

Rapport annuel

2011

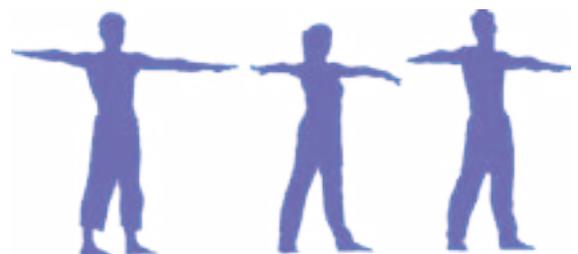


LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES



Rapport annuel

2011



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

Un numéro unique gratuit (*):

00 800 6 7 8 9 10 11

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

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

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

Luxembourg: Office des publications de l'Union européenne, 2012

ISBN 978-92-95073-29-6

doi:10.2804/36295

© Union européenne, 2012

Reproduction autorisée, moyennant mention de la source

© Photos: Parlement européen et iStockphoto

Printed in Luxembourg

IMPRIME SUR PAPIER BLANCHI SANS CHLORE ELEMENTAIRE (ECF)

Sommaire

| | |
|------------------------|----|
| Guide de l'utilisateur | 7 |
| Mandat du CEPD | 9 |
| Avant-propos | 11 |

1 FAITS MARQUANTS DE 2011

| | |
|------------------------------------|-----------|
| 1. FAITS MARQUANTS DE 2011 | 12 |
| 1.1. Aperçu général de 2011 | 12 |
| 1.2. Résultats en 2011 | 16 |

2 SUPERVISION ET MISE EN APPLICATION

| | |
|--|-----------|
| 2. SUPERVISION ET MISE EN APPLICATION | 18 |
| 2.1. Introduction | 18 |
| 2.2. Délégués à la protection des données | 18 |
| 2.3. Contrôles préalables | 20 |
| 2.3.1. Base juridique | 20 |
| 2.3.2. Procédure | 20 |
| 2.3.3. Principales questions liées aux contrôles préalables | 22 |
| 2.3.4. Consultations concernant la nécessité d'un contrôle préalable | 27 |
| 2.3.5. Notifications non soumises au contrôle préalable ou retirées | 27 |
| 2.3.6. Suivi des avis de contrôle préalable | 27 |
| 2.3.7. Conclusions | 28 |
| 2.4. Réclamations | 28 |
| 2.4.1. Les fonctions du CEPD | 28 |
| 2.4.2. Procédure de traitement des réclamations | 29 |
| 2.4.3. Confidentialité garantie aux plaignants | 31 |
| 2.4.4. Réclamations traitées en 2011 | 32 |
| 2.5. Contrôle du respect du règlement | 35 |
| 2.5.1. Exercice général de contrôle et d'établissement de rapports: enquête 2011 | 35 |
| 2.5.2. Contrôles ciblés | 36 |
| 2.5.3. Inspections | 37 |
| 2.6. Consultations relatives aux mesures administratives | 38 |
| 2.6.1. Consultations selon l'article 28, paragraphe 1, et l'article 46, point d) | 38 |
| 2.7. Orientations en matière de protection des données | 42 |
| 2.7.1. Lignes directrices thématiques | 42 |
| 2.7.2. Formation | 44 |

3 POLITIQUE LÉGISLATIVE ET CONSULTATION

| | |
|--|-----------|
| 3. POLITIQUE LÉGISLATIVE ET CONSULTATION | 46 |
| 3.1. Introduction: vue d'ensemble de l'année et tendances principales | 46 |
| 3.2. Cadre d'action et priorités | 47 |
| 3.2.1. Mise en œuvre de la politique de consultation | 47 |
| 3.2.2. Résultats en 2011 | 48 |
| 3.3. Révision du cadre européen en matière de protection des données | 49 |
| 3.3.1. Une approche globale de la protection des données à caractère personnel dans l'Union européenne | 49 |
| 3.4. Espace de liberté, de sécurité et de justice et coopération internationale | 50 |
| 3.4.1. Conservation des données | 50 |
| 3.4.2. Système européen de surveillance du financement du terrorisme (SSFT) | 52 |
| 3.4.3. Système européen de données des dossiers passagers | 52 |
| 3.4.4. Accord entre l'UE et l'Australie sur les données des dossiers passagers | 52 |
| 3.4.5. Accord entre l'UE et les États-Unis concernant les données des dossiers passagers | 53 |
| 3.4.6. Paquet anticorruption | 54 |
| 3.4.7. Propositions législatives concernant certaines mesures restrictives | 54 |
| 3.4.8. Migration | 54 |
| 3.4.9. Victimes de la criminalité | 55 |

| | |
|--|-----------|
| 3.5. Stratégie numérique et technologie | 55 |
| 3.5.1. Neutralité de l'internet | 55 |
| 3.5.2. Projet technologique «Turbine» | 56 |
| 3.6. Marché intérieur y compris données financières | 56 |
| 3.6.1. Système d'information du marché intérieur | 56 |
| 3.6.2. Intégrité et transparence du marché de l'énergie | 57 |
| 3.6.3. Interconnexion des registres du commerce | 58 |
| 3.6.4. Contrats de crédit relatifs aux biens immobiliers à usage résidentiel | 58 |
| 3.6.5. Produits dérivés négociés de gré à gré, contreparties centrales et référentiels centraux | 58 |
| 3.6.6. Exigences techniques pour les virements et les prélèvements en euros | 59 |
| 3.6.7. Scanners corporels dans les aéroports | 60 |
| 3.7. Application transfrontalière de la loi | 60 |
| 3.7.1. Directive relative à l'application des droits de propriété intellectuelle | 60 |
| 3.7.2. Contrôle par les autorités douanières du respect des droits de propriété intellectuelle | 61 |
| 3.7.3. Compétence judiciaire, reconnaissance et exécution des décisions en matière civile et commerciale | 61 |
| 3.7.4. Ordonnance européenne de saisie conservatoire des comptes bancaires | 62 |
| 3.8. Santé publique et consommateurs | 62 |
| 3.8.1. Système de coopération en matière de protection des consommateurs | 62 |
| 3.9. Questions diverses | 63 |
| 3.9.1. Règlement portant réforme de l'OLAF | 63 |
| 3.9.2. Règlement financier de l'UE | 63 |
| 3.9.3. Statistiques européennes de la sécurité face à la criminalité | 63 |
| 3.9.4. Transport | 64 |
| 3.9.5. Politique agricole commune après 2013 | 65 |
| 3.9.6. Contrôle destiné à garantir le respect de la politique de la pêche | 65 |
| 3.10. Accès du public aux documents contenant des données à caractère personnel | 66 |
| 3.11. Affaires judiciaires | 67 |
| 3.11.1. Participation du CEPD à des procédures judiciaires | 67 |
| 3.11.2. Jurisprudence en matière de protection des données | 68 |
| 3.12. Développements technologiques futurs | 68 |
| 3.13. Priorités pour 2012 | 70 |



| | |
|---|-----------|
| 4. COOPÉRATION | 72 |
| 4.1. Groupe de travail «Article 29» | 72 |
| 4.2. Supervision conjointe d'Eurodac | 74 |
| 4.2.1. Rapport sur la suppression préalable des données | 74 |
| 4.2.2. Nouvel exercice pour 2012: empreintes digitales illisibles | 74 |
| 4.2.3. Questionnaire de l'audit de sécurité coordonné | 75 |
| 4.2.4. Système d'information sur les visas | 75 |
| 4.3. Supervision du système d'information douanier (SID) | 75 |
| 4.4. Coopération policière et judiciaire: coopération avec les autorités de contrôle communes et le GTPJ | 76 |
| 4.5. Conférence européenne | 77 |
| 4.6. Conférence internationale | 77 |



| | |
|--|-----------|
| 5. INFORMATION ET COMMUNICATION | 78 |
| 5.1. Introduction | 78 |
| 5.2. Caractéristiques de la communication | 78 |
| 5.2.1. Principaux publics et groupes cibles | 78 |
| 5.2.2. Politique linguistique | 79 |
| 5.3. Relations avec les médias | 79 |
| 5.3.1. Communiqués de presse | 79 |
| 5.3.2. Interviews | 79 |
| 5.3.3. Conférence de presse | 80 |
| 5.3.4. Demandes formulées par les médias | 80 |
| 5.4. Demandes d'informations et de conseils | 81 |
| 5.5. Visites d'étude | 82 |
| 5.6. Outils d'information en ligne | 83 |
| 5.6.1. Site internet | 83 |
| 5.6.2. Newsletter | 83 |

| | |
|--|-----------|
| 5.7. Publications | 83 |
| 5.7.1. Rapport annuel | 83 |
| 5.7.2. Publications thématiques | 84 |
| 5.8. Actions de sensibilisation | 84 |
| 5.8.1. Journée de la protection des données 2011 | 84 |
| 5.8.2. Journée portes ouvertes de l'UE 2011 | 85 |

6 ADMINISTRATION, BUDGET ET PERSONNEL

| | |
|---|-----------|
| 6. ADMINISTRATION, BUDGET ET PERSONNEL | 88 |
| 6.1. Introduction | 88 |
| 6.2. Budget | 88 |
| 6.3. Ressources humaines | 89 |
| 6.3.1. Recrutement | 89 |
| 6.3.2. Programme de stages | 91 |
| 6.3.3. Programme pour les experts nationaux détachés | 91 |
| 6.3.4. Organigramme | 91 |
| 6.3.5. Conditions de travail | 91 |
| 6.3.6. Formation | 92 |
| 6.3.7. Activités sociales | 92 |
| 6.4. Fonctions de contrôle | 92 |
| 6.4.1. Contrôle interne | 92 |
| 6.4.2. Audit interne | 93 |
| 6.4.3. Audit externe | 93 |
| 6.4.4. Sécurité | 93 |
| 6.5. Infrastructure | 94 |
| 6.6. Environnement administratif | 94 |
| 6.6.1. Assistance administrative et coopération interinstitutionnelle | 94 |
| 6.6.2. Règlement intérieur | 94 |
| 6.6.3. Gestion des documents | 95 |
| 6.6.4. Planification | 95 |

7 DÉLÉGUÉ À LA PROTECTION DES DONNÉES DU CEPD

| | |
|--|-----------|
| 7. DÉLÉGUÉ À LA PROTECTION DES DONNÉES DU CEPD | 96 |
| 7.1. Le DPD du CEPD | 96 |
| 7.2. Le registre des traitements | 96 |
| 7.3. Enquête 2011 du CEPD | 97 |
| 7.4. Information et sensibilisation | 97 |

8 PRINCIPAUX OBJECTIFS POUR 2012

| | |
|---|------------|
| 8. PRINCIPAUX OBJECTIFS POUR 2012 | 98 |
| 8.1. Supervision et mise en application | 98 |
| 8.2. Politique législative et consultation | 99 |
| 8.3. Coopération | 100 |
| 8.4. Autres domaines | 100 |

| | |
|---|-----|
| Annexe A — Cadre juridique | 101 |
| Annexe B — Extrait du règlement (CE) n° 45/2001 | 104 |
| Annexe C — Liste des abréviations | 106 |
| Annexe D — Liste des délégués à la protection des données | 108 |
| Annexe E — Liste des avis rendus à la suite d'un contrôle préalable | 111 |
| Annexe F — Liste des avis et observations formelles sur des propositions législatives | 117 |
| Annexe G — Discours du contrôleur et du contrôleur adjoint en 2011 | 121 |
| Annexe H — Composition du secrétariat du CEPD | 124 |

GUIDE DE L'UTILISATEUR

Le lecteur trouvera, immédiatement après ce guide, l'avant-propos du rapport annuel 2011, rédigé par M. Peter Hustinx, contrôleur européen de la protection des données (CEPD) et M. Giovanni Buttarelli, contrôleur adjoint, précédé de l'énoncé de leur mission.

Le chapitre 1, «Faits marquants de 2011», présente les grands axes des activités du CEPD en 2011 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 2011. Il présente également les lignes directrices thématiques adoptées par le CEPD dans le domaine des procédures anti-harcèlement et de l'évaluation du personnel, ainsi que le rapport de suivi sur la vidéosurveillance.

Le chapitre 3, «Consultation», traite de l'évolution du rôle consultatif du CEPD. 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. 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 le travail effectué 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 conjointe (par le CEPD et par les autorités nationales chargées de la protection des données) des systèmes d'information à grande échelle.

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

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

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

Le chapitre 8, «Principaux objectifs pour 2012», donne un aperçu des priorités principales pour l'année 2012.

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 et avis consultatifs relatifs aux contrôles préalables du CEPD, les discours prononcés par le contrôleur et son adjoint, et la composition du secrétariat du CEPD.

Un résumé de ce rapport est également disponible, avec une vue d'ensemble synthétique des développements principaux intervenus en 2011 dans le cadre des activités du CEPD.

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.

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

MANDAT DU CEPD

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

Le CEPD est chargé de:

- superviser et d'assurer le respect des dispositions du règlement (CE) n° 45/2001¹ et des autres actes communautaires relatifs à la protection des droits fondamentaux et des libertés lorsque les institutions et organes de l'UE traitent des données à caractère personnel (contrôle);
- conseiller les institutions et les organes de l'UE pour toutes les questions concernant le traitement de données à caractère personnel, ce qui inclut la consultation dans le cadre de l'élaboration de dispositions législatives et le suivi des nouveaux développements ayant une incidence sur la protection des données à caractère personnel (consultation);
- coopérer avec les autorités nationales de supervision et avec les organes de supervision relevant de l'ancien troisième pilier de l'UE, en vue d'améliorer la cohérence en matière de protection des données à caractère personnel (coopération).

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

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

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

AVANT- PROPOS



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

Le présent rapport concerne l'année 2011, septième année complète d'activité du CEPD en tant que nouvelle 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 troisième année de notre mandat commun en tant que membres de cette autorité.

Au cours de l'année 2011, nous avons 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 de mise en 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 consultation sur de nouvelles mesures législatives, le CEPD a rendu un nombre record d'avis sur différents sujets, le plus important étant le réexamen du cadre juridique de l'UE en matière de protection des données, qui figure parmi nos priorités. Cependant, la mise en œuvre du programme de Stockholm dans l'espace de liberté, de sécurité et de justice et la stratégie numérique, en tant que pierre angulaire de la stratégie «Europe 2020», ont eu des répercussions sur la protection des données. Il en va de même pour les questions concernant le marché intérieur, la santé publique et les consommateurs, ainsi que l'application transfrontalière de la loi.

Dans le même temps, nous avons renforcé notre coopération avec d'autres autorités de surveillance et encore amélioré l'efficacité et l'efficience de notre organisation.

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 2011

1.1. Aperçu général de 2011

Les principales activités du CEPD en 2011 se sont appuyées sur la même stratégie d'ensemble que précédemment, mais leur importance et les domaines couverts ont continué de se développer. L'aptitude du CEPD à agir efficacement s'est également améliorée.

Le cadre juridique² dans lequel le CEPD opère définit un certain nombre de tâches et de compétences qui permettent de distinguer trois fonctions principales. Ces fonctions continuent de faire office de cadre stratégique pour les activités du CEPD et sont présentées dans l'énoncé de sa mission:

- une **fonction de supervision**, qui consiste à superviser et assurer le respect des garanties juridiques existantes par les institutions et organes de l'UE³ chaque fois qu'ils traitent des données à caractère personnel;
- une **fonction de consultation**, qui consiste à conseiller les institutions et les organes de l'UE sur toutes les questions pertinentes, et en particulier sur les propositions législatives ayant une incidence sur la protection des données à caractère personnel;

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

Ces fonctions sont exposées en détail dans les chapitres 2, 3 et 4 du présent rapport annuel, qui présentent les principales activités du CEPD et les progrès accomplis en 2011. Certains éléments clés sont résumés dans ce chapitre.

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

Supervision et mise en application

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

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 celles-ci, utilisez le lien: http://europa.eu/about-eu/institutions-bodies/index_fr.htm

Toutes les institutions et tous les organes de l'UE doivent posséder au moins un **délégué à la protection des données** (DPD). En 2011, le nombre total de DPD est passé à 54. Il est important, pour une supervision efficace, d'interagir régulièrement avec ces délégués et leurs réseaux. Le CEPD a travaillé en étroite collaboration avec le «quatuor de délégués à la protection des données», composé des quatre DPD du Conseil, du Parlement européen, de la Commission européenne et du Centre de traduction des organes de l'Union européenne, qui coordonnent le réseau des DPD. Les réunions du réseau des DPD, auxquelles le CEPD participe, fournissent l'occasion de faire le point sur les activités du CEPD, de donner un aperçu de l'évolution de la protection des données dans l'UE et de discuter de questions qui présentent un intérêt commun.

Le contrôle préalable des traitements à risque a encore constitué un aspect important de la supervision. En 2011, le CEPD a reçu 164 notifications de contrôle préalable et adopté 71 avis de contrôle préalable concernant des procédures administratives standard, telles que l'évaluation du personnel, les enquêtes administratives, les procédures disciplinaires et les procédures anti-harcèlement, mais aussi concernant ses activités principales, telles que le système de protection des consommateurs, le système de gestion de la qualité et les contrôles de qualité ex post de l'OHMI, ainsi que le système d'échange électronique d'informations sur la sécurité sociale de la Commission européenne. Ces avis sont publiés sur le site du CEPD et leur mise en œuvre fait l'objet d'un suivi systématique.

En 2011, le nombre des **réclamations** reçues par le CEPD est passé à 107; 26 de ces réclamations ont été déclarées recevables. De nombreuses réclamations irrecevables concernaient des problématiques nationales, pour lesquelles le CEPD n'est pas compétent. Dans les 15 affaires résolues courant 2011, le CEPD a conclu soit qu'il n'y avait pas de violation des règles de protection des données, soit que le responsable du traitement avait adopté les mesures nécessaires pour se conformer à ces règles. À l'inverse, dans deux dossiers, le CEPD a constaté un non-respect des règles de protection des données et a transmis des recommandations au responsable.

