronique - ERA

Avis du 6 décembre 2012 sur les notifications en vue d'un contrôle préalable reçues du délégué à la protection des données de l'Agence ferroviaire européenne (AFE) concernant le système de courrier électronique et le système de courrier électronique d'arrière-plan de l'AFE (dossiers 2012-136 et 137)

Système internet - ERA

Avis du 6 décembre 2012 sur la notification de contrôle préalable reçue du délégué à la protection des données de l'Agence ferroviaire européenne (ERA) à propos de l'utilisation du système internet de l'ERA (Dossier 2012-0135)

Base de données d'experts scientifiques internes - EFSA

Avis sur la notification d'un contrôle préalable reçue du délégué à la protection des données de l'Autorité européenne de sécurité des aliments («EFSA») à propos du dossier «Base de données d'experts scientifiques internes de l'EFSA» (Dossier 2011-0882)

Procédure de mobilité interne - AECER

Avis du 3 décembre 2012 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de l'Agence exécutive du Conseil européen de la recherche (AECER) concernant la procédure de mobilité interne pour les agents temporaires et contractuels de l'AECER (Dossier 2012-0870)

Étude clinique menée dans le cadre du projet de recherche du lot 4 de PROTECT - EMA

Avis du 29 novembre sur la notification de contrôle préalable reçue du délégué à la protection des données de l'Agence européenne des médicaments à propos de «l'étude clinique menée dans le cadre du projet de recherche du lot 4 de PROTECT» (Dossier 2012-0704)

Procédure de sélection pour le poste de membre du conseil d'administration - EMA

Avis sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Commission européenne à propos de la procédure de sélection pour le poste de membre du conseil d'administration de l'Agence européenne des médicaments (EMA) et le poste de membre des comités scientifiques de l'EMA suivants: le comité des thérapies innovantes, le comité des médicaments orphelins, le comité pédiatrique et le comité pour l'évaluation des risques en matière de pharmacovigilance (Dossier 2011-1166)

Télétravail - Conseil de l'Union européenne

Avis du 23 novembre 2012 sur la notification d'un contrôle préalable reçue du délégué à la protection des données du Secrétariat Général du Conseil à propos du dossier «télétravail» (Dossier 2012-0661)

Procédures anti-harcèlement - EMSA

Avis du 23 novembre 2012 sur la notification d'un contrôle préalable concernant les procédures anti-harcèlement à l'EMSA (Dossier 2012-0302)

Enquêtes administratives - FRA

Avis du 23 novembre 2012 sur la notification d'un contrôle préalable concernant les enquêtes administratives à l'Agence des droits fondamentaux (FRA) (Dossier 2012-0683)

Commission d'invalidité - Eurofound

Avis du 20 novembre 2012 sur la notification d'un contrôle préalable à propos la commission d'invalidité d'Eurofound (Dossier 2011-0643)

Procédure d'attestation - Cedefop

Avis du 19 novembre 2012 sur la notification reçue du délégué à la protection des données du Cedefop en vue d'un contrôle préalable concernant la procédure d'attestation (Dossier 2012-0706)

Surveillance internet - Cedefop

Avis du 15 novembre 2012 sur la notification de contrôle préalable reçue du délégué à la protection des données du Centre européen pour le développement de la formation professionnelle (CEDEFOP) concernant la surveillance de l'utilisation de l'internet (traitement de données en relation avec un système proxy) (Dossier 2011-1069)

Évaluation du personnel - AESA

Avis du 22 octobre 2012 sur la notification de contrôle préalable concernant les procédures d'évaluation du personnel de l'AESA (Dossier 2011-1113)

Stage, évaluation annuelle et reclassement – F4E

Avis du 16 octobre 2012 sur les notifications en vue d'un contrôle préalable reçues du délégué à la protection des données de l'agence Fusion for Energy concernant le stage, l'évaluation annuelle, la pro-

motion, la revalorisation et le reclassement (dossiers 2012-404, 405, 406, 407 et 408)

Assistance, Spécialistes des facteurs humains, Enquêtes sur les accidents ferroviaires - ERA

Avis du 10 octobre 2012 sur la notification de contrôle préalable reçue du délégué à la protection des données de l'Agence ferroviaire européenne concernant les «appels à candidatures en vue de la constitution d'une liste de spécialistes des facteurs humains afin d'assister l'organisme d'enquête national de certains États membres dans les enquêtes sur les accidents ferroviaires» (Dossier 2012-0635)

Instance spécialisée en matière d'irrégularités financières – Conseil de l'Union européenne

Avis du 26 septembre 2012 sur la notification d'un contrôle préalable reçue du Délégué à la protection des données du secrétariat général du Conseil de l'Union européenne à propos du dossier «Instance spécialisée en matière d'irrégularités financières» (Dossier 2012-0533)

Données relatives à la santé – EACEA

Avis du 12 septembre 2012 sur la notification d'un contrôle préalable concernant le traitement de données relatives à la santé à l'EACEA (dossier 2012-0537)

Autorisation d'entrée et du contrôle des accès pour la protection physique (ZES+ZKS) - CCR-ITU à Karlsruhe – Commission européenne

Avis du 24 juillet 2012 sur une notification en vue d'un contrôle préalable reçue du délégué à la protection des données de la Commission européenne à propos de l'autorisation d'entrée et du contrôle des accès pour la protection physique au Centre commun de recherche ITU (Dossier 2008-0726)

Déclarations d'intérêt annuelles – CEPCM (Centre européen de prévention et de contrôle des maladies)

Avis du 19 juillet 2012 sur la notification d'un contrôle préalable reçue du délégué à la protection des données du Centre européen de prévention et de contrôle des maladies concernant le traitement des déclarations d'intérêt annuelles (Dossier 2010-0914)

Évaluations du personnel - CdT

Avis du 19 juillet 2012 sur la notification d'un contrôle préalable reçue du délégué à la protection des données du Centre de Traduction concernant l'évaluation du personnel (Dossier 2012-475)

Désignation du 3ème/2ème médecin dans la commission d'invalidité et commission médicale – Cour de justice

Avis du 18 juillet 2012 sur la notification d'un contrôle préalable à propos du dossier «Désignation du troisième (ou deuxième) médecin dans la commission d'invalidité et commission médicale» (Dossier 2011-0775)