L'application du règlement par les institutions et organes fait également l'objet d'un suivi systématique par le recours à un bilan régulier des indicateurs de performance impliquant toutes les institutions et tous les organes de l'UE. Le CEPD a lancé son troisième bilan surveillant la conformité aux règles de protection des données (enquête 2011), donnant

lieu à un rapport mettant en avant les progrès accomplis par les institutions et organes dans la mise en œuvre du règlement, et soulignant également leurs lacunes. En plus de cet exercice général, des contrôles ciblés ont également été effectués dans les cas où, à la suite des activités de supervision, le CEPD avait des raisons de s'inquiéter du degré de conformité aux normes de certaines institutions ou de certains organes. Ces contrôles ont pris la forme d'une correspondance avec l'institution ou l'organe ou d'une visite d'une journée, notamment au sein de l'Agence ferroviaire européenne, de l'Office communautaire des variétés végétales, de la Fondation européenne pour l'amélioration des conditions de vie et de travail et de l'Agence du système global de navigation par satellite européen.

Le CEPD a également réalisé une inspection sur place au sein du CEDEFOP, de l'OLAF et de la BCE, afin de vérifier la conformité par rapport à des points spécifiques.

Des travaux ont également été effectués en réponse à des **consultations sur les mesures administratives** envisagées par les institutions et organes de l'UE concernant le traitement des données à caractère personnel. Plusieurs questions ont été soulevées, notamment la publication des photos des employés sur l'intranet, l'identification du responsable du traitement lors de l'exploitation d'un système de télévision en circuit fermé (CCTV) dans les locaux d'une autre institution et le traitement des courriers électroniques des employés.

Le CEPD a également adopté des **lignes directrices** relatives aux procédures anti-harcèlement et à l'évaluation du personnel, et a suivi les progrès accomplis par les institutions et organes à la suite des lignes directrices en matière de vidéosurveillance.

Consultation

L'année 2011 a été très chargée en ce qui concerne la consultation, avec un nombre record de 24 avis, 12 observations formelles et 41 observations informelles. Le CEPD a continué d'appliquer une approche proactive de la consultation en se fondant sur un inventaire régulièrement mis à jour des propositions législatives à soumettre à la consultation, ainsi que sur la disponibilité d'observations informelles lors des étapes préparatoires des propositions législatives. Tirant parti de cette disponibilité d'observations informelles, les services de la Commission ont presque doublé le nombre de consultations informelles en 2011 par rapport à 2010.

Les travaux de la Commission sur un cadre juridique modernisé en matière de protection des données en Europe méritent d'être mentionnés plus particulièrement. Le processus de révision législative a été suivi de près par le CEPD qui a apporté une contribution à différents niveaux, y compris un avis sur la communication de la Commission établissant une approche globale de la protection des données en Europe, en janvier, et des observations informelles sur les projets de propositions législatives, en décembre.

Il semble y avoir une diversification générale des domaines relatifs aux questions de protection des données: outre les priorités traditionnelles telles que l'espace de liberté, de sécurité et de justice (ELSJ) et les transferts de données internationaux, de nouveaux domaines émergent progressivement, comme le montre le grand nombre d'avis adoptés en rapport avec le marché intérieur. Les faits marquants suivants incluent une sélection des avis adoptés dans les différents domaines.

Concernant l'**ELSJ**, le CEPD a rendu plusieurs avis très critiques sur des questions telles que le rapport d'évaluation de la directive 2006/24/CE sur la conservation des données et la proposition relative à un système européen de traitement des données des dossiers passagers. Les données des dossiers passagers ont également fait l'objet de deux avis concernant les accords en vue du transfert de ces données vers l'Australie et les États-Unis, respectivement. Le CEPD a également commenté la communication de la Commission sur un système européen de surveillance du financement du terrorisme (SSFT), mettant en doute sa nécessité.

Concernant **la technologie de l'information et la stratégie numérique**, le CEPD a publié un avis novateur sur la neutralité de l'internet, soulignant les répercussions de certaines pratiques de surveillance des fournisseurs d'accès internet. Il a également rendu son tout premier avis sur un projet de recherche financé par l'UE concernant des moyens d'appliquer la biométrie dans le respect de la vie privée.

Dans le domaine du **marché intérieur**, le CEPD a rendu, entre autres, un avis sur le système d'information du marché intérieur (IMI), demandant instamment que les fonctionnalités devant être ajoutées à l'avenir soient clarifiées. Le CEPD a rendu d'autres avis importants sur l'intégrité et la transparence du marché de l'énergie, ainsi que sur les produits dérivés négociés de gré à gré, les contreparties centrales et les référentiels centraux. Dans ces

dossiers, les propositions visaient à accorder aux autorités réglementaires des pouvoirs d'enquête étendus qui n'étaient pas clairement définis. Le CEPD a donc demandé une plus grande clarté.

Plusieurs avis ont été rendus concernant **l'application des lois dans un contexte transfrontalier**. Par exemple, le CEPD a donné des orientations sur les propositions concernant la directive relative au respect des droits de propriété intellectuelle, demandant l'établissement d'un délai de conservation clair et la clarification de la base juridique d'une base de données associée. Concernant la proposition en vue d'une ordonnance européenne de saisie conservatoire des comptes bancaires, il a insisté sur la nécessité de limiter le traitement de données à caractère personnel au minimum nécessaire.

Concernant **la santé publique et les consommateurs**, le CEPD a rendu un avis sur le système de coopération en matière de protection des consommateurs (SCPC), demandant instamment au législateur de réexaminer les délais de conservation et d'étudier des moyens permettant de garantir la prise en compte du respect de la vie privée dès la conception.

Le CEPD est également intervenu dans d'autres domaines, tels que le règlement portant réforme de l'OLAF, le règlement financier de l'UE et l'utilisation de tachygraphes numériques par les conducteurs professionnels.

Affaires portées devant les tribunaux

En 2011, le CEPD est intervenu dans cinq affaires devant le Tribunal et le Tribunal de la fonction publique.

L'une des affaires traitait d'un transfert présumé illégal de données médicales entre les services médicaux du Parlement et ceux de la Commission. Le Tribunal de la fonction publique - prenant cette initiative pour la première fois - a invité le CEPD à intervenir. Dans son jugement, le Tribunal a suivi le raisonnement du CEPD et accordé une compensation financière au demandeur.

Trois autres affaires traitaient de l'accès aux documents des institutions de l'UE. On peut considérer que ces affaires entrent dans le cadre du suivi de l'arrêt *Bavarian Lager*. Dans les trois affaires, le CEPD a plaidé en faveur d'une plus grande transparence. Le Tribunal a suivi ce raisonnement dans une affaire. Dans une autre affaire, il a soutenu la

décision du Parlement de ne pas accorder l'accès. La troisième affaire est encore en cours au moment de la rédaction du présent rapport.

De plus, le CEPD est intervenu dans une procédure en infraction à l'encontre de l'Autriche concernant l'indépendance des APD. Dans son intervention, il a fait valoir que la structure organisationnelle du bureau de l'APD autrichienne ne respectait pas le niveau d'indépendance exigé par la directive 95/46/CE. Cette affaire est également en cours au moment de la rédaction du présent rapport.

Coopération

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

Le CEPD et le groupe de travail «Article 29» ont coopéré sur toute une série de sujets, notamment dans le contexte des sous-groupes sur les dispositions essentielles et sur les frontières, les voyages et l'application de la loi (*BTLE - borders, travel and law-enforcement*). Dans le premier sous-groupe, le CEPD était le rapporteur de l'avis sur la notion de «consentement».

Outre le groupe de travail Article 29, le CEPD a poursuivi sa coopération étroite avec les autorités mises en place pour exercer une **supervision conjointe des systèmes d'information à grande échelle de l'Union**.

Un élément important de ces activités de coopération est **Eurodac**. 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 Bruxelles en juin et octobre 2011. Le groupe a mené une inspection conjointe sur la question de la suppression préalable de données, développé un cadre commun pour l'audit de sécurité complet prévu et a programmé une autre inspection conjointe, dont les résultats seront communiqués en 2012. De plus, le groupe a examiné de manière informelle la question de la supervision conjointe du système d'information sur les visas (VIS), qui est opérationnel depuis octobre 2011.

Un arrangement similaire régit la supervision du **système d'information douanier (SID)**, dans le cadre de laquelle le CEPD a organisé deux réunions du groupe de coordination du contrôle du SID en 2011. Les réunions ont regroupé les représentants des autorités nationales chargées de la protection des données, ainsi que des représentants de l'autorité de contrôle commune des douanes et du secrétariat chargé de la protection des données. Lors de la réunion de juin, le groupe a adopté un plan d'action décrivant ses activités prévues pour 2011 et 2012. Lors de la réunion de décembre, il a convenu de ses deux premières inspections conjointes. Les résultats de ces inspections seront présentés courant 2012.

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 2011, la conférence européenne, organisée par le groupe de travail «Article 29» et le CEPD, s'est tenue à Bruxelles. À Mexico, les commissaires à la vie privée et à la protection des données du monde entier ont adopté une déclaration demandant une coopération efficace dans un monde caractérisé par une circulation massive des données à caractère personnel.

Chiffres-clés du CEPD en 2011

→ 71 avis de contrôle préalable adoptés, et 6 avis de contrôle non préalable

→ 107 réclamations reçues, dont 26 recevables.

Principaux types de violations alléguées: violation de la confidentialité des données, collecte excessive de données ou usage illégal de données par le responsable du traitement

→ 34 consultations sur les mesures administratives. Des conseils ont été donnés sur toute une série d'aspects juridiques liés au traitement des données à caractère personnel par les institutions et organes de l'UE

→ 4 inspections effectuées

→ 2 lignes directrices publiées sur les procédures anti-harcèlement et l'évaluation du personnel

→ 24 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 ou au marché intérieur.

→ 12 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».

→ 41 séries d'observations informelles

→ 14 nouveaux collègues recrutés

1.2. Résultats en 2011

Les principaux objectifs suivants ont été définis en 2010. La plupart de ces objectifs ont été complètement ou partiellement atteints en 2011. Dans certains cas, les travaux se poursuivront en 2012.

- **Sensibilisation**

Le CEPD a investi du temps et des ressources dans des exercices de sensibilisation à l'intention des institutions et des organes de l'UE et des DPD, sous la forme d'orientations thématiques, notamment dans les domaines des procédures anti-harcèlement, de l'évaluation du personnel, et d'ateliers sur la protection des données à l'intention des DPD ou des responsables du traitement.

- **Rôle du contrôle préalable**

En 2011, le CEPD a reçu 164 notifications de contrôle préalable, le deuxième chiffre le plus élevé de son histoire. Cette augmentation est essentiellement liée à la mise en place de visites des agences et d'inspections sur place, ainsi qu'à la publication d'orientations thématiques. Les notifications reçues d'agences nouvellement créées ont également contribué à cette hausse. Le CEPD a continué à mettre fortement l'accent sur la mise en œuvre des recommandations formulées dans les avis de contrôle préalable.

- **Exercices de contrôle et d'établissement de rapports**

Le CEPD a entamé son troisième bilan, surveillant le respect des règles de protection des données (Enquête 2011). En plus de cet exercice général, des contrôles ciblés ont également été effectués dans les cas où, à la suite des activités de supervision, le CEPD avait des raisons de s'inquiéter du degré de conformité aux normes de certaines institutions ou certains organes. Certains de ces contrôles ont été réalisés par correspondance, tandis que d'autres ont pris la forme d'une visite d'une journée de l'organe concerné aux fins de remédier aux défauts de conformité.

- **Inspections**

Les inspections constituent un instrument essentiel qui permet au CEPD de surveiller et de garantir l'application du règlement. En 2011, le CEPD a procédé à quatre inspections et a continué à donner un suivi aux recommandations formulées lors des inspections précédentes. Un audit de sécurité du système d'information sur les visas (VIS) a également été réalisé.

- **Étendue des consultations**

Le CEPD a encore augmenté sa production, rendant un nombre record de 24 avis et 12 séries d'observations formelles. Dans de nombreux cas, la Commission avait déjà consulté le CEPD avant d'adopter ses propositions, ce qui a donné lieu à 41 séries d'observations informelles. De nombreux avis ont été suivis par des présentations devant la commission LIBE du Parlement européen ou les groupes de travail du Conseil concernés. Les propositions pour lesquelles des avis ont été publiés ont été choisies à partir d'un inventaire systématique des matières et des priorités pertinentes pour le CEPD. Les avis, les observations formelles et l'inventaire sont publiés sur le site internet du CEPD.

- **Réexamen du cadre juridique de la protection des données**

Le CEPD a publié un avis sur la communication de la Commission sur une approche globale de la protection des données à caractère personnel, ainsi que des observations informelles sur les propositions législatives. Il a suivi le débat de près et y a apporté sa contribution lorsque cela s'est avéré nécessaire et approprié.

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

Le CEPD a suivi avec attention les développements politiques liés au programme de Stockholm, rendant un avis sur la proposition de directive sur l'utilisation des données PNR à des fins répressives, ainsi que des observations formelles sur la création d'un système européen de surveillance du financement du terrorisme (SSFT). Bien qu'aucune proposition législative n'ait été présentée au sujet des frontières intelligentes, le CEPD a abordé la question dans son avis sur la communication de la Commission relative à la migration.

- **Initiatives dans le domaine des technologies**

Le CEPD a rendu son premier avis sur un projet de recherche financé par l'UE. Le projet traitait de la mise en œuvre de la biométrie dans le respect de la vie privée. Dans le contexte de la stratégie numérique, le CEPD a publié un avis sur la neutralité de l'internet.

- **Autres initiatives**

Le CEPD a publié plusieurs avis et commentaires sur d'autres initiatives ayant des répercussions sur la protection des données à caractère personnel,

comme le système d'information sur le marché intérieur (IMI) et l'utilisation des scanners corporels dans les aéroports.

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

Le CEPD a participé activement aux activités du groupe de travail «Article 29» sur la protection des données, et notamment aux activités des sous-groupes sur les dispositions clés et sur les frontières, les voyages et l'application de la loi.

- **Supervision conjointe**

Le CEPD a assumé efficacement les fonctions de secrétariat pour les autorités chargées de la protection des données impliquées dans la supervision conjointe d'Eurodac et le système d'information douanier. Concernant le système d'information sur les visas, les autorités chargées de la protection des données représentées dans le groupe de coordination du contrôle ont eu un premier échange de vues dans le cadre de l'une des réunions de supervision conjointe d'Eurodac, examinant les implications du système et l'approche de la supervision.

- **Organisation interne**

À la suite de la réorganisation du secrétariat en 2010, l'institution a décidé de lancer une révision stratégique de toutes ses activités de 2011, sous la direction du groupe de travail «révision stratégique», constitué du directeur et de représentants de toutes les équipes et disciplines. En octobre 2011, la première phase de la révision a débouché sur une réunion interne de l'institution qui a permis aux membres et au personnel de réfléchir sur leurs missions, valeurs et objectifs.

- **Gestion des ressources**

En coopération avec le Parlement, le CEPD a réalisé un examen approfondi du marché des fournisseurs de systèmes de gestion des dossiers, et a sélectionné le contractant qui proposait le produit le plus approprié. Fin 2011, le contrat a été signé et les travaux visant à développer un système adapté ont commencé.

Courant 2011, les travaux visant à intégrer le CEPD dans des applications informatiques dans le domaine des ressources humaines sur la base d'accords de niveau de services se sont poursuivis: le système Syslog Formation a été lancé avec succès, les travaux sur le système SysperII ont commencé, et un accord sur l'introduction du système MIPS a été trouvé en 2012.

2

SUPERVISION ET MISE EN APPLICATION

2.1. Introduction

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

Tout au long de l'année 2011, le CEPD a continué de mener à bien ses principales activités opérationnelles, 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 a continué de représenter un aspect important des activités de supervision du CEPD en 2011, notamment en raison d'une augmentation du nombre de notifications reçues. Le nombre et la complexité des réclamations reçues ont également augmenté, entraînant la résolution de 15 affaires en 2011. Dans le cadre des consultations sur les mesures administratives, le CEPD a examiné différentes questions.

Outre ses activités de supervision courantes, le CEPD a également élaboré d'autres moyens permettant de veiller au respect du règlement conformément à la politique de conformité et d'application adoptée en décembre 2010. En plus de son bilan général, le CEPD a effectué des exercices de contrôle ciblé dans les cas où, à la suite des activités de supervision, il avait des raisons de s'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 concernés, de visites d'une journée réalisées par le management aux fins de remédier aux défauts de conformité ou d'inspections visant à vérifier la conformité par rapport à des points spécifiques.

Le CEPD a également poursuivi ses activités de sensibilisation, notamment en organisant une formation spécifique pour les DPD, sous la forme d'un atelier ou d'une téléconférence, et en élaborant des orientations thématiques à l'intention des institutions et organes dans le domaine des procédures anti-harcèlement et de l'évaluation du personnel.

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 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). Plusieurs institutions ont également nommé des coordinateurs de la protection des données chargés de coordonner tous les aspects de la protection des données au sein d'une direction ou d'une unité particulière.

En 2011, six nouveaux DPD ont été nommés au sein de nouvelles agences ou entreprises communes, portant le nombre total des DPD à 54. Comme de

nombreux mandats ont expiré cette année, il y a également eu un fort taux de rotation dans les institutions et les agences établies.

Depuis plusieurs années, les DPD se rencontrent régulièrement afin d'échanger leurs expériences et d'examiner les questions horizontales. Ce réseau informel a fait la preuve de son efficacité en matière de collaboration, ce qui a continué d'être le cas en 2011.

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 des DPD qui ont eu lieu en avril 2011 à l'Agence des droits fondamentaux à Vienne et en octobre 2011 chez le Médiateur européen à Strasbourg. Le CEPD a profité de l'occasion pour fournir aux DPD des informations sur ses récents travaux, donner un aperçu de l'évolution récente de la protection des données dans l'UE et discuter de questions présentant un intérêt commun.

Plus spécifiquement, le CEPD a utilisé cette enceinte pour discuter des procédures et instruments de contrôle préalable; présenter l'évolution

récente de la protection des données; informer les DPD sur le réexamen du cadre juridique; présenter les lignes directrices thématiques et l'enquête 2011; donner des informations sur les initiatives de formation et faire part de l'évolution des lignes directrices en matière de vidéosurveillance. Ce forum permet également de partager des initiatives en vue de la Journée européenne de la protection des données (le 28 janvier).

Le 8 juin 2011, le CEPD a organisé un atelier destiné aux DPD dans le cadre de son programme de formations (voir également le point 2.7.2). L'objectif était d'offrir une formation de base aux DPD, notamment ceux qui avaient été récemment nommés. Le programme incluait une introduction aux principes et définitions essentiels du règlement et des présentations sur des thèmes spécifiques tels que la base juridique du traitement des données, les droits des personnes concernées, ainsi que le transfert et le traitement de données pour le compte du responsable du traitement. Ces présentations se sont appuyées sur des exemples concrets tirés des activités de supervision du CEPD. La session de l'après-midi a été consacrée à la coopération entre les DPD et le CEPD, avec un accent sur les aspects pratiques du traitement des réclamations, les procédures de contrôle préalable et la sécurité des traitements. Cet atelier a été largement suivi et la participation active des DPD a favorisé un échange productif d'expériences et de préoccupations.



30^e réunion des DPD à Strasbourg, octobre 2011.

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. Au cours de la période considérée, le CEPD a continué d'appliquer les critères élaborés au cours des années précédentes⁴ 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

Notification

Les contrôles préalables doivent être effectués par le CEPD après réception de la notification du DPD. Si celui-ci doute 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*.

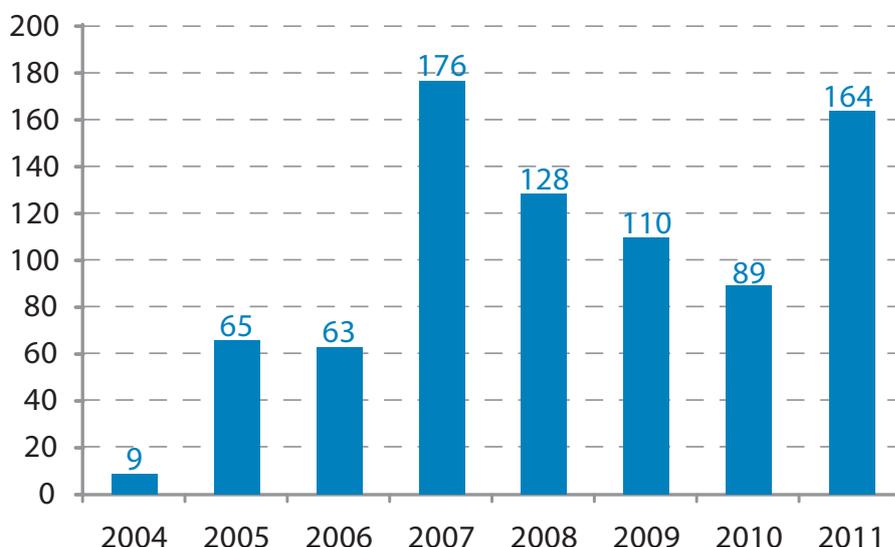
Délai, suspension et prolongation

Le CEPD doit rendre son avis dans les deux mois qui suivent la réception d'une notification⁵. Lorsqu'il demande des informations complémentaires, le délai de deux mois est généralement suspendu jusqu'à ce que les informations en question lui aient été communiquées. Cette période de suspension comprend le délai accordé au DPD pour formuler ses observations et fournir, le cas échéant, des informations complémentaires sur le projet final. Lorsque la complexité du dossier l'exige, le CEPD peut également prolonger la période initiale de deux mois supplémentaires. Si, au terme de ce délai de deux mois, éventuellement prolongé, aucune décision n'a été rendue, l'avis du CEPD est réputé favorable. Jusqu'à présent, ce cas de figure dans lequel l'avis aurait été rendu de manière tacite ne s'est jamais produit.

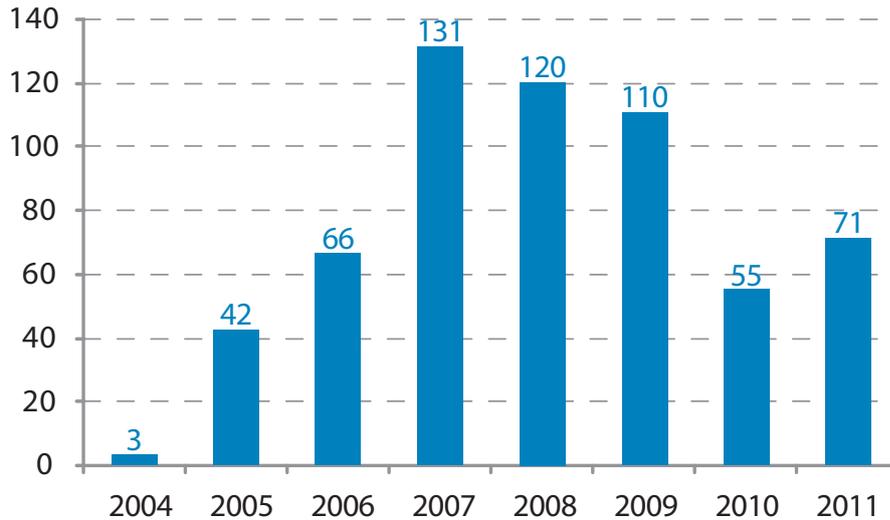
⁴ Voir le rapport annuel 2005, point 2.3.1.

⁵ Pour les cas examinés *a posteriori* reçus avant le 1^{er} septembre 2011, le mois d'août a été exclu du calcul des délais, tant pour les institutions/organes que pour le CEPD.

Notifications au CEPD, par an



Avis du CEPD à la suite d'un contrôle préalable, par an



Registre

En 2011, le CEPD a reçu 164 notifications de contrôle préalable - le deuxième chiffre le plus élevé de son histoire. Cela représente une hausse spectaculaire avec près de deux fois plus de notifications reçues en 2011 qu'en 2010. Même si le CEPD est venu 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 2011, ont entraîné une hausse du nombre de notifications.

L'article 27, paragraphe 5, du règlement prévoit que le CEPD doit tenir un registre de tous les traitements qui lui sont notifiés en vue d'un contrôle préalable. Ce registre contient les informations visées à l'article 25 et est, par souci de transparence, accessible au public sur le site internet du CEPD (à l'exception des mesures de sécurité, qui ne sont pas mentionnées dans le registre public).

Avis

Conformément à l'article 27, paragraphe 4, du règlement, la position finale du CEPD revêt la forme d'un avis qui est notifié au responsable du traitement et au délégué à la protection des données de l'institution ou de l'organe. En 2011, le CEPD a rendu **71 avis de contrôle préalable** et **6 avis sur des «contrôles non préalables»** (voir le point 2.3.5). Cela représente une hausse importante par rapport à l'année précédente et tient également compte du fait que le CEPD s'est occupé d'un nombre important de

dossiers avec avis conjoint: en 2011, il y a eu 10 avis conjoints concernant au total 52 notifications (par exemple, un avis conjoint sur les données concernant la santé traitant au total 18 notifications). En rendant ces avis conjoints à la suite de la publication de lignes directrices, par exemple sur les données concernant la santé et la lutte contre le harcèlement, le CEPD a donc augmenté son efficacité au détriment de sa visibilité statistique.

Comme l'année précédente, un **nombre important de ces avis** ont été adressés à la **Commission européenne**, avec 16 avis de contrôle préalable (et trois contrôles non préalables). Contrairement aux années précédentes où les autres grandes institutions de l'UE (le Parlement européen et le Conseil) étaient fréquemment les destinataires des avis du CEPD, les agences et organes de l'UE se sont placés en deuxième position en 2011, recevant un nombre exceptionnellement élevé d'avis du CEPD (en partie sous la forme d'avis conjoints). On peut citer, par exemple, six avis ayant trait aux traitements adressés à l'Office communautaire des variétés végétales, cinq avis adressés à la Fondation européenne pour l'amélioration des conditions de vie et de travail et trois ou quatre avis adressés à plusieurs autres agences de l'UE. Les agences de l'UE ont donc continué de notifier leurs activités principales et leurs procédures administratives standard conformément aux procédures pertinentes établies par le CEPD (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 conclusions, le CEPD indique généralement que le traitement ne semble pas violer 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. Par exemple, le CEPD a introduit une interdiction temporaire à l'encontre d'un traitement qui s'est avéré violer les principes de protection des données (voir le point 2.3.3.10).

Une fois que le CEPD a rendu son avis, celui-ci est rendu public. Tous les avis publiés sont disponibles sur le site internet du CEPD 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 s'appuie sur des bases identiques et que les avis du CEPD sont adoptés à l'issue d'une analyse complète de toutes les informations pertinentes. Ce manuel comprend un modèle d'avis basé sur l'expérience pratique accumulée et est mis à jour en permanence. Un système de gestion des tâches a été mis en place pour s'assurer que toutes les recommandations relatives à un dossier donné sont mises en œuvre et, le cas échéant, que toutes les décisions sont respectées (voir le point 2.3.6).

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

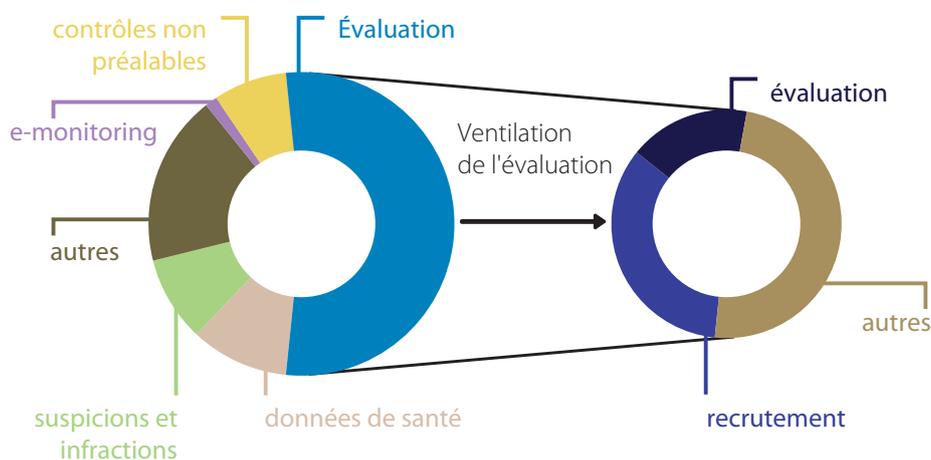
En octobre 2008, le CEPD a lancé une nouvelle procédure applicable aux contrôles préalables ex post

dans les agences de l'UE. Étant donné que les procédures standard sont identiques dans la plupart des agences de l'UE et qu'elles sont fondées sur des décisions de la Commission, l'idée est de rassembler les notifications portant sur un thème similaire et soit de rendre un avis collectif (pour plusieurs agences), soit de réaliser un « mini-contrôle préalable » traitant uniquement des besoins spécifiques de chaque agence. Pour aider les agences à remplir leurs notifications, le CEPD présente 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 premier thème était le **recrutement**, qui a fait l'objet d'un avis horizontal du CEPD en mai 2009, couvrant les notifications de 12 agences. Un deuxième ensemble de lignes directrices a été envoyé aux agences à la fin septembre 2009 concernant le **traitement des données relatives à la santé**, 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, le CEPD a 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 (sur les orientations thématiques, voir le point 2.7).

2.3.3. Principales questions liées aux contrôles préalables

Avis 2011 par catégories principales



2.3.3.1. Traitement des données relatives à la santé sur le lieu de travail

À la suite de la publication des **lignes directrices du CEPD** sur le traitement des données relatives à la santé sur le lieu de travail, le CEPD a réalisé un exercice particulièrement difficile en examinant 18 notifications de contrôle préalable concernant les traitements de 18 agences dans le domaine des visites d'embauche, des visites annuelles et des congés maladie. À la lumière des similarités entre les procédures et les pratiques de protection des données, le CEPD a décidé de rendre un avis conjoint le 11 février 2011 (dossier 2010-0071).

L'avis conjoint sur le traitement des données relatives à la santé sur le lieu de travail a soulevé trois questions essentielles:

- premièrement, le **concept général de «données relatives à la santé»** et l'impact des principes de protection des données sur les traitements concernant les examens de pré-recrutement, les examens médicaux annuels et les congés de maladie;
- deuxièmement, l'absence d'éléments importants dans les contrats conclus entre plusieurs agences et leurs prestataires externes de services médicaux, notamment de mesures de sécurité et de clauses relatives à la protection des données au regard de l'article 23 du règlement;
- troisièmement, la portée incomplète des déclarations de confidentialité utilisées: pour que le traitement soit licite en vertu des articles 11 et 12 du règlement, le responsable du traitement doit informer les personnes concernées de *tous* les éléments liés aux traitements, en particulier lorsque le traitement se fonde sur le consentement de la personne concernée.



Les institutions, agences et organes de l'UE traitent des données relatives à la santé.

2.3.3.2. Système de coopération en matière de protection des consommateurs («SCPC»)

Le système de coopération en matière de protection des consommateurs (SCPC) est un système informatique, conçu et exploité par la Commission, qui facilite la coopération entre les autorités des États membres et la Commission européenne dans le domaine de la protection des consommateurs, conformément au règlement (CE) n° 2006/2004 relatif à la coopération en matière de protection des consommateurs. Le 4 mai 2011, le CEPD a rendu un avis de contrôle préalable concernant l'échange d'informations comprenant des données à caractère personnel par les autorités compétentes dans le cadre de cette coopération (dossier 2009-0019).



Les technologies d'information modernes contribuent à la protection des consommateurs.

La Commission européenne joue un rôle central dans la configuration de l'architecture du système SCPC et dans l'exploitation du système, et elle est soumise au contrôle du CEPD. Dans son avis, le CEPD a recommandé que la Commission européenne adopte des mesures techniques et organisationnelles. Un grand nombre des recommandations formulées dans l'avis – y compris celles concernant la formation, l'établissement de lignes directrices relatives à la protection des données, l'information des personnes concernées et l'intégration de **solutions de «prise en compte du respect de la vie privée dès la conception» dans l'architecture du système** – devraient également faciliter le respect des règles relatives à la protection des données par les autres utilisateurs du système, tels que les autorités compétentes des États membres.

2.3.3.3. Système de gestion de la qualité et contrôles de qualité ex post de l'OHMI

Depuis 2007, l'Office de l'harmonisation dans le marché intérieur (OHMI) procède à des contrôles de qualité ex ante et ex post portant sur les décisions prises par ses examinateurs de marques à des fins de contrôle de la qualité. Les résultats de ces contrôles révèlent les erreurs éventuelles et les types d'erreurs commises par les examinateurs. En septembre 2009, l'OHMI a informé les examinateurs que les résultats des contrôles de qualité ex post («CQEP») seraient également utilisés aux fins de leur appréciation annuelle des performances. En conséquence, le système de contrôles de qualité ex post a été soumis pour contrôle préalable au CEPD, qui a rendu son avis le 9 juin 2011 (dossier 2010-0869).

Vu le **changement de finalité** du traitement (du contrôle général de la qualité à l'évaluation des performances des individus), dans son avis, le CEPD a conseillé à l'OHMI d'adopter une décision interne établissant des **garanties appropriées de protection des données** et assurant que les données des CQEP ne constituent pas l'unique fondement de l'appréciation annuelle des performances des examinateurs. Le CEPD a en outre recommandé l'adoption de mesures visant à garantir l'exactitude des données, à informer les examinateurs au sujet du traitement et à s'assurer qu'ils jouissent de tous leurs droits en tant que personnes concernées.

2.3.3.4. Système de contrôle de l'accès – Centre commun de recherche (CCR) - Site Ispra

Le système de contrôle de l'accès du site Ispra du Centre commun de recherche (CCR) a pour objectif de protéger les locaux contre les accès non autorisés et les menaces internes et externes. La procédure de contrôle préalable a été suscitée par le fait que des lecteurs biométriques couvraient l'accès à certaines zones protégées qui n'étaient utilisées que par quelques membres du personnel. Le CEPD a rendu un avis le 15 juillet 2011 (dossier 2010-0902).

Le CEPD a conclu que la Commission européenne avait **violé le règlement** au motif qu'elle avait installé et exploité un système de contrôle d'accès biométrique sans informer au préalable le CEPD du traitement envisagé. En outre, le CEPD a notamment demandé au CCR:

- d'adopter une base juridique pour les traitements effectués par le système de contrôle d'accès à l'aide de la biométrie;
- de se conformer aux lignes directrices TVCC et rendre compte au CEPD des mesures mises en œuvre à cet égard;
- de réexaminer les choix technologiques réalisés au moyen d'une **analyse d'impact**, y compris un calendrier pour mettre en œuvre les changements technologiques.

2.3.3.5. Étude de reconnaissance des empreintes digitales des enfants âgés de moins de 12 ans réalisée par le CCR

Le Centre commun de recherche (CCR) a réalisé une étude intitulée «Étude de reconnaissance des empreintes digitales des enfants âgés de moins de 12 ans» dans le champ d'application du système européen d'information sur les visas (VIS). L'étude a examiné le développement physiologique de la structure en crêtes des empreintes digitales des enfants (distance entre les crêtes, emplacement des minuties) et le taux de reconnaissance résultant d'algorithmes de mise en correspondance d'empreintes digitales adaptés aux enfants. Le traitement porte sur des données biométriques et est dès lors soumis au contrôle préalable du CEPD, afin de vérifier que des garanties strictes ont été appliquées; le CEPD a publié son avis le 25 juillet 2011 (dossier 2011-0209).



La reconnaissance des empreintes digitales fait partie des identifiants biométriques les mieux connus. Il s'agit d'une méthode automatisée qui permet de vérifier l'existence d'une correspondance entre deux empreintes digitales humaines.

Le CEPD a reconnu l'importance de l'étude biométrique, mais a souligné la nécessité que le responsable du traitement réalise une **évaluation des risques** et établisse une **politique d'accès** concernant le traitement en question.