Réclamations visées à l'article 90 bis du statut des fonctionnaires - OLAF

Avis du 16 juillet 2012 sur la notification en vue d'un contrôle préalable reçue de la déléguée à la protection des données de l'Office européen de lutte antifraude (OLAF) concernant le traitement de données à caractère personnel en rapport avec les réclamations visées à l'article 90 bis du statut des fonctionnaires (Dossier 2012-0274)

Procédures disciplinaires et enquêtes administratives - CdT

Avis du 06 juillet 2012 sur la notification en vue d'un contrôle préalable concernant les procédures administratives et les enquêtes administratives (Dossier 2011-0916)

Échanges interinstitutionnels de personnel des services linguistiques

Avis conjoint du 5 juillet 2012 sur une notification d'un contrôle préalable reçue des délégués à la protection des données de la Commission européenne, du Conseil, du Parlement européen, de la Banque centrale européenne, du Centre de traduction des organes de l'Union européenne, du Comité économique et social européen, du Comité des régions et de la Cour des comptes européenne concernant les échanges interinstitutionnels de personnel des services linguistiques des institutions et organes de l'Union européenne (Dossiers conjoints 2011-0560 et 2011-1029)

Sélection et nomination des deux groupes des parties intéressées - AEAPP

Avis du 3 juillet 2012 sur la notification en vue d'un contrôle préalable concernant la sélection et la nomination des deux groupes des parties intéressées de l'Autorité européenne des assurances et des pensions professionnelles (AEAPP) (Dossier 2012-0264)

Gestion du Bureau Véhicules de Service – Conseil de l'Union européenne

Avis du 27 juin 2012 sur la notification en vue d'un contrôle préalable concernant la gestion du bureau «Véhicules de service» – Conseil de l'Union européenne (dossier 2012-0157)

Certification - CdT

Avis du 11 juin 2012 sur la notification d'un contrôle préalable concernant la procédure de certification, Centre de traduction (Dossier 2011-1156)

Évolution de carrière et évaluation du personnel d'encadrement intermédiaire et supérieur - Cedefop

Avis du 11 juin 2012 sur la notification en vue d'un contrôle préalable concernant la promotion, l'évolution de carrière ainsi que l'évaluation du personnel d'encadrement intermédiaire et supérieur, Cedefop (Dossiers 2012-009 et 2012-010)

Stage, rapport d'évolution de carrière et reclassement - EAHC

Avis du 11 juin 2012 sur la notification en vue d'un contrôle préalable concernant le stage, le rapport d'évolution de carrière et le reclassement, l'Agence exécutive pour la santé et les consommateurs (Dossiers 2010-828 et 2010-149)

Stage - AFE

Avis du 14 juin 2012 sur les notifications reçues du DPD de l'AFE en vue d'un contrôle préalable concernant le stage, le REC, le reclassement, l'évaluation de la capacité à travailler dans une troisième langue et l'utilisation d'indicateurs de performance dans le REC des AAF ainsi que le renouvellement du contrat de travail des fonctionnaires de l'AFE (Dossiers 2011-960, 2011-961, 2011-962, 2012-087 et 2012-138)

Données relatives à la santé – F4E

Lettre du 7 juin 2012 sur la notification d'un contrôle préalable concernant le traitement de données relatives à la santé dans l'action F4E (Dossiers 2011-1088, 2011-1089, 2011-1090, 2011-1091)

Enregistrement de ligne téléphonique

Avis du 7 juin 2012 sur la notification d'un contrôle préalable relatif au dossier «enregistrement de la ligne réservée aux appels au dispatching technique relatifs aux interventions dans les immeubles de l'UE à Luxembourg (n° 12 ou 32220)» (Dossier 2011-0986)

Recrutement en ligne – OEDT

Avis du 31 mai 2012 sur la notification d'un contrôle préalable concernant les procédures de recrutement en ligne de l'OEDT (Dossier 2012-0290)

Procédures d'évaluation, de stage et de reclassement du personnel - FRONTEX

Avis du 30 mai 2012 sur la notification en vue d'un contrôle préalable concernant les procédures d'évaluation, de stage et de reclassement du personnel, FRONTEX (Dossier 2011-969)

Évaluation annuelle - EACI

Avis du 29 mai 2012 sur les notifications en vue d'un contrôle préalable concernant l'évaluation annuelle, le reclassement, le stage et l'évaluation de la capacité à travailler dans une troisième langue, Agence exécutive pour la compétitivité et l'innovation (EACI) (Dossiers 2011-998, 2011-999 et 2011-1000)

Enregistrement de la ligne téléphonique - CE

Avis du 24 mai 2012 sur une notification d'un contrôle préalable relatif au dossier «Enregistrement de la ligne téléphonique utilisée pour les rapports du service de gardiennage et les appels relatifs aux interventions liées au système de contrôle d'accès aux bâtiments de la Commission (Bruxelles)», Commission européenne (Dossier 2011-0987)

Système «Safe Mission Data» - PE

Avis du 24 mai 2012 sur une notification en vue d'un contrôle préalable concernant le système «Safe Mission Data», Parlement européen (Dossier 2012-0105)

Lire plus

Vacances d'emploi hors encadrement – Commission européenne

Avis du 22 mai 2012 sur la notification en vue d'un contrôle préalable concernant le dossier «Vacances d'emploi hors encadrement» - Commission européenne (Dossier 2012-0276)

Register of telephone calls - BEI

Avis du 15 mai 2012 sur la notification d'un contrôle préalable à propos du dossier «Register of telephone calls (téléphonie mobile)», Banque européenne d'investissement (Dossier 2009-0704)

Système de stages d'études - F4E

Avis du 11 mai 2012 sur la notification en vue d'un contrôle préalable concernant la procédure de sélection pour le système de stages d'études et gestion du système, Fusion for Energy (Dossier 2012-246)

Procédures d'octroi et de gestion des subventions - EACEA

Avis du 11 mai 2012 sur la notification d'un contrôle préalable concernant les procédures d'octroi et de gestion des subventions, Agence exécutive «Éducation, audiovisuel et culture» (Dossier 2011-1083)

Traitement de données à caractère personnel par le Comité déontologique et de conformité - BEI

Avis du 11 avril 2012 sur la notification d'un contrôle préalable concernant le traitement de données à caractère personnel par le Comité déontologique et de conformité, Banque européenne d'investissement (Dossier 2011-1141)

Accréditation de journalistes au Parlement européen

Avis du 3 avril 2012 sur la notification en vue d'un contrôle préalable concernant l'accréditation des journalistes au du Parlement européen (Dossier 2011-0991)