2.3.3.6. Échange électronique d'informations sur la sécurité sociale - Commission européenne

Le CEPD a procédé au contrôle préalable d'un système informatique pour l'échange d'informations sur la sécurité sociale créé par la Commission européenne. Le système, qui devrait être pleinement opérationnel à compter de 2012, vise à faciliter le calcul et le paiement des prestations de sécurité sociale pour les personnes ayant travaillé dans plus d'un État membre, et permet une vérification plus efficace des données.

Dans son avis du 28 juillet 2011 (dossier 2011-0016), le CEPD a salué la proposition de créer un «guichet unique» pour les personnes qui souhaitent exercer leurs droits. Le CEPD a néanmoins invité la Commission européenne à garantir que les personnes concernées peuvent pleinement faire valoir leurs droits auprès du point de contact correspondant dans l'État membre. Afin d'assurer la sécurité des données, le CEPD a également recommandé d'adopter plusieurs mesures techniques, et notamment de transmettre des données cryptées uniquement, de telle sorte que la Commission européenne n'ait pas accès au contenu des données sensibles transitant via le système. Le système étant encore en phase de production, le CEPD a souligné qu'il devrait être informé de toute modification substantielle apportée à la conception du système qui pourrait avoir une incidence sur le niveau de protection des données.

2.3.3.7. Système de contrôle d'accès physique - Commission européenne

Le système de contrôle d'accès physique (PACS) de la Commission européenne exécute toutes les fonctions de sécurité physique et est fondé sur l'utilisation des **données biométriques**. L'utilisation de ces données présente des risques particuliers au regard des droits et libertés des personnes concernées, en raison de **caractéristiques inhérentes à ce type de données**. **Par exemple**, en rendant possible la mesure des caractéristiques du corps humain par des machines et en permettant l'utilisation ultérieure de ces caractéristiques, la biométrie modifie définitivement la relation entre corps et identité. Ces risques justifient que ces traitements de données fassent l'objet d'un contrôle préalable de la part du CEPD afin de vérifier que de sérieuses garanties ont été appliquées. Le CEPD a rendu son avis le 8 septembre 2011 (dossier 2010-0427).

Le CEPD a félicité la Commission européenne de l'avoir fait intervenir à un stade très précoce, facilitant ainsi l'élaboration d'une approche respectueuse de la vie privée concernant la mise en œuvre des traitements en cause. Entre autres aspects du PACS, le CEPD a axé son analyse sur les catégories de personnes concernées, l'existence de procédures de secours pour les personnes qui ne sont pas admissibles à l'enrôlement, même si cette situation est temporaire (par exemple, en raison d'empreintes digitales endommagées), les délais de conservation et les mesures de sécurité mises en œuvre.

2.3.3.8. *Projet «IDEAS-Exclusion d'experts par les proposants» - ERCEA*

Les propositions de projets soumises à l'Agence exécutive du Conseil européen de la recherche (ERCEA) font l'objet d'une évaluation par les pairs, c'est-à-dire une évaluation par des panels composés de chercheurs et d'universitaires indépendants. L'avis du CEPD du 21 septembre 2011 (dossier 2010-0661) concerne une procédure notifiée par l'Agence exécutive du Conseil européen de la recherche, dans le cadre de laquelle les proposants qui présentent une proposition de projet peuvent demander à ce qu'un maximum de trois personnes déterminées ne participent pas à l'évaluation par les pairs de leur proposition. La finalité du traitement est de garantir une évaluation juste, équitable et objective des propositions de projets, et de répondre aux préoccupations des proposants quant à la justesse du résultat de l'évaluation et à l'objectivité des experts.

À la lumière du principe de la **qualité des données**, le CEPD a invité l'ERCEA à envisager la possibilité de déterminer des catégories prédéfinies plutôt qu'un champ de «texte libre» pour soumettre des raisons précises permettant d'exclure certains pairs du panel. Le CEPD a également conseillé à l'ERCEA de mettre en place des procédures pour garantir que les droits d'accès et de rectification des experts concernés soient limités pour autant qu'une telle limitation constitue une mesure nécessaire. Sous réserve des restrictions visées à l'article 20 du règlement, tous les experts devraient, par exemple, être en mesure de vérifier s'ils souhaitent rectifier des données objectives et/ou ajouter leur propre déclaration «neutralisante» ou «contrebalançant» l'appréciation subjective du proposant.

2.3.3.9. *Systèmes renforçant la coopération entre les administrations douanières - OLAF*

À l'aide de la même plateforme, trois systèmes (l'unité de coopération opérationnelle virtuelle, le courtier d'assistance mutuelle et le système d'information douanier) visent à renforcer la coopération en matière douanière dans les États membres, la Commission européenne et, dans certains cas, des pays tiers et des organisations internationales. À cet effet, ils permettent l'échange d'informations sur les personnes, les sociétés et les marchandises soupçonnées de violations des réglementations douanière et agricole, afin de demander aux autorités liées aux systèmes de prendre certaines mesures (par exemple, des contrôles spécifiques ou une sur-

veillance discrète). Les systèmes nécessitent le traitement de données sensibles (suspicion de comportement criminel et données relatives à la santé).

Dans son avis conjoint du 17 octobre 2011 sur les trois systèmes (dossiers joints 2010-0797, 2010-0798 et 2010-0799), le CEPD a demandé à l'OLAF de mieux informer les personnes concernées et lui a conseillé d'évaluer la nécessité de traiter certaines catégories de données traitées, ainsi que les délais de conservation applicables.

2.3.3.10. *Politique de «retour au travail» - EU-OSHA*

Dans le cadre de la politique de «retour au travail» de l'Agence européenne pour la sécurité et la santé au travail (EU-OSHA), afin de faciliter le retour au travail des membres du personnel après un congé de maladie, le chef d'unité concerné ou le département des ressources humaines (RH) est chargé de veiller à ce que les mesures soient coordonnées entre le membre du personnel, son médecin généraliste, le délégué à la santé au travail, le service des ressources humaines et toute autre partie prenante (par exemple, les délégués syndicaux et les représentants du personnel). Cela implique l'entretien de contacts réguliers avec le membre du personnel malade, les orientations en vue d'un examen médical et vers des thérapies individuelles telles que la psychothérapie, et l'évaluation de la fonction du

Dans son avis du 24 octobre 2011 (dossier 2011-0752), le CEPD a conclu que certains éléments du traitement enfreignaient les principes de nécessité et de proportionnalité et violaient les principes d'adéquation, de pertinence et de proportionnalité, ainsi que d'exactitude, et a donc **interdit temporairement le traitement**. Le CEPD a noté que, bien que la finalité déclarée du traitement fasse clairement référence à l'aptitude à travailler dans l'environnement de travail, du point de vue de la médecine du travail et de la médecine préventive, seuls les médecins spécialistes - et non pas le chef d'unité ou le département des ressources humaines - sont à même de certifier ces aspects. Le CEPD a fait part d'autres inquiétudes quant à la façon dont l'EU-OSHA prévoit de veiller à ce que tout consentement de la personne concernée soit fondé et donné librement et que seules les données appropriées, pertinentes - non excessives - soient collectées, traitées et transférées.

membre du personnel et des examens médicaux, qui peut donner lieu à une réaffectation ou à un ajustement du temps de travail, des responsabilités et des tâches.

2.3.4. Consultations concernant la nécessité d'un contrôle préalable

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

En cas de doute, les institutions et les organes de l'UE peuvent consulter le CEPD quant à la nécessité d'un contrôle préalable en vertu de l'article 27, paragraphe 3, du règlement. En 2011, le CEPD a reçu 13 consultations de ce type de la part de DPD. Parmi les questions examinées par le CEPD, on peut citer des activités de traitement concernant la mobilité dans un contexte de restructuration et l'utilisation des communications électroniques (téléphonie mobile, courrier électronique et internet).

2.3.5. Notifications non soumises au contrôle préalable ou retirées

À l'issue d'une analyse minutieuse, il a été conclu que six dossiers ne devaient pas faire l'objet d'un contrôle préalable en 2011. Dans ces situations (appelées aussi «contrôles non préalables»), le CEPD peut malgré tout faire des recommandations. En outre, une notification a été retirée et une a été remplacée.

*Dans son avis du 12 novembre 2009 (dossier 2009-0477) concernant la vérification envisagée des pointages Flexitime par rapport aux données sur l'accès physique recueillies par le Conseil de l'Union européenne, le CEPD a confirmé ses doutes quant à la proportionnalité du traitement envisagé. Il a indiqué que le traitement violerait le règlement à plusieurs niveaux (licéité du traitement, nécessité et proportionnalité, changement de finalité et qualité des données) si la vérification des pointages Flexitime par rapport aux données sur le contrôle d'accès physique comme décrit dans la notification était effectuée hors du cadre d'une enquête administrative. Le 6 juillet 2011, le CEPD a reçu une lettre du délégué à la protection des données du Conseil de l'Union européenne l'informant que, comme suite à l'avis de contrôle préalable du CEPD ci-dessus, le responsable du traitement des données avait **retiré la notification** et le système envisagé n'avait pas été mis en œuvre.*

2.3.6. Suivi des avis de contrôle préalable

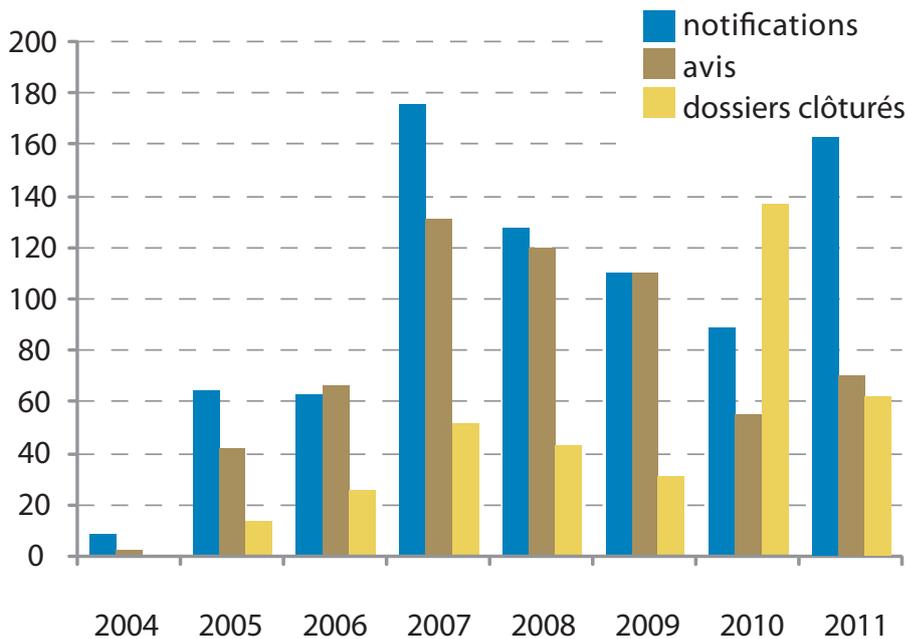
*Le CEPD conclut généralement ses avis de contrôle préalable en indiquant que le traitement ne semble pas violer les dispositions du règlement, à condition que certaines **recommandations** soient prises en compte. Des recommandations sont également formulées lorsque le CEPD examine un dossier afin de décider de la nécessité d'un contrôle préalable et lorsque certains aspects essentiels semblent nécessiter des rectifications. Si le responsable du traitement ne respecte pas ces recommandations, le CEPD peut exercer les pouvoirs qui lui sont conférés en vertu de l'article 47 du règlement.*

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

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

2.3.7. Conclusions

Situation comparative



Les 71 avis de contrôle préalable formulés par le CEPD ont jeté une lumière précieuse sur les traitements des administrations européennes, et ont permis au CEPD de renforcer son expertise et de fournir des orientations génériques dans certains domaines, par exemple en matière de procédures administratives communes. Cela apparaît clairement dans les traitements liés à l'évaluation du personnel et aux procédures anti-harcèlement (voir le point 2.7 «Lignes directrices thématiques»). Le CEPD continuera de fournir ces orientations aux institutions et agences, et il continuera de faciliter le processus de notification des agences.

Concernant le suivi des avis de contrôle préalable du CEPD, 62 dossiers ont été clos en 2011. Le CEPD continuera de contrôler de près le travail de suivi afin de faire en sorte que les institutions et agences intègrent les recommandations formulées par le CEPD en temps utile et de façon satisfaisante.

2.4. Réclamations

2.4.1. 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 données à caractère personnel. 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 des personnes morales ne sont pas recevables.

Les plaignants doivent également s'identifier et les requêtes anonymes ne sont donc pas considérées

comme des «réclamations». Toutefois, les informations anonymes peuvent être prises en considération dans le cadre d'une autre procédure (enquête d'initiative ou demande de notification d'un traitement de données, etc.).

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

Un membre du personnel d'une institution de l'UE a déposé une réclamation concernant le refus d'accès à certaines données figurant dans les documents rédigés dans le cadre d'une évaluation comparative réalisée à différentes étapes d'une procédure de contestation concernant une décision d'octroi de points de mérite. Il a demandé au CEPD d'ordonner à l'institution de lui accorder l'accès aux documents concernés car ceux-ci contenaient des données à caractère personnel le concernant. Cependant, l'institution a affirmé que les documents en question n'avaient jamais existé. Le plaignant a dès lors considéré que l'institution devait rédiger les documents «manquants». Le CEPD n'a pas suivi le raisonnement du plaignant. En effet, l'allégation selon laquelle l'institution n'avait pas correctement conduit la procédure administrative en ne préparant pas tous les documents pertinents sort du cadre des règles relatives à la protection des données. Dès lors, aucune violation des règles relatives à la protection des données n'a été établie dans cette affaire.

Le traitement de données à caractère personnel faisant l'objet d'une réclamation doit être effectué par **l'un des organes ou institutions de l'UE**. En

outre, le CEPD n'est pas une instance de recours pour les décisions prises par les autorités nationales chargées de la protection des données.

Un citoyen d'un pays non membre de l'UE s'est plaint auprès du CEPD du fait qu'un visa d'entrée dans l'espace Schengen lui avait été refusé, ainsi qu'à sa famille, apparemment sur la base des informations fournies par le système d'information Schengen (SIS). Le plaignant a demandé au CEPD de lui permettre d'accéder aux données à caractère personnel figurant dans le SIS à son sujet et à celui de sa famille. Cependant, même si le SIS est établi sur la base du droit de l'UE, s'agissant du droit d'accès des personnes concernées, la supervision n'est pas exercée par le CEPD mais par les autorités nationales chargées de la protection des données (APD), au niveau national. Le plaignant a dès lors été avisé qu'en vertu de l'accord de Schengen en vigueur, il peut demander assistance à l'APD nationale de son choix.

2.4.2. Procédure de traitement des réclamations

Le CEPD examine les réclamations en vertu du cadre juridique en vigueur, des principes généraux du droit de l'Union européenne et des bonnes pratiques administratives communes aux institutions et organes de l'UE. En décembre 2009, le CEPD a adopté un **manuel interne** dont le but est de mettre des orientations en matière de traitement des réclamations à la disposition de son personnel. Ce manuel a été mis à jour en septembre 2011 afin de refléter les modifications apportées à la structure organisationnelle du CEPD et d'intégrer les récents développements dans la pratique du traitement des réclamations.

Le CEPD a également mis en place un **outil statistique** conçu pour examiner les activités liées aux réclamations, et en particulier pour suivre l'évolution de certains dossiers.

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

- de la nature et de la gravité de la violation alléguée des règles régissant la protection des données;

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

En février 2011, le CEPD a amélioré le processus de dépôt des réclamations en créant un **formulaire en ligne de dépôt de plainte** interactif sur son site internet. Une version provisoire de ce formulaire est disponible sur le site internet du CEPD depuis début 2010. Ce formulaire aide les plaignants à évaluer la recevabilité de leur réclamation, et donc à ne soumettre au CEPD que des cas pertinents. Il permet

également au CEPD d'obtenir 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 le nombre de réclamations irrecevables d'environ 60 % au dernier trimestre 2011.

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.

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

Un membre du personnel a envoyé au CEPD un grand nombre de documents échangés avec une institution qui l'employait et a demandé au CEPD de les examiner tous afin de vérifier si les règles de protection des données étaient respectées. Le plaignant n'a formulé aucune allégation spécifique relative à une violation des règles de protection des données et n'a fourni au CEPD aucune indication ou suspicion d'une telle violation. Le CEPD a considéré que la réclamation ne concernait aucune violation, réelle ou potentielle, des règles de protection des données, et a décidé de clôturer l'affaire sans enquête supplémentaire.

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

Une réclamation est en principe **irrecevable** si le plaignant **n'a pas d'abord contacté l'institution**

concernée pour qu'elle remédie à la situation. Si le plaignant n'a pas contacté l'institution, il doit fournir au CEPD des raisons suffisantes pour expliquer cette inaction.

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

Pour assurer le traitement cohérent des réclamations concernant la protection des données et

éviter toute redondance inutile, le **Médiateur européen** et le CEPD ont signé un mémorandum d'accord en novembre 2006. 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.

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

Si une réclamation est recevable, le CEPD ouvrira **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 données à caractère personnel et à toutes les informations nécessaires à l'enquête. Il peut également avoir accès à tous les locaux dans lesquels un responsable du traitement, une institution ou un organe exerce ses activités.

À la fin de l'enquête, il envoie sa **décision** au plaignant ainsi qu'au responsable du traitement des données. Dans 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 au CEPD de **revoir** sa décision dans un délai d'un mois à compter de la date d'adoption de cette décision. Les parties concernées peuvent également introduire un recours direct auprès de la Cour de justice.

Les plaignants n'ont contesté aucune décision du CEPD en 2011. À une occasion, en 2011, le responsable du traitement des données concerné a contesté la décision du CEPD devant le Tribunal (affaire T-345/11). Le Tribunal a rejeté la demande pour des raisons de procédure et n'a pas examiné l'affaire au fond.