Contrôle et évaluation des auxiliaires interprètes de conférence - CE

Avis du 29 mars 2012 sur la notification de contrôle préalable concernant le contrôle continu de la qualité et l'évaluation des auxiliaires interprètes de conférence au sein de la DG Interprétation, Commission européenne (Dossier 2012-912)

Évaluation annuelle et reclassement des agents temporaires - ENISA

Avis du 27 mars 2012 sur la notification en vue d'un contrôle préalable concernant l'évaluation annuelle et le reclassement des agents temporaires, Agence européenne chargée de la sécurité des réseaux et de l'information (Dossiers 2010-936 et 2010-937)

Promotion et reclassement - EFSA

Avis du 26 mars 2012 sur la notification en vue d'un contrôle préalable concernant la promotion et le reclassement, Autorité européenne de sécurité des aliments (Dossier 2012-0079)

Appels à manifestation d'intérêt pour la sélection d'experts - EACEA

Avis du 22 mars 2012 sur la notification en vue d'un contrôle préalable concernant les appels à manifestation d'intérêt pour la sélection d'experts (Dossier 2012-0007)

Contrôle des travaux des experts externes - EACEA

Avis du 22 mars 2012 sur une notification en vue d'un contrôle préalable concernant le contrôle des travaux des experts externes (Dossier 2012-008)

Évaluation de la performance - FRA

Avis du 21 mars 2012 sur la notification en vue d'un contrôle préalable reçue du délégué à la protection des données de l'Agence des droits fondamentaux de l'Union européenne concernant l'évaluation de la performance, la période de stage, l'évolution de carrière, le reclassement ainsi que l'évaluation et la période de stage du directeur (2011-938, 2011-954, 2011-1076 and 2011-1077)

Organisation des réunions et des repas des réunions des réunions des chefs d'État ou de gouvernement - Conseil

Avis du 16 mars 2012 sur une notification en vue d'un contrôle préalable reçue du délégué à la protection des données du Conseil de l'Union européenne concernant l'«organisation des réunions et des repas des réunions des chefs d'État ou de gouvernement, des sommets ou des réunions officielles avec des pays tiers et du Conseil de l'Union européenne et d'autres réunions au niveau ministériel ou supérieur» (Dossier 2011-0933)

Règlement exigeant le gel de fonds

Avis du 22 février 2012 sur la notification d'un contrôle préalable concernant le traitement de données à caractère personnel dans le cadre de règlements instituant des mesures restrictives liées à la PESC et consistant à geler des fonds (Dossier 2010-0426)

Lire plus

Colonies de vacances - Conseil

Avis du 22 février 2012 sur la notification en vue d'un contrôle préalable à propos du dossier «Colonies de vacances» (Dossier 2011-0950)

Télétravail - CdR

Avis du 13 février 2012 sur la notification d'un contrôle préalable à propos du dossier «télétravail» (Dossier 2011-1133)

Stage des Chefs d'unité/Directeurs nouvellement nommés - CCE

Avis du 13 février 2012 sur une notification en vue d'un contrôle préalable à propos du dossier procédures «stage des Chefs d'unité/Directeurs nouvellement nommés» (Dossier 2011-0988)

Procédures d'évaluation du personnel - EACEA

Avis du 6 février 2012 sur la notification en vue d'un contrôle préalable concernant le rapport d'évolution de carrière, le stage et le reclassement, Agence exécutive «Éducation, audiovisuel et culture» (Dossiers conjoints 2010-589 et 2011-1071 et 2011-1072)

Procédures d'évaluation du personnel - ACCP

Avis du 6 février 2012 sur la notification d'un contrôle préalable concernant l'évaluation du personnel, la procédure de stage pour les agents contractuels et le reclassement des agents temporaires, Agence communautaire de contrôle des pêches (ACCP) (Dossier 2011-0952)

Procédures d'enquête - OLAF

Avis du 3 février 2012 sur les notifications en vue d'un contrôle préalable concernant les nouvelles procédures d'enquête de l'OLAF (enquêtes internes, enquêtes externes, plaintes rejetées et informations entrantes ne présentant aucun intérêt dans le cadre d'enquêtes, enquêtes de coordination et mise en œuvre des recommandations de l'OLAF), Office européen de lutte anti-fraude (OLAF) (Dossiers 2011-1127, 2011-1129, 2011-1130, 2011-1131, 2011-1132)

Enquêtes administratives et procédures disciplinaires - OCVV

Lettre du 3 février 2012 sur la notification en vue d'un contrôle préalable au sujet du traitement des enquêtes administratives et des procédures disciplinaires de l'Office communautaire des variétés végétales (OCVV) (Dossier 2011-1128)

Titularisation des fonctionnaires stagiaires/Gestion des rapports de stage des agents - CdR

Avis du 26 janvier 2012 sur la notification d'un contrôle préalable à propos du dossier «Titularisation des fonctionnaires stagiaires/Gestion des rapports de stage des agents» (Dossier 2011-1118)

Période de stage et certification - OEDT

Avis du 08 mars 2012 sur les notifications de contrôle préalable concernant les procédures de recrutement du personnel à l'IMI (Dossiers 2011-0822 et 2011-1080)

Procédures de promotion - Conseil de l'Union européenne

Lettre du 17 février 2012 concernant la notification en vue d'un contrôle préalable concernant la période de stage et les procédures de certification à l'OEDT (Dossier 2011-1161)

Recrutement du personnel - IMI

Lettre du 13 février 2012 sur la notification en vue d'un contrôle préalable concernant les procédures de recrutement du personnel à l'IMI (Dossier 2011-0872)

Recrutement et évaluation du personnel - CleanSky

Avis du 13 février 2012 sur la notification en vue d'un contrôle préalable concernant les procédures de recrutement et d'évaluation de recrutement du personnel pour CleanSky (Dossier 2011-0839)

Recrutement du personnel – EC Artemis

Avis du 27 janvier 2012 sur la notification en vue d'un contrôle préalable concernant les procédures de recrutement les procédures de recrutement du personnel de l'entreprise conjointe Artemis (Dossier 2011-0831)

Sélection de conseillers confidentiels et procédures informelles pour les cas de harcèlement - OCVV

Avis du 23 janvier 2012 sur la notification en vue d'un contrôle préalable concernant la sélection de conseillers confidentiels et les procédures informelles applicables dans les cas de harcèlement à l'Office communautaire des variétés végétales (OCVV) (Dossier 2011-1073)