2.4.3. Confidentialité garantie aux plaignants

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

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

Si le plaignant exige l'**anonymat** envers l'institution, le DPD ou les tiers concernés, il est invité à en expliquer les raisons. Le CEPD analyse ensuite les arguments du plaignant et examine les conséquences pour la viabilité de son enquête future. Si le CEPD décide de ne pas accepter l'anonymat du plaignant, il explique pourquoi et demande au plaignant s'il accepte que le CEPD examine la réclamation sans garantir l'anonymat ou s'il préfère retirer sa réclamation. Si le plaignant décide de retirer sa réclamation, l'institution concernée ne sera pas informée de l'existence de cette dernière. Dans ce cas, le CEPD peut entreprendre d'autres actions en



Le CEPD garantit la confidentialité et l'anonymat aux plaignants et aux informateurs qui le demandent.

la matière, sans révéler à l'institution concernée l'existence de la réclamation. Il s'agit alors d'une enquête d'initiative ou d'une demande de notification d'un traitement de données.

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

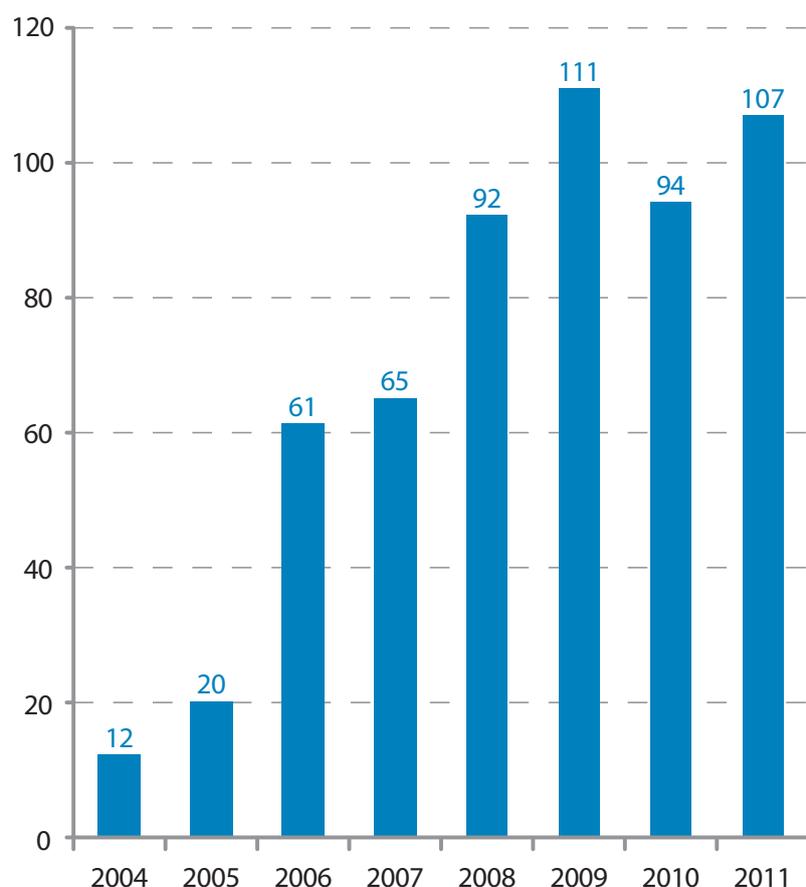
2.4.4. Réclamations traitées en 2011

2.4.4.1. Nombre de réclamations

Le nombre et la complexité des réclamations reçues par le CEPD ont augmenté en 2011. **En 2011, le CEPD a reçu 107 réclamations** (une hausse de 14 % par rapport à 2010). Sur ce total, **81 ont été jugées irrecevables**, la majorité portant sur un traitement au niveau national, et pas au niveau d'une institution ou d'un organe de l'UE.

Les 26 réclamations restantes ont nécessité une enquête approfondie (une hausse de 4 % par rapport à 2010). De plus, neuf réclamations recevables, déposées les années précédentes (une en 2008, cinq en 2009 et trois en 2010), en étaient toujours à la phase de l'enquête, de l'examen ou du suivi au 31 décembre 2011.

Nombre de réclamations reçues



2.4.4.2. Nature des plaignants

Sur les 107 réclamations déposées, 19 (18 %) ont été soumises par des membres du personnel des institutions ou organes de l'UE, y compris des anciens membres et des candidats. En ce qui concerne les 88 autres réclamations, le plaignant ne semblait pas avoir de lien professionnel avec l'administration de l'UE.

2.4.4.3. Institutions concernées par les réclamations

Sur les 26 réclamations recevables déposées en 2011, 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 de données à caractère personnel que les autres institutions et organes de l'UE. Le nombre relativement élevé de réclamations concernant l'OLAF et l'EPSO peut s'expliquer par la nature des activités exercées par ces organes.

2.4.4.4. Langue des réclamations

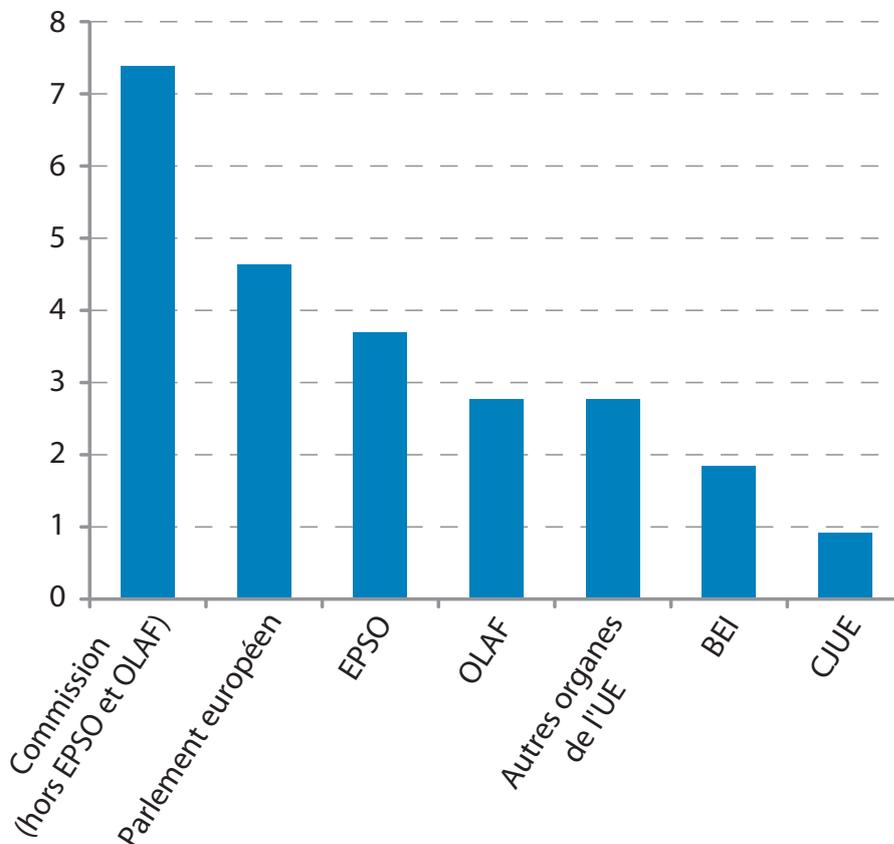
La majorité des réclamations ont été déposées en anglais (57 %), en français (20 %) ou en allemand (15 %). Les réclamations dans d'autres langues sont relativement rares (8 %).

2.4.4.5. Types de violations invoqués

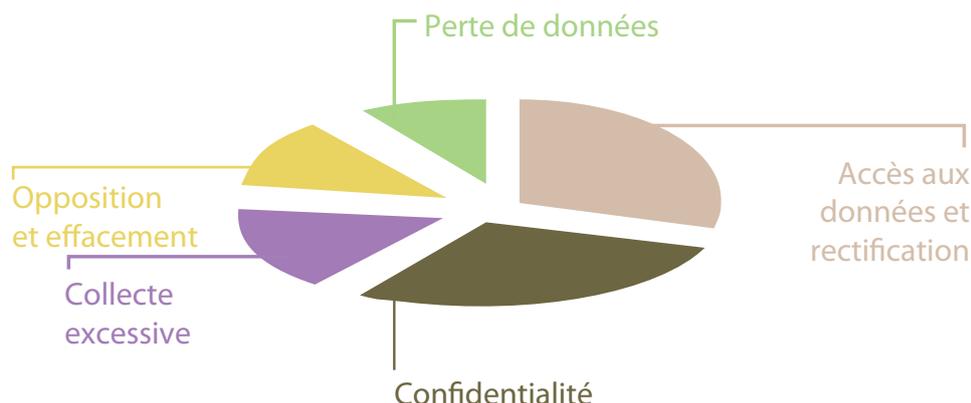
Les violations des règles en matière de protection des données alléguées par les plaignants en 2011 concernaient principalement:

- une atteinte aux droits des personnes concernées, comme les droits d'accès ou de rectification des données (30 %) ou le droit d'opposition et d'effacement (13 %);
- une violation de la confidentialité (30 %), une collecte excessive de données à caractère personnel (17 %) ou une perte de données (9 %).

Institutions et organes de l'Union concernés



Types de violations invoqués



2.4.4.6. Résultats des enquêtes du CEPD

Dans 15 affaires résolues courant 2011, 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 réclamation concernant le transfert, dans le cadre du départ d'un fonctionnaire vers une autre institution, du nombre de jours de congés de maladie pris au cours des trois dernières années. Le CEPD a confirmé qu'un tel transfert est bel et bien nécessaire pour que l'institution employant le fonctionnaire puisse remplir ses obligations en vertu de l'article 59, paragraphe 4, du statut des fonctionnaires. Le CEPD a dès lors conclu qu'il n'y avait pas violation des règles de protection des données dans cette affaire.

À l'inverse, dans deux dossiers, le CEPD a constaté un non-respect des règles de protection des don-

nées et a transmis des recommandations au responsable du traitement des données.

Le CEPD a reçu une réclamation alléguant que certains documents contenant des données à caractère personnel très sensibles concernant le plaignant et d'autres personnes avaient été accessibles à tout le personnel sur le serveur d'un organe de l'UE pendant plusieurs semaines. L'accès à ces documents n'a été limité par le responsable du traitement des données qu'après l'intervention du plaignant. Après avoir mené une enquête sur la question, le CEPD a conclu que la divulgation non autorisée des données à caractère personnel figurant dans les documents concernés constituait une violation de l'article 22 du règlement (CE) n° 45/2001. Afin de limiter le risque de voir une telle situation se reproduire à l'avenir, le CEPD a conseillé au responsable du traitement des données de mettre en œuvre un système complet de droits d'accès aux différentes parties du serveur.

Dans une affaire, le CEPD a conclu que le non-respect des règles relatives de protection des données n'était pas lié à une violation de ces règles par le responsable du traitement des données.

Un candidat participant à un concours de l'EPSO a déposé une réclamation ayant trait à la communication d'un document renfermant des données à caractère personnel sensibles par le jury du concours à une personne extérieure au concours. Après avoir mené une enquête, le CEPD a considéré que le responsable du traitement des données concerné avait adopté des mesures raisonnables pour éviter une telle divulgation non autorisée, notamment en faisant signer à tous les membres du jury une déclaration les informant explicitement de leurs obligations en matière de confidentialité. Le CEPD a conclu que la divulgation des données à caractère personnel était illégale et due à l'action individuelle d'un membre particulier du jury. Le CEPD a invité l'autorité investie du pouvoir de nomination à envisager une procédure disciplinaire à l'encontre du membre du jury concerné.

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, des contrôles ciblés** ont également été effectués dans les cas où, à la suite de ses activités de supervision, le CEPD avait des raisons de s'inquiéter du degré de conformité aux normes de certaines institutions ou certains organes. Certains de ces contrôles ont été réalisés **par correspondance**, tandis que d'autres ont pris la forme d'une **visite** d'une journée de l'organe concerné aux fins de remédier aux défauts de conformité. Enfin, des **inspections** ont été opérées dans certaines institutions et certains organes pour vérifier leur respect du règlement concernant des questions spécifiques.

2.5.1. Exercice général de contrôle et d'établissement de rapports: enquête 2011

Dans le document stratégique qu'il a adopté en décembre 2010⁶, le CEPD annonce qu'il «*continuera de mener ces «enquêtes» périodiques afin de garantir 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*».

⁶ Voir le document stratégique du CEPD du 13 décembre 2010, intitulé «Contrôler et garantir le respect du règlement (CE) n° 45/2001», p. 9.

En avril 2011, le CEPD s'est lancé dans son troisième bilan général. L'exercice a eu un champ d'application étendu puisqu'il concernait six institutions de l'UE et 52 organes de l'UE, et il s'est concentré sur les aspects donnant une bonne indication des progrès accomplis par les institutions et organes dans la mise en œuvre du règlement. Les conclusions de cet exercice ont été rassemblées dans un rapport.

L'analyse et le rapport se sont fondés sur les réponses aux lettres du CEPD soulevant des questions particulières reçues de la part des institutions et organes de l'UE (y compris des organes des anciens deuxième et troisième piliers) avant septembre 2011. La teneur des lettres du CEPD varie légèrement en fonction du statut des institutions et organes, c'est-à-dire, nouveaux ou anciens et ayant ou non désigné un délégué à la protection des données (DPD).

Les réponses ont été présentées dans des tableaux comparatifs, par groupes d'institutions et d'organes. Sur la base des résultats de chaque groupe, des **références** ont été établies afin de fournir une indication du seuil qu'une institution ou un organe du groupe concerné devrait raisonnablement pouvoir atteindre. Le CEPD a établi ces références de manière concrète, à la lumière des faits, pour permettre d'effectuer une **comparaison entre pairs**.

Cette enquête générale a été rendue publique dans le cadre de la politique de mise en application du CEPD. Elle a mis l'accent sur les progrès accomplis par les institutions et organes, tout en soulignant également leurs lacunes en matière de conformité.

Le CEPD tiendra compte des conclusions de cet exercice pour planifier ses futures activités de supervision et de mise en application. Ce programme associera des **orientations** à l'intention des institutions

et organes, des **actions de mise en application** et des mesures visant à encourager la **responsabilisation**. Le CEPD a notamment planifié des visites de conformité suscitées par un **manque d'engagement manifeste de la part d'une institution ou d'un organe** sur la base des résultats de l'exercice 2011.

2.5.2. Contrôles ciblés

Visite médicale d'embauche effectuée par le service médical du Parlement (dossier 2010-0279)

Courant 2010, plusieurs membres du Parlement européen ont soulevé des questions concernant l'utilisation appropriée du questionnaire médical pour les assistants parlementaires accrédités, dans le cadre de la visite médicale d'embauche. Le 17 mars 2011, le CEPD a effectué une enquête dans l'objectif d'obtenir des informations sur les pratiques du service médical du Parlement en la matière.

Après avoir analysé les informations recueillies au cours de l'enquête, le CEPD a conseillé au service médical du Parlement d'indiquer clairement aux assistants accrédités:

- le statut du questionnaire médical, à savoir que toutes les questions sont en principe considérées comme nécessaires et pertinentes et que, dans l'éventualité où une personne ne souhaite pas répondre à certaines questions, les médecins détermineront, de manière empirique et sur la base de l'examen médical, quelles informations sont pertinentes ou non, et
- les conséquences d'un refus de répondre aux questions jugées nécessaires par les médecins et de se présenter à la visite médicale d'embauche.

Deuxièmement, le CEPD a conseillé au service médical d'établir, à l'intention de tous les acteurs du service médical, une politique documentée sur la collecte de données dans le cadre de la visite médicale d'embauche.

Dans le cadre du suivi, le CEPD a considéré que le dossier était clos pourvu que le Parlement communautaire officiellement la politique documentée à tous les acteurs de son service médical et qu'il garantisse l'application rigoureuse de ces orientations.

Visites de plusieurs agences

Entre janvier et septembre 2011, à la suite d'un certain nombre de questions repérées dans le cadre de son bilan de 2009 et de son suivi, le CEPD a visité plusieurs agences de l'UE afin d'aborder et de mieux comprendre leur faible degré de respect du règlement relatif à la protection des données. Parmi ces agences, on peut citer l'Agence ferroviaire européenne, l'Office communautaire des variétés végétales, la Fondation européenne pour l'amélioration des conditions de vie et de travail et l'Agence du système global de navigation par satellite européen.

Les visites ont suivi un déroulement similaire:

- une réunion entre le contrôleur ou le contrôleur adjoint et le directeur de l'agence;
- d'autres réunions rassemblant le délégué à la protection des données et les responsables du traitement;
- des présentations sur le règlement relatif à la protection des données et l'approche du CEPD quant au contrôle et à la garantie du respect du règlement.

Ces réunions ont offert au CEPD la possibilité de soulever certaines préoccupations et permis aux agences de fournir des mises à jour sur leurs progrès vers le respect du règlement.

À la fin de chaque visite, une feuille de route spécifique a été convenue, détaillant les actions prioritaires à adopter par l'agence, sous le contrôle du CEPD, afin d'assurer un degré plus élevé de respect du règlement. En général, les agences visitées ont réalisé des efforts satisfaisants. Des organes qui présentaient un taux de notifications au titre de l'article 25 proche de 0 atteignent à présent un niveau de 60, 70, 80 et, dans un cas, 100 %. En outre, chaque organe dispose maintenant d'un inventaire intelligible et de bonne qualité.

2.5.3. Inspections

Les inspections constituent un 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.

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

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

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

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

En 2011, le CEPD a procédé au suivi des inspections antérieures. En mai 2011, le CEPD a effectué une inspection au CEDEFOP et à l'OLAF. Il a également réalisé des inspections ciblées, à la suite d'une réclamation, à la BCE en octobre 2011 et à l'OLAF en décembre 2011.

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

À la suite de son inspection sur place au Centre commun de recherche d'Ispra, fin 2010, le CEPD a adopté un rapport d'inspection concernant 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 2011, le CCR a adopté plusieurs mesures visant à harmoniser ses traitements avec le règlement relatif à la protection des données, sur la base du rapport d'inspection adopté par le CEPD. Il doit cependant



Les inspections constituent un instrument fondamental pour le CEPD dans son rôle d'autorité de supervision.

accentuer ses efforts en vue d'instaurer des mesures supplémentaires pour garantir la conformité. Le CEPD devrait conclure cet exercice en 2012.