Procédures de passation de marché et d'octroi de subvention - CEDEFOP

Avis du 19 janvier 2012 sur la notification d'un contrôle préalable concernant les procédures de passation de marché et d'octroi de subvention du Centre européen pour le développement de la formation professionnelle (CEDEFOP) (dossier 2011-0542)

Procédures d'évaluation du personnel – EC PCH

Avis du 16 janvier 2012 sur la notification d'un contrôle préalable concernant le stage et l'évaluation annuelle, Entreprise commune Piles à combustible et Hydrogène (Dossier 2011-835)

Procédure de passation de marchés - Agence communautaire de contrôle des pêches

Avis du 13 janvier 2012 sur la notification d'un contrôle préalable concernant l'appel à manifestation d'intérêt n° CFCA/2010/CEI/01 et les contrats qui en découlent, Agence communautaire de contrôle des pêches (ACCP) (Dossier 2011-1001)

Sous-traitance partielle de la Caisse Maladie - EIB

Lettre du 10 janvier 2012 sur la notification modifiée d'un contrôle préalable concernant la sous-traitance partielle de la caisse maladie à la Banque Européenne d'Investissement (BEI) (dossier 2011-1039)

Procédures d'évaluation du personnel – EU-OSHA

Avis conjoint du 9 janvier 2012 sur les notifications en vue d'un contrôle préalable concernant les procédures d'évaluation du personnel à l'Agence européenne pour la sécurité et la santé au travail (EU-OSHA) (Dossiers 2011-957, 2011-958, 2011-959)

Liste de cas non soumis à un contrôle préalable en 2012

Carte de profils professionnels - CEPCM

Lettre du 20 décembre 2012 relative à une notification de contrôle préalable concernant les activités de traitement liées à la carte de profils professionnels du CEPCM (Dossier 2012-0900)

Personnel statutaire – ERCEA

Lettre du 20 décembre 2012 relative à une notification de contrôle préalable concernant les activités de traitement dans le contexte de la cessation de fonctions du personnel statutaire de l'ERCEA (Dossier 2012-0898)

Actions de formation - ERCEA

Lettre du 19 décembre 2012 sur la notification en vue d'un contrôle préalable concernant la «gestion des demandes de formation et activités de formation pour le personnel de l'ERCEA» (Dossier 2012-0915)

Utilisation du téléphone - ETF

Réponse du 11 décembre 2012 concernant un contrôle préalable des activités de traitement de données à caractère personnel liées à l'utilisation du téléphone à l'ETF (Dossier 2012-0917)

Étude sur la satisfaction du personnel - EACI

Réponse du 9 octobre 2012 sur la notification en vue d'un contrôle préalable concernant les activités de traitement liées à l'«étude relative à la satisfaction du personnel de l'EACI» (Dossier 2012-0527)

Opérations de traitement dans l'application MATRIX - FRA

Réponse du 12 septembre 2012 sur la notification en vue d'un contrôle préalable concernant les opérations de traitement dans l'application MATRIX à l'Agence des droits fondamentaux (FRA) (Dossier 2012-0090)

Fonction de recherche - OLAF

Avis du 10 août 2012 sur la notification en vue d'un contrôle préalable reçue de la déléguée à la protection des données de l'Office européen de lutte antifraude (OLAF) concernant le traitement de données à caractère personnel en rapport avec la fonction de recherche (Dossier 2012-0279)

Horaire flexible - FRA

Réponse du 13 avril 2012 à une notification de contrôle préalable au sujet des traitements de données sur «l'horaire flexible» au sein de l'Agence des droits fondamentaux de l'Union européenne (FRA) (Dossier 2012-0089)

European Union Transaction Log (EUTL) – Commission européenne

Réponse du 13 avril 2012 à une notification de contrôle préalable concernant les opérations de traitement du European Union Transaction Log (EUTL) à la Commission européenne (Dossier 2011-1153)

Activités extérieures - Médiateur européen

Réponse du 12 janvier 2012 à la notification en vue d'un contrôle préalable concernant la procédure de traitement concernant les activités extérieures des membres du Bureau du Médiateur européen (Dossier 2012-0005)

Modules d'apprentissage sur ordinateur - Conseil

Réponse du 10 janvier 2012 à une notification de contrôle préalable concernant les opérations de traitement dans le cadre des modules d'apprentissage par ordinateur relatifs à la sécurité au Conseil de l'Union européenne (Dossier 2011-1058)

Annexe F — Liste des avis et observations formelles sur des propositions législatives

Avis sur des propositions législatives

Essais cliniques de médicaments

Avis du 19 décembre 2012 sur la proposition de règlement relatif aux essais cliniques de médicaments à usage humain et abrogeant la directive 2001/20/CE

Statut et financement des partis politiques européens

Avis du Contrôleur européen de la protection des données du 13 décembre 2012 sur la proposition de règlement relatif au statut et au financement des partis politiques européens et des fondations politiques européennes

Corps volontaire européen d'aide humanitaire

Avis du 23 novembre 2012 sur la proposition de règlement portant création du corps volontaire européen d'aide humanitaire

Intermédiation en assurance, organismes de placement collectif en valeurs mobilières et produits de placement

Avis du 23 novembre 2012 sur les propositions d'une directive sur l'intermédiation en assurance, d'une directive modifiant certaines dispositions de la directive 2009/65/CE portant coordination des dispositions législatives, réglementaires et administratives concernant certains organismes de placement collectif en valeurs mobilières et d'un règlement sur les principaux documents d'information relatifs aux produits de placement

Informatique en nuage en Europe

Avis du 16 novembre 2012 sur la communication de la Commission intitulée «Exploiter le potentiel de l'informatique en nuage en Europe»

Dépôt des archives historiques des institutions à l'Institut universitaire européen de Florence

Avis du 10 octobre 2012 sur la proposition par la Commission de règlement du Conseil modifiant le règlement (CEE, Euratom) n° 354/83 en ce qui concerne le dépôt des archives historiques des institutions à l'Institut universitaire européen de Florence

Financement, gestion et suivi de la politique agricole commune (transparence, post-Schecke)

Avis du 9 octobre 2012 concernant la modification de la proposition COM(2011) 628 final/2 présentée par la Commission relative à un règlement du Parlement européen et du Conseil relatif au financement, à la gestion et au suivi de la politique agricole commune