Inspection au CEDEFOP

Le CEPD a effectué une inspection sur place au Centre européen pour le développement de la formation professionnelle (CEDEFOP) à Thessalonique le 31 mai et le 1^{er} juin 2011. Cette inspection s'inscrivait dans le plan d'inspection annuel 2011 du CEPD, sur la base d'un exercice d'évaluation interne des risques. L'inspection a porté sur trois domaines principaux: les procédures de recrutement de personnel, avec l'accent sur les pratiques actuelles et futures, le contrôle de l'accès aux locaux gérés par les services de sécurité et le registre et inventaire des notifications.

Des cas de contrôle préalable ou l'analyse de cas de consultation ont fourni des informations de référence pour l'inspection. Sur la base de ses conclusions, le CEPD a élaboré un rapport d'inspection comportant des recommandations en vue de mieux assurer le respect du règlement européen sur la protection des données. Le CEDEFOP a donné un suivi au rapport d'inspection et a présenté des mesures correctives et des commentaires concernant les recommandations du CEPD. Ce dossier devrait être clos au cours du premier trimestre 2012.

Inspection à l'OLAF

Les 14 et 15 juillet 2011, le CEPD a effectué une inspection sur place dans les locaux de l'OLAF. Cette inspection a été entreprise sur la base de l'article 47, paragraphe 2, du règlement, à la suite de plusieurs avis du CEPD concernant les enquêtes externes et internes et le contrôle d'accès physique et logique

de l'OLAF. L'enquête s'est particulièrement concentrée sur l'identification des personnes concernées, le respect de l'obligation d'informer les personnes concernées et le respect des obligations de protection des données en matière de transferts. Le 12 octobre 2011, le CEPD a adopté un rapport final d'inspection, dans lequel il a formulé plusieurs recommandations que l'OLAF devrait commenter d'ici le début de l'année 2012.

Inspection à la Banque centrale européenne

En octobre 2011, le CEPD a effectué une inspection à la Banque centrale européenne (BCE). Cette inspection s'est déroulée dans le cadre d'une enquête sur la protection des données à caractère personnel au cours des enquêtes administratives internes. L'inspection a consisté en une vérification sur place de plusieurs dossiers concernant des enquêtes internes au cours desquelles la BCE a accédé aux fichiers électroniques ou aux données du trafic. Après l'inspection, plusieurs questions complémentaires concernant l'application et les principes de la circulaire administrative n° 01/2006 de la BCE relative aux enquêtes administratives internes ont été adressées à la BCE. L'enquête n'est pas encore terminée.

Inspection ciblée à l'OLAF

En octobre 2009, le CEPD a reçu deux réclamations à l'encontre de l'OLAF, concernant la collecte et le traitement ultérieur de données à caractère personnel dans le cadre d'une enquête externe sur la société qui employait les plaignants. Après avoir soigneusement analysé les réclamations et les réponses pertinentes de l'OLAF, le CEPD a décidé d'effectuer une visite sur place dans les locaux de l'OLAF en décembre 2011. La visite avait pour objectif d'éclaircir des questions liées à la proportionnalité de la collecte de preuves numériques renfermant des données à caractère personnel par l'OLAF, au moyen d'outils d'identification criminelle (par exemple, copie ou saisie de disques durs).

La visite visait à évaluer la procédure générale par rapport à la collecte et au traitement ultérieur des preuves numériques avant, pendant et après une enquête externe de l'OLAF, notamment en accédant au matériel pertinent dans le laboratoire d'analyse judiciaire de l'OLAF. Les informations obtenues au cours de la visite serviront à finaliser la décision du CEPD au sujet des réclamations susmentionnées.

Système d'information sur les visas

Le système d'information sur les visas (VIS) permet aux États membres de la zone Schengen d'échanger des données concernant les visas de courte durée. Ce système a été créé par la décision 2004/512/CE du Conseil du 8 juin 2004 et le règlement (CE) n° 767/2008 du Parlement européen et du Conseil du 9 juillet 2008. Il permet aux autorités compétentes des États membres d'échanger des données concernant les demandes de visa et les visas émis, refusés, annulés, révoqués ou prolongés. Des données biométriques sont traitées dans le cadre du fonctionnement du VIS.

Le règlement (CE) n° 767/2008 prévoit une supervision conjointe entre les autorités nationales chargées de la protection des données et le CEPD. Il prévoit notamment que le CEPD effectue tous les quatre ans une vérification des activités de traitement des données réalisées dans l'unité centrale et l'infrastructure de communication. Afin de mener cette mission à bien, le CEPD a procédé à deux visites sur place, une en juillet et une en novembre 2011. Le calendrier des visites a été choisi afin de fournir des orientations avant le lancement du système et de vérifier les mesures de sécurité mises en place. La visite de novembre a donc donné au CEPD un point de référence auquel comparer les inspections à venir.

2.6. Consultations relatives aux mesures administratives

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

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

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

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

Dans le cadre des consultations menées sur des mesures administratives envisagées par une institution ou un organe, plusieurs questions ont été examinées en 2011. Les sous-points suivants rendent compte de certains de ces dossiers.

2.6.1.1. Publication des photos des employés sur l'intranet

Le projet «Who is who» du Comité des Régions prévoyait d'afficher une photo des membres du personnel du Comité en sus de leurs fonctions et responsabilités sur l'intranet. À cette fin, le secrétaire général comptait envoyer un message Outlook aux membres du personnel, les informant de ce nouveau projet et de la **possibilité de refuser** la publication de leur photo en cliquant sur l'icône «Non, je ne veux pas que ma photo soit publiée».

Dans sa réponse à la consultation, le CEPD a souligné que le **«consentement indubitable»** en vertu de l'article 5, point d), du règlement implique que dans chaque cas particulier, la personne concernée devrait donner son consentement librement et en pleine connaissance de cause. Le système proposé n'offrait pas la certitude totale que malgré l'absence d'action spécifique de sa part, le membre du personnel avait réellement l'intention de voir sa photo publiée. Les personnes concernées doivent être en position d'avoir pleinement conscience qu'elles donnent leur consentement et de ce à quoi elles consentent. Le système le plus approprié pour obtenir le consentement est donc le **mécanisme d'accord préalable**, requérant du membre du personnel une action affirmative pour marquer son consentement avant la publication de sa photo.

Le CEPD a dès lors recommandé que le membre du personnel puisse donner son consentement en cliquant sur une icône indiquant, par exemple, «Oui, je souhaite que ma photo soit publiée». Le CEPD a également conseillé au Comité de préciser aux membres du personnel qu'ils sont entièrement libres de donner ou de refuser leur consentement.

2.6.1.2. Rôle d'une agence dans un projet de recherche (notion de responsable du traitement)

L'Agence européenne des médicaments (EMA) a consulté le CEPD sur certaines questions juridiques soulevées par sa participation à une étude clinique dans le cadre d'un projet de recherche européen. Le projet est mené par un consortium de 29 membres, dont l'EMA assure la coordination.

En particulier, le délégué à la protection des données de l'Agence a demandé si l'EMA pouvait être considérée comme un **«responsable du traitement conjoint»** avec tous les autres participants au projet de recherche, et si le traitement de données à caractère personnel aux fins de l'étude clinique relevait du champ d'application du règlement. Le 21 mars 2011, le CEPD a adopté un avis soulignant les aspects suivants de la notion de «responsable du traitement»:

- Bien que l'EMA ait précisé que les objectifs et les moyens du traitement des données étaient définis par un comité directeur, le CEPD a estimé que, dans ce cas, **la notion de «responsable du traitement» devait être analysée par rapport à l'ensemble du consortium.**
- Le CEPD a considéré que tous les membres du consortium décidaient en commun de la conduite de l'étude. Le CEPD n'était pas en mesure d'évaluer spécifiquement la mesure dans laquelle les membres du consortium, individuellement ou ensemble, contrôlaient le traitement. Le CEPD a centré son analyse sur les responsabilités de l'EMA, qui doit être considérée comme l'un des responsables du traitement.

2.6.1.3. Système de télévision en circuit fermé (CCTV) exploité dans les locaux d'une autre institution

L'Agence exécutive du réseau transeuropéen de transport (TEN-T EA) a consulté le CEPD sur la question de la relation entre responsable du traitement et sous-traitant lorsque le système de télévision en circuit fermé (CCTV) d'une agence est exploité par une autre institution. Le système de vidéosurveillance de l'agence est conçu, installé, exploité et géré par la Commission sur la base d'un «accord de niveau de service».

Le CEPD a répondu le 28 juillet 2011, rappelant l'avis 1/2010 du groupe de travail «Article 29» sur la

protection des données concernant les notions de «responsable du traitement» et de «sous-traitant» et soulignant que la notion de **responsable du traitement est fonctionnelle**, car elle vise à attribuer les responsabilités aux personnes qui exercent une influence de fait. Il a également précisé que, en cas de doute, des éléments tels que le degré de contrôle réel exercé par une partie, l'image donnée aux personnes concernées et les attentes raisonnables que cette visibilité peut susciter chez ces dernières peuvent servir à identifier le responsable du traitement.

Selon les faits, il est apparu que la Commission ne jouait pas simplement un rôle de sous-traitant et que son rôle s'apparentait davantage à celui d'un responsable du traitement. Cependant, le CEPD a signalé que l'agence ne pouvait s'exonérer de ses responsabilités de responsable du traitement au motif qu'elle était obligée de conclure un contrat avec la Commission, dont les services sont standard et proposés à tous ses partenaires.

L'Agence devrait agir avec la diligence requise pour examiner les pratiques concernées de la Commission, communiquer les pratiques de la Commission aux membres de son personnel et aux visiteurs, et soulever avec la Commission (et en dernier ressort avec le CEPD, si la légalité est en jeu) toute préoccupation qu'elle pourrait avoir concernant la légalité ou la personnalisation des services de la Commission si elle le juge nécessaire.

2.6.1.4. *Traitement des données figurant dans les courriers électroniques des employés*

La Cour de justice de l'Union européenne (CJUE) a consulté le CEPD sur des questions générales concernant le traitement de données lié à la fourniture d'un service de messagerie électronique aux employés. Le CEPD a répondu le 2 septembre 2011, soulignant les questions suivantes:

- La fourniture d'un service de messagerie électronique aux employés constitue un **traitement de données à caractère personnel** en vertu du règlement. Les employeurs doivent respecter les exigences juridiques du règlement, ainsi que le principe de confidentialité des communications conformément à l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et à l'article 7 de la Charte des droits fondamentaux de l'UE.
- Même si la CJUE peut désigner spécifiquement un service particulier (par exemple, l'unité de l'informatique) responsable au premier chef et interlocuteur privilégié pour ce traitement, c'est elle qui sera finalement considérée comme **responsable du traitement**.



La vidéosurveillance doit être utilisée de façon responsable et avec des mesures de sauvegarde effectives.

- Il appartient au responsable du traitement de définir les modalités applicables au traitement des données à caractère personnel dans le cadre de l'utilisation de la messagerie électronique, et de **communiquer de façon transparente** ces modalités aux usagers. Le CEPD recommande l'adoption de «**règles régissant l'utilisation de la messagerie électronique**», définissant l'objectif et les modalités du traitement. Il appartient au responsable du traitement de s'assurer que le traitement est nécessaire et que les mesures adoptées conformément à cet objectif sont proportionnelles. Les règles doivent être portées à l'attention de tous les usagers, éventuellement au terme d'une consultation des représentants du personnel.

De telles règles régissant l'utilisation de la messagerie électronique devraient notamment définir:

- le ou les **objectif(s) du traitement des données à caractère personnel** réalisé dans le cadre de l'utilisation de la messagerie électronique. L'objectif doit être légitime (par exemple, assurer le fonctionnement et la sécurité d'un système de courrier électronique, et non pas contrôler l'utilisation du système dans un cas particulier);
- les modalités applicables à **l'usage privé de la messagerie électronique** (par exemple, obligation d'indiquer clairement le caractère privé de la correspondance dans l'objet du message ou le dossier d'archivage);
- le ou les **délai(s) de conservation** des messages et des copies de sauvegarde dans le système, en accord avec le principe de proportionnalité. Il est également conseillé de préciser le délai après lequel les courriers électroniques sont définitivement supprimés du serveur;
- les différents types de **mesures de sécurité** mises en place;
- les **droits d'accès** établis pour permettre au personnel du service informatique de garantir le fonctionnement correct du système de courrier électronique;
- les **mesures de contrôle** mises en place par les responsables du traitement, qui doivent être proportionnelles à l'objectif du traitement et transparentes pour les usagers (pas de contrôle silencieux de l'utilisation de la messagerie électronique). Dans ce contexte, le CEPD a attiré l'attention sur les orientations fournies dans le



L'utilisation de courriers électroniques implique un traitement de données.

document de travail concernant la surveillance des communications électroniques sur le lieu de travail publié par le groupe de travail «Article 29»⁷.

2.6.1.5. Utilisation des données statistiques d'une base de données à des fins d'évaluation du personnel

L'Agence ferroviaire européenne (ERA) a consulté le CEPD concernant son intention d'utiliser des **données statistiques sur le nombre d'opérations financières validées dans le système ABAC** («*Accrual Based ACcounting*») aux fins d'évaluer les acteurs financiers.

Les informations concernant le nombre réel de transactions validées par chaque agent sont disponibles en ligne dans le système ABAC. Elles figurent également dans les rapports de la société Business Object.

Dans sa réponse du 5 mai 2011, le CEPD a considéré que l'ERA n'avait pas réussi à démontrer la nécessité d'utiliser les données ABAC à des fins d'évaluation du personnel, étant donné notamment que l'agence collecte déjà des données destinées à l'évaluation dans les rapports d'évolution de carrière. En outre, aucun des instruments juridiques existants ne prévoit le traitement de ces données à cette fin. En vertu de l'article 6, paragraphe 1, du règlement, le traitement des données à des fins autres que celles pour lesquelles elles ont été recueillies doit être expressément autorisé par le règlement intérieur de l'institution ou de l'organe concerné(e). Par conséquent, le règlement intérieur devrait expressément autoriser l'utilisation des données recueillies pour la comptabilité aux fins d'évaluer certains agents financiers.

⁷ Disponible à l'adresse http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_fr.pdf



Les statistiques peuvent inclure des données à caractère personnel.

Le CEPD a également demandé qu'une notification en vue d'un (vrai) contrôle préalable soit soumise en temps utile avant l'introduction de cette nouvelle procédure.

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 au personnel du CEPD de traduire son expertise en une orientation générale pour les institutions et organes. En 2011, ces orientations ont pris la forme d'une formation à l'intention des nouveaux DPD ou des responsables du traitement, ou de lignes directrices thématiques dans le domaine de l'évaluation du personnel et du traitement des données à caractère personnel dans les procédures anti-harcèlement. Le CEPD travaille actuellement sur des lignes directrices pour les absences et les congés, la passation des marchés et la sélection des experts, l'e-monitoring et les transferts de données.

2.7.1. Lignes directrices thématiques

Lignes directrices relatives aux procédures anti-harcèlement

En février 2011, le CEPD a publié des lignes directrices sur la façon de gérer le traitement des données à caractère personnel dans les procédures de harcèlement. Plus spécifiquement, ces lignes directrices traitent de la procédure informelle mise en place par les institutions et organes communautaires pour combattre - mais aussi prévenir - le harcèlement. La sélection des conseillers confidentiels, qui jouent un rôle clé dans cette procédure, est également abordée dans ce document.

La confidentialité qu'attend la personne concernée est la pierre angulaire de la procédure informelle. Du point de vue de la protection des données, la difficulté consiste à assurer la **confidentialité des données** tout en permettant de prévenir les cas de harcèlement. Les lignes directrices font donc la distinction entre les données 'tangibles' (objectives), qui peuvent être structurellement transférées au service des ressources humaines dans certaines circonstances pour faciliter l'identification des cas récurrents et multiples, et les données 'intangibles' (subjectives), qui ne peuvent jamais être structurellement transférées pour préserver le caractère confidentiel de la procédure.

Le CEPD insiste également sur les principes du droit d'accès aux données de la personne concernée et de son droit à l'information. Compte tenu du principe de proportionnalité, les restrictions à ces droits s'appliquent au cas par cas.

Ces lignes directrices devront être utilisées par les agences dans leur notification au CEPD de procédures dans ce domaine en vue d'un contrôle préalable, mais elles devront également servir de guide pratique pour toutes les institutions et tous les organes. Le 21 octobre 2011, le CEPD a rendu un avis conjoint sur les notifications présentées par neuf agences en vue d'un contrôle préalable à la lumière de ces lignes directrices.

Lignes directrices relatives à l'évaluation du personnel

En juillet 2011, le CEPD a publié des lignes directrices relatives au traitement des données à caractère personnel dans le domaine de l'évaluation du personnel par les institutions et organes de l'UE.

Ces lignes directrices ont pour objectif d'offrir des conseils pratiques et une assistance à tous les délégués à la protection des données et responsables du traitement dans leur mission de notification des traitements de données existants et/ou futurs au CEPD dans les procédures réglementaires suivantes:

- l'évaluation annuelle / le rapport d'évolution de carrière (REC),
- la période probatoire,
- la promotion des fonctionnaires,
- le reclassement des agents temporaires,
- l'évaluation de la capacité à travailler dans une troisième langue avant la première promotion,
- le reclassement ou le renouvellement d'un contrat pour une durée indéterminée,
- la certification des fonctionnaires AST, et
- «l'attestation» des anciens fonctionnaires C et D.

Le réseau des DPD a été consulté sur le projet de lignes directrices en mai 2011, et une présentation des lignes directrices a été réalisée à l'occasion de la réunion des DPD, en octobre 2011.

Dans les lignes directrices, le CEPD a exprimé sa préoccupation quant au long délai de conservation des données à caractère personnel figurant dans l'évaluation annuelle et les rapports de stage, ainsi que dans les pièces justificatives concernant d'autres procédures d'évaluation conservées dans les dossiers du personnel. Il a recommandé que les délais dépassant la carrière des membres du personnel concernés soient réexaminés et a conseillé comme bonne pratique un délai maximal de cinq ans après un exercice d'évaluation donné.