Services de confiance pour les transactions électroniques

Avis du 27 septembre 2012 sur la proposition de la Commission pour un règlement du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (règlement sur les services de confiance électroniques)

Création du système «EURODAC» pour la comparaison des empreintes digitales

Avis du 5 septembre 2012 du Contrôleur européen de la protection des données sur la proposition modifiée de règlement du Parlement européen et du Conseil relatif à la création du système «EURODAC» pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) n° […/…]

Détachement de travailleurs effectué dans le cadre d'une prestation de services

Avis du 19 juillet 2012 sur la proposition de la Commission de directive du Parlement européen et du Conseil relative à l'exécution de la directive 96/71/CE concernant le détachement de travailleurs effectué dans le cadre d'une prestation de services et la proposition de la Commission de règlement du Conseil relatif à l'exercice du droit de mener des actions collectives dans le contexte de la liberté d'établissement et de la libre prestation des services

Stratégie européenne pour un internet mieux adapté aux enfants

Avis du 17 juillet 2012 sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – «Stratégie européenne pour un internet mieux adapté aux enfants»

Amélioration du règlement des opérations sur titres dans l'Union européenne

Avis du 9 juillet 2012 sur la proposition de règlement du Parlement européen et du Conseil concernant l'amélioration du règlement des opérations

sur titres dans l'Union européenne et les dépositaires centraux de titres (DCT) et modifiant la directive 98/26/CE

Système d'information Schengen de deuxième génération (SIS II)

Avis du 9 juillet 2012 sur la proposition de règlement du Conseil relatif à la migration du système d'information Schengen (SIS) vers le système d'information Schengen de deuxième génération (SIS II) (refonte)

Simplification du transfert des véhicules à moteur immatriculés dans un autre État membre à l'intérieur du marché unique

Avis du 9 juillet 2012 sur la proposition de règlement du Parlement européen et du Conseil relatif à la simplification du transfert des véhicules à moteur immatriculés dans un autre État membre à l'intérieur du marché unique

Centre européen de lutte contre la cybercriminalité

Avis du 29 juin 2012 relatif à la communication de la Commission européenne au Conseil et au Parlement européen concernant l'établissement d'un Centre européen de lutte contre la cybercriminalité

Fonds européens de capital-risque

Avis du 14 juin 2012 relatif à la proposition de règlement sur les fonds européens de capital-risque et à la proposition de règlement sur les fonds d'entrepreneuriat social européens.

Systèmes intelligents de mesure

Avis du 8 juin 2012 sur la recommandation de la Commission relative à la préparation de l'introduction des systèmes intelligents de mesure

Registre de l'Union pour la période d'échanges débutant le 1er janvier 2013

Avis du 11 mai 2012 sur le règlement de la Commission établissant le registre de l'Union pour la période d'échanges débutant le 1er janvier 2013 et pour les périodes d'échanges suivantes du système d'échanges de quotas d'émission de l'Union

Accord commercial anti-contrefaçon (ACAC)

Avis du 24 avril 2012 sur la proposition de décision du Conseil relative à la conclusion de l'Accord commercial anti-contrefaçon entre l'Union européenne et ses États membres, l'Australie, le Canada, le Japon, la République de Corée, les États-Unis du Mexique, le Royaume du Maroc, la Nouvelle-Zélande, la République de Singapour, la Confédération suisse et les États-Unis d'Amérique

Paquet «Ouverture des données»

Avis du 18 avril 2012 sur le paquet de mesures de la Commission européenne relatif à l'ouverture des données, qui comprend une proposition de directive modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public (ISP)

Contrôle légal des comptes

Avis du 13 avril 2012 Sur la proposition de la Commission concernant une directive modifiant la directive 2006/43/CE concernant le contrôle légal des comptes annuels et des comptes consolidés, et sur la proposition de règlement relatif aux exigences spécifiques applicables au contrôle légal des comptes des entités d'intérêt public

Accord de coopération douanière UE-Canada sur la sécurité de la chaîne d'approvisionnement

Avis du 13 avril 2012 sur la proposition de décision du Conseil relative à la conclusion de l'accord de coopération douanière entre l'Union européenne et le Canada en ce qui concerne les questions liées à la sécurité de la chaîne d'approvisionnement

Menaces transfrontalières pour la santé

Avis du 28 mars 2012 sur la proposition de décision du Parlement européen et du Conseil relative aux menaces transfrontalières graves pour la santé

Révision de la directive sur les qualifications professionnelles

Avis du 8 mars 2012 sur la proposition de la Commission de directive du Parlement européen et du Conseil modifiant la directive 2005/36/CE relative à la reconnaissance des qualifications professionnelles et le règlement […] concernant la coopération administrative par l'intermédiaire du système d'information du marché intérieur

Paquet de mesures pour une réforme de la protection des données

Avis du 7 mars 2012 sur le paquet de mesures pour une réforme de la protection des données

Permis de conduire qui intègrent les fonctionnalités d'une carte de conducteur

Avis du 17 février 2012 sur la proposition de directive du Parlement européen et du Conseil modifiant la directive 2006/126/CE du Parlement européen et du Conseil en ce qui concerne les permis

de conduire qui intègrent les fonctionnalités d'une carte de conducteur

Agences de notation de crédit

Avis du 10 février 2012 sur la proposition de la Commission de règlement du Parlement européen et du Conseil modifiant le règlement (CE) n o 1060/2009 sur les agences de notation de crédit

Opérations d'initiés et manipulations de marché

Avis du 10 février 2012 sur les propositions de la Commission de règlement du Parlement européen et du Conseil sur les opérations d'initiés et les manipulations de marché, et de directive du Parlement européen et du Conseil relative aux sanctions pénales applicables aux opérations d'initiés et aux manipulations de marché

Marchés d'instruments financiers

Avis du 10 février 2012 sur les propositions de la Commission relatives à une directive du Parlement européen et du Conseil concernant les marchés d'instruments financiers abrogeant la directive 2004/39/CE du Parlement européen et du Conseil et à un règlement du Parlement européen et du Conseil concernant les marchés d'instruments financiers modifiant le règlement sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux

Accès à l'activité des établissements de crédit

Avis du 10 février 2012 sur les propositions de la Commission concernant une directive concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, et un règlement concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement

UE-États-Unis mixte de coopération douanière

Avis du 9 février 2012 sur la Proposition de décision du Conseil sur la proposition de décision du Conseil relative à une position à prendre par l'Union au sein du comité mixte de coopération douanière Union européenne-États-Unis concernant la reconnaissance mutuelle du programme relatif aux opérateurs économiques agréés de l'Union européenne et du programme de partenariat douane-commerce contre le terrorisme des États-Unis

Coopération administrative dans le domaine des droits d'accise

Avis du 27 janvier 2012 sur la proposition de règlement du Conseil relatif à la coopération administrative dans le domaine des droits d'accise

Règlement extrajudiciaire et règlement en ligne des litiges de consommation

Avis du 12 janvier 2012 sur les propositions législatives relatives au règlement extrajudiciaire et au règlement en ligne des litiges de consommation

Observations formelles sur des propositions législatives

Service d'appel d'urgence (eCall) interopérable dans toute l'UE

Lettre du 19 décembre 2012 sur le règlement délégué de la Commission complétant la directive 2010/40/UE du Parlement européen et du Conseil en ce qui concerne la mise à disposition harmonisée d'un service d'appel d'urgence (eCall) interopérable dans toute l'UE (C(2012)8509 final)

Consultation sur l'autorégulation

Lettre du 19 décembre 2012 relative à la consultation publique lancée par la Commission sur l'autorégulation

Code de conduite pour les archives

Lettre du 3 décembre 2012 adressée à Mme Day, Secrétaire générale de la Commission européenne, relative au projet du Bureau européen des archivistes nationaux (EBNA) et du Groupe européen d'archives (EAG) visant à élaborer un code de conduite pour le secteur des archives, afin d'encadrer l'application des exigences en matière de protection des données, en tenant compte des spécificités du secteur

Protection des données à caractère personnel en Nouvelle-Zélande

Lettre du 9 novembre 2012 à Mme Françoise Le Bail, Directeur général de la DG Justice, concernant le projet de décision d'exécution de la Commission constatant le niveau de protection adéquat des données à caractère personnel en Nouvelle-Zélande conformément à la directive 95/46/CE

Internet ouvert

Observations du CEPD du 15 octobre 2012 sur la consultation publique de la DG Connect sur des aspects spécifiques de la transparence, de la gestion du trafic et des changements de fournisseurs dans le cadre de l'internet ouvert

Amélioration de la sécurité des réseaux et de l'information (SRI) dans l'UE

Observations du CEPD du 10 octobre 2012 sur la consultation publique de la DG Connect concernant l'amélioration de la sécurité des réseaux et de l'information (SRI) dans l'UE

Gestion collective des droits d'auteur

Lettre du 9 octobre 2012 à M. Michel BARNIER, commissaire chargé du marché intérieur et des services, concernant la proposition de directive relative à la gestion collective des droits d'auteur

Contenus illégaux hébergés par des intermédiaires en ligne

Observations du CEPD du 13 septembre 2012 sur la consultation publique de la DG MARKT sur les procédures de notification des contenus illégaux hébergés par des intermédiaires en ligne

Agenda du consommateur européen - Favoriser la confiance et la croissance

Observations du CEPD du 16 juillet 2012 sur la communication de la Commission - Un agenda du consommateur européen - Favoriser la confiance et la croissance

Stratégie de l'UE en vue de l'éradication de la traite des êtres humains pour la période 2012-2016

Observations du CEPD du 10 juillet 2012 concernant la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – «La stratégie de l'UE en vue de l'éradication de la traite des êtres humains pour la période 2012-2016»

Proposition de directive concernant le gel et la confiscation des produits du crime

Lettre du 18 juin 2012 à Mme Cecilia Malmström, Commissaire en charge des affaires intérieures, concernant le gel et la confiscation des produits du crime au sein de l'Union européenne

Commission spéciale de la criminalité organisée, de la corruption et du blanchiment de capitaux (CRIM)

Lettre du 7 juin 2012 à Mme Sonia Alfano, députée européenne, concernant l'implication du CEPD dans la commission spéciale de la criminalité organisée, de la corruption et du blanchiment de capitaux (CRIM)

Marché européen des paiements par carte, par internet et par téléphone mobile

Lettre du 11 avril 2012 concernant le Livre Vert: «Vers un marché européen intégré des paiements par carte, par internet et par téléphone mobile»

Système Européen de Surveillance des Frontières (EUROSUR)

Commentaires du CEDP du 8 février 2012 sur la proposition de la Commission pour établir un Système Européen de Surveillance des Frontières (EUROSUR)

Responsabilité d'entreprise

Lettre du 10 janvier 2012, sur dossier «responsabilité d'entreprise» adopté par la Commission le 25 octobre 2011

Annexe G — Discours du contrôleur et du contrôleur adjoint en 2012

En 2012, le contrôleur et le contrôleur adjoint ont continué de consacrer beaucoup de temps et d'efforts à l'explication de leur mission et à la sensibilisation à la protection des données en général. Ils ont également abordé un certain nombre de questions particulières dans des discours prononcés lors de différentes manifestations organisées dans les institutions de l'Union européenne, dans les États membres et au-delà.

Parlement européen

8 février	Contrôleur, Conférence du groupe S&D, amélioration de la gouvernance de Schengen (Bruxelles) (*)
6 mars	Contrôleur, Conférence sur les discriminations génétiques (Bruxelles)
15 mars	Contrôleur, Conférence sur le droit administratif de l'Union européenne (Bruxelles)
27 mars	Contrôleur, Fondation européenne de l'internet, informatique dématérialisée (Bruxelles)
28 mars	Contrôleur, Plate-forme de la vie privée, proposition de règlement relatif à la protection des données (Bruxelles)
25 avril	Contrôleur adjoint, commission IMCO, croissance et mobilité (Bruxelles) (*)
26 avril	Contrôleur adjoint, commission LIBE, ACAC (Bruxelles)*
16 mai	Contrôleur adjoint, commission LIBE, atelier sur l'ACAC (Bruxelles) (*)
29 mai	Contrôleur, atelier de LIBE sur la proposition de règlement relatif à la protection des données (Bruxelles)
20 juin	Contrôleur et Contrôleur adjoint, commission LIBE, rapport annuel 2011 (Bruxelles)
26 juin	Contrôleur, Conférence du groupe Verts, émergence de la «forteresse électronique Europe» (Bruxelles)
28 juin	Contrôleur, Groupe Verts/ALE, audition relative à la réforme de la protection des données (Bruxelles) (*)
10 octobre	Contrôleur, audition interparlementaire relative à la réforme de la protection des données (Bruxelles) (*)
11 octobre	Contrôleur, Commission LIBE, règlement EURODAC (Bruxelles) (*)

Conseil

24 janvier	Contrôleur, Représentation permanente de la Pologne, Journée de la protection des données (Bruxelles)
2 février	Contrôleur, Conférence «One Europe – One Market» de la Présidence danoise (Copenhague) (*)
14 mars	Contrôleur, Groupe de travail sur la protection des données et l'échange d'informations (Bruxelles)
4 octobre	Contrôleur, Conférence internationale sur le cyberespace (Budapest)

Commission européenne

25 janvier	Contrôleur et Contrôleur adjoint, DPD et CPD, Journée de la protection des données (Bruxelles)
19 mars	Contrôleur, Conférence de l'UE sur la vie privée et la protection des données (Washington DC) (*)
30 mai	Contrôleur, Groupe européen d'archives, réforme de la protection des données (Copenhague)
21 juin	Contrôleur, Assemblée numérique, réforme de la protection des données (Bruxelles)
24 septembre	Contrôleur, Séminaire du coordinateur de l'UE pour la lutte contre la traite des êtres humains (Bruxelles)

Autres institutions et organes de l'Union européenne

10 mai	Contrôleur, Agence des droits fondamentaux, réforme de la protection des données (Vienne) (*)

16 mai	Contrôleur adjoint, séminaire de l'ERA sur le centre de lutte contre la cybercriminalité d'Europol (Bruxelles) (*)
20 septembre	Contrôleur et contrôleur adjoint, Conférence de l'ERA sur le nouveau règlement relatif à la protection des données (Trèves)
19 octobre	Contrôleur adjoint, Directeurs d'agences (Stockholm) (*)
5 novembre	Contrôleur et contrôleur adjoint, Conférence de l'ERA sur la nouvelle directive relative à la protection des données (Trèves)
8 novembre	Contrôleur et Contrôleur adjoint, Atelier sur les organisations internationales (Bruxelles)

Conférences internationales

27 janvier	Contrôleur, Conférence Ordinateurs, vie privée et protection des données (Bruxelles)
9 mars	Contrôleur, Sommet mondial sur la vie privée de l'IAPP (Bruxelles)
3 mai	Contrôleur et contrôleur adjoint, Autorités européennes chargées de la protection des données (Bruxelles)
7 mai	Contrôleur, Journée européenne de la protection des données (Berlin)
9 octobre	Contrôleur, Conférence d'Amsterdam sur la vie privée (Amsterdam)
22 octobre	Contrôleur, Conférence Public Voice (Punta del Este, Uruguay)
23 octobre	Contrôleur et contrôleur adjoint, Commissaires à la vie privée et à la protection des données (Punta del Este, Uruguay)
15 novembre	Contrôleur, Congrès d'IAPP Europe sur la protection des données (Bruxelles)
3 décembre	Contrôleur, Conférence KnowledgeNet d'IAPP Europe (Bruxelles)
4 décembre	Contrôleur, Conférence Protection des données et vie privée (Bruxelles) (*)

Autres événements

18 janvier	Contrôleur, 5ème Conférence annuelle sur le traitement de données à caractère personnel (Paris) (*)
20 janvier	Contrôleur, Chambre du commerce américaine, l'économie numérique (Bruxelles)
26 janvier	Contrôleur, Académie européenne, réforme de la protection des données (Berlin)
17 février	Contrôleur, European Biometrics Association (Bruxelles)
22 février	Contrôleur, Atelier sur la responsabilité (Bruxelles)
24 février	Contrôleur, Conférence sur les défis émergents dans le droit du respect de la vie privée (Melbourne) (* et **)
5 mars	Contrôleur, Plate-forme des affaires européennes (Bruxelles)
8 mars	Contrôleur, e-Forum de Westminster, réforme de la protection des données (Londres)
15 mars	Contrôleur, Forum sur les règles d'entreprise contraignantes (Amsterdam)
20 mars	Contrôleur, C-PET, réforme de la protection des données (Washington DC)
21 mars	Contrôleur adjoint, atelier sur l'informatique dématérialisée (Bruxelles)
26 mars	Contrôleur, European Voice, réforme de la protection des données (Bruxelles)
27 mars	Contrôleur, Chambre du commerce américaine en France (Paris) *
29 mars	Contrôleur, Association néerlandaise pour le respect de la vie privée (Utrecht)
12 avril	Contrôleur, Tech America, réforme de la protection des données (Bruxelles)

16 avril	Contrôleur, Atelier sur les institutions nationales de défense des droits de l'homme (Louvain)
20 avril	Contrôleur et Contrôleur adjoint, Séminaire sur le respect de la vie privée (Cambridge)
24 avril	Contrôleur, Forum UE/États-Unis sur le droit économique (Bruxelles)
26 avril	Contrôleur, Berkeley Law Forum (Palo Alto, États-Unis) (*)
27 avril	Contrôleur, Forum sur l'avenir du respect de la vie privée (Mountain View, États-Unis)
22 mai	Contrôleur, Forum sur le droit de la vie privée (Francfort)
31 mai	Contrôleur, Atelier sur la responsabilité (Bruxelles)
6 juin	Contrôleur, Forum ISMS, réforme de la protection des données (Bruxelles)
8 juin	Contrôleur, Digital Europe, réforme de la protection des données (Bruxelles)
8 juin	Contrôleur adjoint, Columbia Institute for Tele-Information (New York) (*)
11 juin	Contrôleur, Sommet Reuters, réforme de la protection des données (Londres)
12 juin	Contrôleur, Protection des données et liberté de l'information (Oxford) (*)
15 juin	Contrôleur, Conférence sur le droit de la protection des données (Fribourg)
18 juin	Contrôleur, DuD 2012 , réforme de la protection des données (Berlin) (*)
19 juin	Contrôleur, E-Forum numérique, réforme de la protection des données (Luxembourg)
20 juin	Contrôleur, Eurosmart, réforme de la protection des données (Bruxelles)
21 juin	Contrôleur, Time.Lex (Bruxelles)
21 juin	Contrôleur adjoint, Am Cham Italy et mission des États-Unis (Rome)
25 juin	Contrôleur, Conseil économique, réforme de la protection des données (Bruxelles)
26 juin	Contrôleur, Cabinet DN, réforme de la protection des données (Bruxelles)
27 juin	Contrôleur, Biometrics Institute (Londres)
12 juillet	Contrôleur, Microsoft, réforme de la protection des données (Bruxelles)
12 septembre	Contrôleur, Freedom - Not Fear (Bruxelles)
19 septembre	Contrôleur, World Smart Week, réforme de la protection des données (Nice)
3 octobre	Contrôleur, CEPS, contrôle électronique (Bruxelles)
16 octobre	Contrôleur, Séminaire GSMA-ETNO sur la vie privée en ligne (Bruxelles) (*)
7 novembre	Contrôleur, Swiss Re, protection des données au niveau mondial (Zurich)
13 novembre	Contrôleur, L'internet des objets Europe (Bruxelles)
14 novembre	Contrôleur, Commerce électronique en Europe (Bruxelles)
26 novembre	Contrôleur, ECTA, réforme de la protection des données (Bruxelles)
28 novembre	Contrôleur, Eurocommerce, réforme de la protection des données (Bruxelles)
30 novembre	Contrôleur, Conseil européen des ordres des médecins (Bruxelles)