Le CEPD a demandé aux DPD de lui soumettre toute notification en suspens avant le 21 octobre 2011. À la fin du mois de décembre 2011, il avait reçu 43 notifications de 21 institutions et organes, concernant 57 procédures d'évaluation. Il a l'intention de traiter toutes les procédures d'évaluation concernées, par institution ou organe de l'UE, dans un avis conjoint.

Rapport de suivi sur les lignes directrices en matière de vidéosurveillance

En mars 2010, le CEPD a publié des **lignes directrices en matière de vidéosurveillance**⁸ en vertu des pouvoirs qui lui sont conférés à l'article 47, paragraphe 1, point a), du règlement (CE) n° 45/2001.

Le rapport de suivi, rédigé courant 2011 et publié début 2012, est une analyse systématique et comparative des rapports d'activité adressés au total par 42 institutions et organes de l'UE. En plus de reconnaître les bonnes pratiques, ce rapport souligne les lacunes des institutions et organes qui sont en retard dans leurs efforts visant à garantir le respect des lignes directrices. En outre, il clarifie certains aspects des lignes directrices, lorsque les organes ont soulevé des questions dans le cadre de l'élaboration de leur politique de vidéosurveillance ou que l'analyse des rapports sur l'état d'avancement a mis en évidence un besoin de clarification.

Dans le rapport, le CEPD prend note des efforts considérables réalisés par les institutions et organes qui ont présenté leur rapport sur l'état d'avancement en 2011 et est généralement assuré que les lignes directrices ont contribué à accroître le niveau de sensibilisation et de transparence en matière de vidéosurveillance au sein des institutions et organes de l'UE.

⁸ http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_FR.pdf.

Cependant, plus d'un an après l'adoption des lignes directrices et près de deux ans après le début du processus de consultation, le CEPD est déçu de constater que la mise en œuvre des lignes directrices a été mise en attente ou considérablement retardée dans plusieurs institutions et organes.

2.7.2. Formation

À la suite de sa visite de l'ENISA, en septembre 2010, le CEPD a organisé une session de formation à l'intention du personnel de l'ENISA le 10 février 2011. Il a donné des conseils pratiques sur «la sélection et le recrutement du personnel». Ce thème a été choisi parce qu'un suivi de contrôle préalable était en cours et que le CEPD avait déjà publié des lignes directrices thématiques sur le sujet. Le personnel des ressources humaines, le DPD, le directeur et le chef de l'administration ont participé à la session de formation.

Le 8 juin 2011, le CEPD a organisé un atelier d'une journée sur la protection des données, à l'intention des délégués à la protection des données de toutes les institutions et de tous les organes de l'UE. L'objectif était d'offrir une formation de base aux DPD, en particulier ceux qui avaient été récemment nommés. L'atelier a commencé par une introduction aux principes et définitions essentiels du règlement. La session suivante incluait des présentations

sur des questions juridiques (par exemple, la base juridique du traitement de données, les droits des personnes concernées, le transfert de données et le traitement pour le compte du responsable du traitement). La session de l'après-midi a été consacrée à la coopération entre les DPD et le CEPD, avec un accent sur les aspects pratiques du traitement des réclamations, les procédures de contrôle préalable et la sécurité des traitements.

Cet atelier a été largement suivi et la participation active des DPD a favorisé un échange productif d'expériences et de préoccupations. Le CEPD s'appuiera sur cette expérience et, d'après les commentaires reçus, organisera un atelier similaire à l'intention des coordinateurs de la protection des données en 2012.

En novembre 2011, le personnel du CEPD a proposé une formation à l'occasion du Forum des auditeurs, une conférence mensuelle destinée aux auditeurs internes de la Commission européenne. La présentation comprenait une introduction générale à la protection des données et au respect des règles de protection des données par les services d'audit interne dans l'exercice de leurs fonctions. La formation a réuni beaucoup de participants de la Commission et a également été suivie par vidéoconférence par les services d'audit interne de la Cour des comptes européenne, de la Cour de justice de l'Union européenne et de la Banque centrale européenne.



Les institutions et organes de l'UE traitent des données à caractère personnel au cours des procédures d'évaluation du personnel.

À la demande du DPD de l'Agence exécutive du réseau transeuropéen de transport, le personnel du CEPD a proposé une formation générale sur la protection des données et le règlement au personnel de l'Agence exécutive du réseau transeuropéen de transport le 1^{er} décembre 2011. La première session a été consacrée à la protection des données et aux principes fondamentaux du règlement. Elle a été suivie par une présentation de la politique de mise en application du CEPD et par une séance de questions-réponses. La formation a réuni beaucoup de participants du personnel de l'Agence exécutive du réseau transeuropéen de transport.

3

POLITIQUE LÉGISLATIVE ET CONSULTATION

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

En 2011, la Commission a publié de nombreuses propositions législatives ayant une incidence sur la protection des données et a réalisé des avancées importantes vers un nouveau cadre juridique, général et exhaustif, de protection des données en Europe.

Les travaux en cours concernant la nouvelle législation relative à la protection des données se sont poursuivis du début à la fin de l'année 2011: le 14 janvier, le CEPD a publié son avis sur la communication de la Commission intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne». En décembre, il a présenté à la DG Justice, qui est responsable du nouveau cadre juridique, des observations informelles sur des projets de propositions. Dans les deux cas, le CEPD a apporté une contribution importante à la procédure législative. Il continuera de le faire en 2012.

Ce projet constituait l'une des priorités du CEPD en 2011 et il le sera encore dans les années à venir, au fur et à mesure de l'évolution de la procédure législative: une fois que la Commission aura présenté sa proposition et la communication l'accompagnant en 2012, le CEPD formulera un avis. Ensuite, les discussions se poursuivront au Parlement européen et au Conseil.

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 ou les transferts de données internationaux, de nouveaux domaines émergent progressivement. En 2011, plusieurs avis ont été rendus sur des questions concernant le marché intérieur, les programmes de contrôle de la pêche et les programmes de soutien à l'agriculture.

Concernant **l'espace de liberté, de sécurité et de justice**, la question de la nécessité a été un thème récurrent. À de nombreuses reprises, le CEPD a rendu des avis dans lesquels ce principe de protection des données a occupé une place importante. Cela a été le cas pour le rapport d'évaluation sur la directive sur la conservation des données, la communication sur la migration et la proposition en vue d'un programme européen sur les données des dossiers passagers.

La nécessité est une notion essentielle dans le cadre de la protection des données. Il s'agit d'une norme plus stricte que la simple norme d'«utilité»: une mesure ne peut être considérée comme nécessaire que s'il n'est pas possible d'obtenir les mêmes résultats avec des moyens moins intrusifs. Cette norme doit être appliquée avec la plus grande rigueur, particulièrement lors de l'évaluation de mesures existantes. Ce niveau de preuve est inscrit dans le droit européen et a été largement appliqué par la Cour de justice de l'Union européenne au Luxembourg, ainsi que par la Cour européenne des droits de l'homme à Strasbourg, généralement en liaison étroite avec la norme de proportionnalité.

Les données des dossiers passagers ont également constitué un thème récurrent lorsque le CEPD a été consulté sur des initiatives dans le domaine de l'application du droit international et de la coopération en matière de sécurité. Il a rendu des avis sur les propositions d'accords avec les États-Unis et l'Australie.

Le nombre croissant d'avis liés au **marché intérieur** est un nouveau développement. Entre autres, le CEPD a adopté un avis sur le système d'information du marché intérieur et les produits dérivés négociés de gré à gré.

Autre élément nouveau, le CEPD a publié son premier **avis sur les activités de recherche financées par l'UE**, donnant des conseils concernant les activités européennes de recherche et de développement. Cet avis a appliqué le document stratégique «Le CEPD et la recherche et le développement technologique dans l'UE».

La large gamme des questions abordées dans le cadre des activités consultatives du CEPD démontre que le traitement des données à caractère personnel et la protection des données sont réellement devenus des questions horizontales qui ne peuvent être limitées à des domaines politiques spécifiques. Au contraire, elles revêtent un caractère transversal qui justifie le rôle du CEPD en tant que conseiller compétent des institutions de l'UE.

Le présent chapitre du rapport annuel ne met pas uniquement l'accent sur la consultation législative: il aborde également les relations entre le CEPD et les juridictions de l'UE et la surveillance des nouveaux développements par le CEPD, notamment dans le domaine des nouvelles technologies. La coopération avec les APD, y compris la supervision conjointe des systèmes d'information à grande échelle, est abordée au chapitre 4.

3.2. Cadre d'action et priorités

3.2.1. Mise en œuvre de la politique de consultation

Même si les méthodes de travail du CEPD dans le domaine de la consultation ont évolué au fil des ans, les approches fondamentales des interventions n'ont pas changé. Le document stratégique adopté en mars 2005 et intitulé «Le CEPD en tant que conseiller des institutions communautaires à l'égard

des propositions de législation et documents connexes»⁹ reste d'actualité, bien qu'il faille désormais le lire à la lumière du traité de Lisbonne.

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

Les consultations législatives fondées sur l'article 28, paragraphe 2, du règlement (CE) n° 45/2001, constituent l'élément central du rôle consultatif du CEPD. Selon cet article, la Commission consulte le CEPD lorsqu'elle adopte une proposition législative ayant trait à la protection des droits et libertés des individus. Les avis du CEPD donnent une analyse complète des aspects liés à la protection des données d'une proposition ou d'un autre texte.

En règle générale, le CEPD ne formule des avis sur les textes non législatifs (comme les documents de travail, communications ou recommandations de la Commission) que lorsque la protection des données en est un élément important. Il rédige occasionnellement des commentaires par écrit à des fins plus limitées, afin de faire passer un message rapide et fondamental, de se concentrer sur un ou plusieurs aspects techniques, voire même de synthétiser ou de répéter des observations antérieures. Par exemple, le CEPD a rédigé deux lettres ayant trait à plusieurs propositions législatives concernant des mesures restrictives car les questions de protection des données figurant dans ces propositions étaient essentiellement similaires à celles traitées dans des avis précédents.

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

Le CEPD est à la disposition des institutions de l'UE à tous les stades de l'élaboration des politiques et du processus législatif et utilise toute une série

⁹ Disponible sur le site internet du CEPD, sous Publications > Documents.

d'autres instruments dans son rôle consultatif. Même s'il doit pour cela entretenir des contacts étroits avec les institutions, il est essentiel qu'il conserve son indépendance.

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 notamment le cas des projets à long terme, comme la réforme du cadre juridique de l'OLAF, à laquelle le CEPD a 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 est généralement envoyé au CEPD au cours de la consultation inter-services, c'est-à-dire avant sa publication. Ces observations informelles, au nombre de 41 en 2011, 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

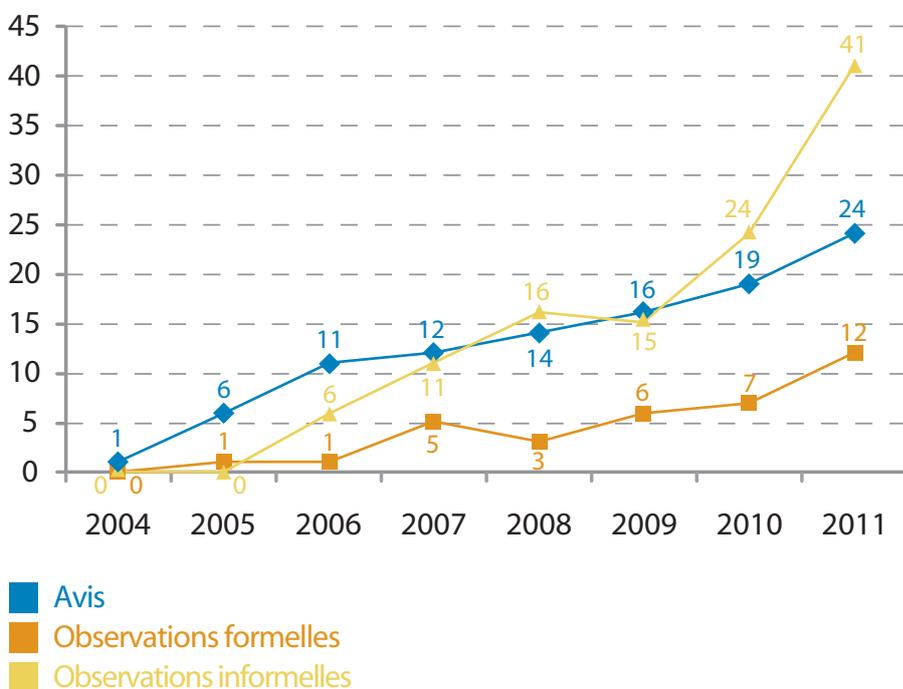
de garantir que les principes de protection des données sont dûment pris en considération au moment de la rédaction d'une proposition législative, et il est très souvent possible de résoudre des problèmes cruciaux à cette étape. En règle générale, ces observations informelles ne sont pas rendues publiques. Si elles sont suivies par un avis ou des observations formelles, ces documents mentionnent généralement le fait que des observations informelles ont été présentées auparavant.

Des contacts réguliers avec les services de l'institution concernée auront lieu après la publication d'observations ou d'avis du CEPD. Dans certains cas, le CEPD et son personnel sont 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 2011

En 2011, la hausse régulière du nombre d'avis rendus s'est maintenue. Le CEPD a rendu 24 avis, 12 observations formelles et 41 observations informelles sur toute une série de thèmes.

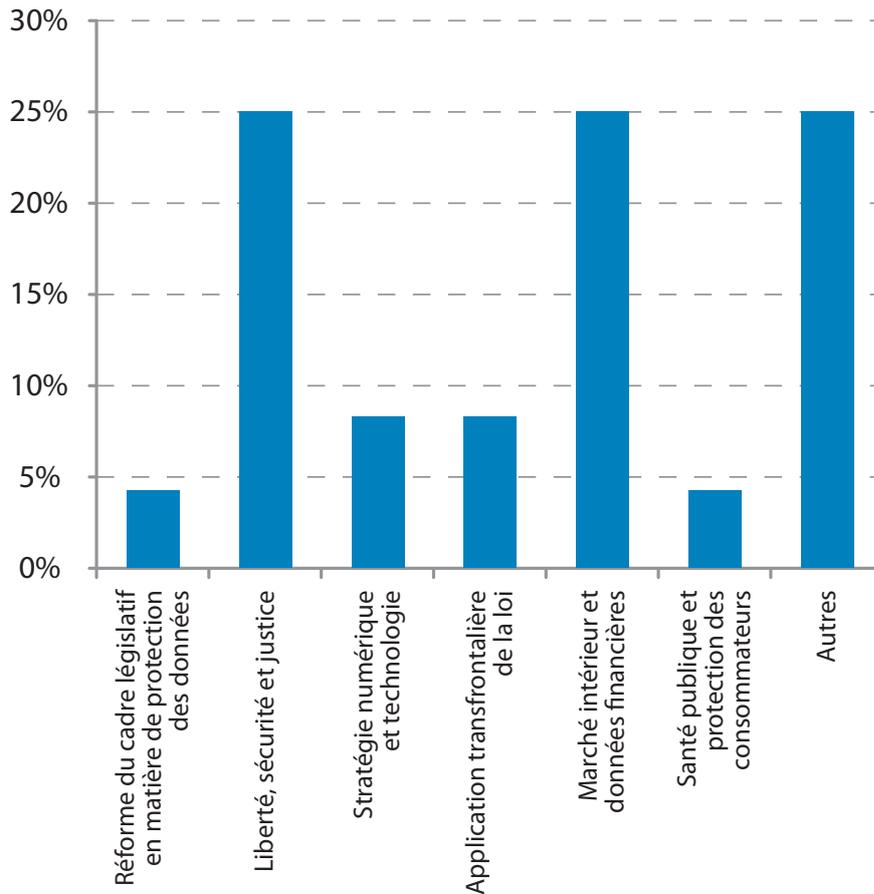
Évolution des avis législatifs 2004-2011



Grâce à ces avis et aux autres instruments utilisés, le CEPD a mis en œuvre ses priorités pour 2011, telles

que définies dans son inventaire. Les 24 avis ont couvert différents domaines politiques de l'UE.

Principaux domaines de politique des avis législatifs en 2011



L'inventaire 2011 a défini quatre principaux domaines d'attention:

- vers un nouveau cadre juridique de la protection des données,
- développement de l'espace de liberté, de sécurité et de justice,
- développements technologiques et stratégie numérique,
- autres initiatives ayant d'importantes répercussions sur la protection des données.

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

3.3.1. Une approche globale de la protection des données à caractère personnel dans l'Union européenne

Le 14 janvier 2011, le CEPD a publié un avis sur la communication de la Commission relative à la révision du cadre juridique européen pour la protection des données à caractère personnel. La communication marque une étape essentielle sur la voie d'un nouveau cadre juridique qui constituera le développement le plus important dans le domaine de la protection des données au niveau de l'Union européenne depuis l'adoption de la directive européenne sur la protection des données il y a 17 ans.

Selon le CEPD, les principes directeurs guidant le processus de révision devraient être les suivants:

- **les droits des personnes doivent être consolidés:** le CEPD propose d'introduire une notification obligatoire sur les failles de sécurité couvrant tous les secteurs concernés, ainsi que de nouveaux droits, en particulier dans l'environnement en ligne, tels que le droit à l'oubli et la portabilité des données. Les données relatives aux enfants doivent également être mieux protégées;
- **la responsabilité des organisations doit être renforcée:** le nouveau cadre doit comporter des incitations pour que les responsables du traitement dans le secteur public et privé prennent l'initiative d'intégrer de nouveaux outils dans leur processus opérationnels en vue d'assurer le respect de la protection des données (principe de responsabilisation). Le CEPD propose l'introduction de dispositions générales sur la responsabilisation et la «prise en compte du respect de la vie privée dès la conception»;
- **l'intégration de la coopération policière et judiciaire dans le cadre juridique** est une condition sine qua non pour assurer une protection efficace à l'avenir;
- **une harmonisation plus poussée** doit constituer l'un des principaux objectifs de la révision. La directive sur la protection des données devrait être remplacée par un règlement directement applicable;
- le nouveau cadre juridique doit être formulé de manière **technologiquement neutre** et doit avoir pour ambition de créer une **sécurité juridique** sur le long terme;
- les pouvoirs d'exécution des **autorités chargées de la protection des données** devraient être renforcés et leur indépendance mieux garantie dans l'UE.