(*) Texte disponible sur le site internet du CEPD

(**) Vidéo disponible sur le site internet du CEPD

Annexe H — Composition du secrétariat du CEPD

Directeur, chef du Secrétariat

Christopher DOCKSEY

• Supervision et mise en application

Sophie LOUVEAUX *Chef d'unité faisant fonction*	Pierre VERNHES (*) *Conseiller juridique*
Jaroslaw LOTARSKI (*) *Responsable réclamations*	Maria Verónica PEREZ ASINARI *Responsable consultations administratives*
Delphine HAROU *Responsable contrôles préalables*	Athena BOURKA (*) *Expert national détaché*
Raffaele DI GIOVANNI BEZZI *Juriste*	Elisabeth DUHR (*) *Expert national détaché*
Daniela GUADAGNO *Juriste / Expert national détaché*	Ute KALLENBERGER *Juriste*
Xanthi KAPSOSIDERI *Juriste*	Luisa PALLA *Assistante supervision et mise en application*
Antje PRISKER *Juriste*	Dario ROSSI *Assistant supervision et mise en application* *Correspondant comptabilité* *Vérificateur financier ex-post*
Tereza STRUNCOVA *Juriste*	Michaël VANFLETEREN *Juriste*

• Politique législative et consultation

Hielke HIJMANS *Chef d'unité*	Herke KRANENBORG *Responsable contentieux et politique législative*
Anne-Christine LACOSTE *Responsable coopération internationale et politique législative*	Zsuzsanna BELENYESSY *Juriste*
Gabriel Cristian BLAJ *Juriste*	Alba BOSCH MOLINE *Juriste*
Isabelle CHATELIER *Juriste*	Katarzyna CUADRAT-GRZYBOWSKA (*) *Juriste*
Priscilla DE LOCHT *Juriste*	Amanda JOYCE *Assistante politique et consultation*
Elise LATIFY *Juriste*	Per JOHANSSON *Juriste*
Owe LANGFELDT (*) *Juriste / intérimaire*	Vera POZZATO *Juriste*
Galina SAMARAS *Assistante politique et consultation*	

• Politique IT

Achim KLABUNDE *Chef de secteur*	Massimo ATTORESI *Conseiller technologie et sécurité*
Andy GOLDSTEIN *Conseiller technologie et sécurité*	Bart DE SCHUITENEER *Conseiller technologie RLSI*
Luis VELASCO (*) Conseiller technologie	

• Opérations, planning et assistance

Andrea BEACH *Chef de secteur*	Marta CORDOBA-HERNANDEZ *Assistante administrative*
Kim DAUPHIN *Assistante administrative / intérimaire*	Milan KUTRA *Assistant administratif*
Kim Thien LÊ *Assistante administrative*	Ewa THOMSON *Assistante administrative*

• Information et communication

Olivier ROSSIGNOL *Chef de secteur*	Parminder MUDHAR *Conseiller information et communication*
Agnieszka NYKA *Conseiller information et communication*	Benoît PIRONET *Développeur web*

• Ressources humaines, budget et administration

Leonardo CERVERA NAVAS *Chef d'unité*	Maria SANCHEZ LOPEZ *Responsable finances*
Pascale BEECKMANS *Finance Assistant* *GEMI*	Laetitia BOUAZZA-ALVAREZ *Assistante administrative*
Isabelle DELATTRE (*) *Assistante finances et comptabilité*	Anne LEVÊCQUE *Assistante ressources humaines GECO*
Vittorio MASTROJENI *Conseiller ressources humaines*	Julia MALDONADO MOLERO (*) *Assistante administrative / intérimaire*
Daniela OTTAVI *Conseiller finances et passation de marchés*	Aida PASCU *Assistante administrative* *RLS*
Sylvie PICARD *Déléguée à la protection des données* *CCI*	Anne-Françoise REYNDERS *Assistante ressources humaines* *& coordinatrice formation*

(*) Membres du personnel ayant quitté le CEPD dans le courant de l'année 2012

Contrôleur européen de la protection des données

Rapport annuel 2012

Luxembourg: Office des publications de l'Union européenne

2013 — 125 pp. — 21 × 29.7 cm

ISBN 978-92-95076-78-5
doi:10.2804/52280

COMMENT VOUS PROCURER LES PUBLICATIONS DE L'UNION EUROPÉENNE?

Publications gratuites:

- un seul exemplaire: sur le site EU Bookshop (http://bookshop.europa.eu);
- exemplaires multiples/posters/cartes:
  auprès des représentations de l'Union européenne (http://ec.europa.eu/represent_fr.htm),
  des délégations dans les pays hors UE (http://eeas.europa.eu/delegations/index_fr.htm),
  en contactant le réseau Europe Direct (http://europa.eu/europedirect/index_fr.htm)
  ou le numéro 00 800 6 7 8 9 10 11 (gratuit dans toute l'UE) (*).

  (*) Les informations sont fournies à titre gracieux et les appels sont généralement gratuits (sauf certains opérateurs, hôtels ou cabines téléphoniques).

Publications payantes:

- sur le site EU Bookshop (http://bookshop.europa.eu).

Abonnements:

- auprès des bureaux de vente de l'Office des publications de l'Union européenne (http://publications.europa.eu/others/agents/index_en.htm).

QT-AA-13-001-FR-C

LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

Le gardien européen de la protection des données personnelles

www.edps.europa.eu

@EU_EDPS

Office des publications

ISBN 978-92-95076-79-2