Le CEPD a accueilli favorablement l'intention de la Commission de réformer le cadre juridique de protection des données, ce qu'il a déjà demandé à plusieurs reprises.¹⁰ La révision du cadre juridique

¹⁰ Voir par exemple l'avis du 25 juillet 2007 sur la communication de la Commission au Parlement européen et au Conseil relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données, JO C 255, 27.10.2007, p. 1

figurait d'ailleurs déjà en tête des priorités du CEPD en 2009 et 2010. Le CEPD a partagé l'avis de la Commission que, dans l'avenir, un système solide de protection des données est absolument nécessaire, tout en se fondant sur l'idée que les principes généraux de vie privée et de protection des données restent valides.

Dans son avis, le CEPD a soutenu les principaux enjeux et défis recensés par la Commission, mais a demandé des solutions plus ambitieuses afin de rendre le système plus efficace et de donner aux citoyens un meilleur contrôle sur leurs données à caractère personnel.

La Commission adoptera deux propositions législatives début 2012: une proposition de règlement général relatif à la protection des données et une proposition de directive sur la protection des données dans le domaine répressif. Le CEPD continuera naturellement de suivre le processus législatif et fournira de nouvelles contributions en fonction des besoins.

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

3.4.1. Conservation des données

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

L'avis du CEPD, adopté le 31 mai 2011, a analysé le rapport de la Commission qui évalue la mise en œuvre et l'application de la directive sur la conservation des données et mesure son impact sur les opérateurs économiques et les consommateurs.

Le CEPD a estimé que la directive **ne répondait pas aux exigences imposées par les droits fondamentaux à la protection de la vie privée et des données** pour les raisons suivantes:

- la nécessité de conservation des données fixée par la directive n'a pas été clairement démontrée;



La directive sur la conservation des données constitue une atteinte considérable à la vie privée.

- la conservation des données pourrait être régulée d'une manière moins intrusive pour la vie privée;
- la directive laisse une trop grande marge de manœuvre aux États membres pour décider des finalités pour lesquelles les données peuvent être utilisées, et pour déterminer qui peut accéder aux données et sous quelles conditions.

Le CEPD a souligné que les informations fournies par les États membres n'étaient pas suffisantes pour tirer une conclusion positive sur la nécessité de la conservation des données telle que prévue par la directive. Il est donc nécessaire d'examiner plus en avant le caractère nécessaire et proportionnel de la directive, et en particulier de considérer des moyens alternatifs, moins intrusifs, pour la vie privée.

Le rapport (d'évaluation) de la Commission joue un rôle dans d'éventuelles décisions de modifier la directive. Le CEPD a donc demandé à la Commission d'envisager sérieusement toutes les options dans ce nouveau processus, y compris la possibilité d'abroger la directive, éventuellement associée à une proposition de mesure alternative, plus ciblée, au niveau européen.

Si, sur la base de nouvelles informations, la nécessité d'un instrument européen sur la conservation des données est démontrée, cet instrument devrait respecter les exigences fondamentales suivantes:

- établir des règles globales et véritablement harmoniser les obligations de conservation des données, ainsi que l'accès et l'utilisation ultérieure des données par les autorités compétentes;
- être exhaustif, c'est-à-dire fixer un objectif clair et précis qui ne peut pas être contourné;
- être proportionné et ne pas aller au-delà de ce qui est nécessaire.

*Le CEPD a souligné que l'invasion massive de la vie privée que représente la directive sur la conservation des données nécessitait une réelle justification. Il a donc demandé à la Commission européenne d'utiliser l'exercice d'évaluation pour **prouver la nécessité** de la directive. Des faits et chiffres concrets devraient permettre d'évaluer s'il aurait été possible d'obtenir les résultats présentés dans l'évaluation en utilisant d'autres méthodes moins intrusives.*

3.4.2. Système européen de surveillance du financement du terrorisme (SSFT)

Le 25 octobre 2011, le CEPD a adressé ses observations sur la communication de la Commission du 13 juillet 2011 à la commissaire européenne chargée des affaires intérieures. Il a soutenu tous les arguments avancés par le groupe de travail «Article 29» dans sa lettre du 29 septembre 2011, notamment concernant les principes de nécessité et de proportionnalité, les relations entre les responsables du traitement des données et les sous-traitants, les transferts de données en masse, les types de données traitées, la conservation, les droits des personnes concernées, les APD, la sécurité des données et la coopération entre les États membres. En outre, il a mis en avant **la nécessité et la proportionnalité en tant que garanties procédurales** qui devraient être introduites dans tout système de surveillance du financement du terrorisme (SSFT) de l'UE.

3.4.3. Système européen de données des dossiers passagers

En 2011, comme les années précédentes, le traitement proposé des données des dossiers passagers (*Passenger Name Records – données PNR*) par les forces de l'ordre a soulevé des questions liées à la protection des données dans un contexte européen.

Le 25 mars 2011, le CEPD a adopté un avis analysant la nouvelle proposition de la Commission visant à obliger les transporteurs aériens à fournir aux États membres de l'UE les données des dossiers passagers (*Passenger Name Records - données PNR*) de vols à destination ou en provenance du territoire de l'Union afin de lutter contre les infractions graves et le terrorisme.

Dans son avis, le CEPD a rappelé que la nécessité de recueillir ou de stocker d'énormes quantités de données à caractère personnel doit s'appuyer sur une **démonstration claire de la relation entre l'utilisation et le résultat** (principe de nécessité). Il s'agit d'un préalable indispensable à tout développement d'un système PNR. Selon le CEPD, les réglementations actuelles ne parviennent pas à démontrer la nécessité et la proportionnalité d'un système qui prévoit une collecte à grande échelle des données PNR aux fins d'une évaluation systématique de tous les passagers.

3.4.4. Accord entre l'UE et l'Australie sur les données des dossiers passagers

Le 15 juillet 2011, le CEPD a adopté un avis sur une proposition de la Commission concernant un accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (données PNR). Le CEPD a approuvé les garanties prévues dans les propositions, notamment en ce qui concerne l'application concrète de l'accord et plus particulièrement les aspects de sécurité des données, la supervision et les dispositions d'exécution.

Il a cependant mis en évidence une **marge d'amélioration** considérable, notamment en ce qui concerne la portée de l'accord, la définition du terrorisme et l'inclusion de certaines finalités exceptionnelles, ainsi que la durée de conservation des données PNR. Il a également considéré que la base juridique de l'accord devrait être réexaminée et mentionner l'article 16 du traité sur le fonctionnement de l'Union européenne (TFUE).

Le CEPD a également rappelé le contexte plus large de la **légitimité** de tout système PNR, considéré comme la collecte systématique de données passagers à des fins d'évaluation des risques. Ce n'est que si le système respecte les exigences fondamentales de la nécessité et de la proportionnalité visées aux articles 7 et 8 de la Charte des droits fondamentaux et à l'article 16 TFUE qu'une proposition peut satisfaire aux autres exigences du cadre de protection des données.

Parmi les recommandations du CEPD, on peut citer ce qui suit:

- **champ d'application:** le champ d'application devrait être beaucoup plus limité compte tenu du type d'infractions concernées. Le CEPD recommande de définir explicitement les infractions mineures et de les écarter du champ d'application, ainsi que d'exclure la possibilité pour les États membres d'élargir ce dernier;
- **conservation des données:** aucune donnée ne devrait être conservée au-delà de 30 jours sous une forme identifiable, sauf dans les cas nécessitant une enquête plus approfondie;
- **principes de protection des données:** il convient d'introduire un niveau plus élevé de garanties, notamment au niveau des droits des personnes concernées et des transferts à des pays tiers;



Les compagnies aériennes et les agences de voyage recueillent des informations à caractère personnel au moment où un passager effectue une réservation avant de voyager.

- **liste de données PNR:** le CEPD se réjouit du fait que les données sensibles ne soient pas incluses dans la liste des données à traiter mais il considère toujours que cette liste est trop vaste et qu'elle devrait être davantage restreinte;
- **évaluation du système de données PNR de l'UE:** l'évaluation de la mise en œuvre du système devrait être fondée sur des données statistiques exhaustives, incluant le nombre de personnes effectivement condamnées - et pas seulement poursuivies - sur la base du traitement de leurs données à caractère personnel.

Enfin, le CEPD a rappelé que la nécessité de recueillir ou de conserver d'énormes quantités d'informations personnelles doit s'appuyer sur une démonstration claire de la relation entre l'utilisation et le résultat (principe de nécessité). Il s'agit d'un préalable indispensable à tout développement d'un système PNR. Selon le CEPD, ni la proposition ni son analyse d'impact ne parviennent à démontrer la nécessité et la proportionnalité d'un système qui prévoit une collecte à grande échelle des données PNR aux fins d'une évaluation systématique de tous les passagers.

3.4.5. Accord entre l'UE et les États-Unis concernant les données des dossiers passagers

Le CEPD a critiqué la nouvelle proposition en vue d'un accord entre l'UE et les États-Unis concernant les données des dossiers passagers (données PNR) car la nécessité et la proportionnalité des régimes PNR n'ont pas encore été démontrées. Dans son avis du 9 décembre 2011, il a critiqué:

- la **période de conservation de 15 ans:** le CEPD conseille d'effacer les données après leur analyse ou après une période maximale de 6 mois;
- la **limitation de finalité trop large:** la finalité devrait être limitée à la lutte contre le terrorisme ou à une liste bien déterminée de criminalité transnationale grave;
- la **liste des données devant être transférées** au DHS (*Department of Homeland Security*): elle doit être rétrécie et exclure les données sensibles;
- les **exceptions à la méthode «push»:** les autorités américaines ne devraient pas être en mesure d'accéder directement aux données (méthode «pull»);

- les **limites quant à l'exercice des droits des personnes concernées**: chaque citoyen devrait être en mesure d'exercer un droit de recours juridictionnel effectif de réparation;
- les **règles relatives aux transferts ultérieurs**: le DHS ne devrait pas transférer les données à d'autres autorités américaines ou à des pays tiers à moins qu'ils ne garantissent un niveau de protection équivalent.

Le CEPD a considéré que ni les principales préoccupations précédemment exprimées par le CEPD et les autorités nationales chargées de la protection des données de l'UE, ni les conditions posées par le Parlement européen pour donner son accord n'avaient été respectées.

3.4.6. Paquet anticorruption

Le 6 juillet 2011, le CEPD a publié des observations formelles sur le paquet anticorruption, qui consistait en une communication exposant l'approche de l'Union européenne pour mettre un frein à la corruption, une décision de la Commission de mettre en place un rapport européen anticorruption régulier et un rapport sur les conditions de la participation de l'UE au Groupe d'États contre la corruption du Conseil de l'Europe.

La communication fait référence à une stratégie envisagée visant à accroître la qualité des enquêtes financières et à développer les renseignements financiers, y compris le partage d'informations entre les États membres, les agences de l'UE et les pays tiers. À cet égard, le CEPD a encouragé la Commission à **garantir un niveau suffisant de protection des données dans cette future stratégie**. Il a également recommandé que le partage de meilleures pratiques envisagé dans le rapport anticorruption européen soit compris comme incluant les pratiques permettant de garantir la protection des données dans les enquêtes anticorruption.

3.4.7. Propositions législatives concernant certaines mesures restrictives

Le 16 mars et le 9 décembre 2011, le CEPD a adressé des lettres à la Commission européenne, au Parlement européen, au Conseil et au Haut Représentant de l'Union pour les affaires étrangères et la politique de sécurité, en réponse à la consultation de la Commission sur diverses propositions législatives concernant certaines mesures restrictives à l'encontre de l'Iran, de la République de Guinée-Bissau, de la Côte

d'Ivoire, de la Biélorussie, de la Tunisie, de l'Égypte, de la Lybie, de la Syrie, de l'Afghanistan et de la Birmanie/Myanmar. Dans ses lettres, le CEPD a réaffirmé sa position selon laquelle lorsque des institutions européennes adoptent des mesures restrictives à l'encontre de certaines personnes, les **principes de protection des données et toute restriction nécessaire devraient être énoncés de façon claire et complète**.

Dans ses propositions, la Commission envisageait de lutter contre les violations des droits de l'homme en imposant des mesures restrictives - notamment le gel d'avoirs et de ressources économiques - à des personnes physiques ou morales considérées comme impliquées dans ces violations. À cet effet, la Commission européenne publie et diffuse des «listes noires» des personnes physiques ou morales concernées par ces mesures restrictives.

Le CEPD a critiqué le fait que, bien que le texte original proposé par la Commission européenne et la haute représentante incluait des références importantes aux règles de protection des données, ces références ont été largement affaiblies par le Conseil. Il a réitéré sa recommandation à l'intention de la Commission européenne, du Haut Représentant et du Conseil, d'abandonner l'approche fragmentaire actuelle, permettant l'adoption par chaque pays ou organisation de règles spécifiques, et de développer plutôt un **cadre cohérent pour les mesures restrictives**, assurant le respect des droits fondamentaux et en particulier, du droit fondamental à la protection des données à caractère personnel.

3.4.8. Migration

En 2011, la Commission a travaillé sur une approche globale de la migration. Afin de faire connaître sa position et son programme, elle a publié une communication à ce sujet en mai. Le 7 juillet 2011, le CEPD a adopté un avis sur cette communication.



L'utilisation de la biométrie devrait être accompagnée de mesures de sauvegarde strictes.

Dans son avis, le CEPD mis l'accent sur la **nécessité de prouver la nécessité de nouveaux instruments proposés** tels que le système entrée-sortie. À cette fin, il a rappelé la jurisprudence de la Cour européenne des droits de l'homme et de la Cour européenne de justice qui prévoit que le degré de preuve nécessaire pour affecter les droits à la vie privée et à la protection des données est celui «nécessaire dans une société démocratique», et il a développé la notion de nécessité.

Une autre question examinée était l'utilisation de la biométrie. Dans ce dossier, le CEPD a recommandé que **toute utilisation de la biométrie soit accompagnée de garanties strictes et complétée par une procédure de secours** pour les personnes dont les caractéristiques biométriques peuvent ne pas être lisibles. En outre, il a **demandé à la Commission de ne pas réintroduire la proposition visant à accorder un accès à Eurodac** (un système d'information à grande échelle consacré au stockage des empreintes digitales, voir le point 4.2) **en vue de l'application de la loi**.

En indiquant clairement sa position sur le sujet, le CEPD a donné des orientations à la Commission sur la façon d'évaluer la nécessité. Il convient de noter que les documents ultérieurs de la Commission, tels que la communication sur les frontières intelligentes, indiquent que la Commission a accordé davantage d'attention à cette notion.

3.4.9. Victimes de la criminalité

Le 17 octobre 2011, le CEPD a publié son avis sur le paquet législatif relatif aux victimes de la criminalité, qui met l'accent sur les aspects liés à la vie privée de la protection des victimes de la criminalité. Le CEPD a accueilli favorablement les objectifs stratégiques des propositions et approuvé globalement l'approche de la Commission. Néanmoins, il a considéré il y aurait matière à renforcer et à clarifier la protection de la vie privée des victimes et des données à caractère personnel les concernant prévue par la proposition de directive.

Concernant la proposition de règlement relatif à la reconnaissance mutuelle des mesures de protection en matière civile, qui traite de la protection des personnes physiques contre d'autres personnes représentant une menace pour elles («harcèlement»), le CEPD a considéré que la **personne représentant la menace devrait recevoir uniquement** les données à caractère personnel strictement nécessaires à l'exécution de la mesure.

3.5. Stratégie numérique et technologie

En 2011, la Commission a réalisé des travaux importants dans le domaine de la société de l'information et des nouvelles technologies. Elle a particulièrement concentré ses efforts sur la mise en œuvre de la stratégie numérique et le programme Europe 2020. Plusieurs de ces initiatives étaient extrêmement pertinentes pour la protection des données et ont donc été suivies de près par le CEPD. Le CEPD a également surveillé les projets européens de recherche et de développement technologique pertinents, et y a participé.

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 la consultation publique sur la directive relative à l'application des droits de propriété intellectuelle¹¹ et le cadre juridique du système de coopération en matière de protection des consommateurs (SCPC).¹²

3.5.1. Neutralité de l'internet

Le 7 octobre 2011, le CEPD a adopté un avis sur la communication de la Commission relative à l'internet ouvert et à la neutralité de l'internet en Europe.



La neutralité de l'internet soulève de nombreuses questions liées à la protection des données.

Le CEPD a souligné les **conséquences** importantes de certaines pratiques de surveillance des FAI sur le **droit fondamental à la vie privée et la protection des données des utilisateurs**, plus particulièrement en termes de confidentialité des communications. Il a invité la Commission à lancer un débat impliquant tous les acteurs concernés en vue de **clarifier les modalités d'application du**

¹¹ Voir ci-dessous le point 3.7.1

¹² Voir ci-dessous le point 3.8.1

cadre juridique de la protection des données dans ce contexte.

Il a recommandé l'élaboration d'orientations en vue notamment de:

- déterminer les pratiques d'inspection **légitimes**, telles que celles nécessaires à des fins de sécurité;
- déterminer si la surveillance requiert **le consentement des utilisateurs**, par exemple dans les cas où le filtrage vise à limiter l'accès à certaines applications et certains services, tels que les services de partage de fichiers.

Les orientations devraient notamment concerner l'application des **garanties de protection des données** nécessaires, telles que la limitation de la finalité et la sécurité.

3.5.2 Projet technologique «Turbine»

Le 1^{er} février 2011, le CEPD a émis un avis basé sur son document stratégique intitulé «Le CEPD et la recherche et le développement technologique dans l'UE», adopté en 2008. Ce document décrit le rôle que pourrait jouer le CEPD en ce qui concerne les projets de recherche et de développement technologique (RDT) relevant du programme-cadre de recherche et développement technologique de la Commission.

Dans son avis, le CEPD a analysé le projet de recherche «Turbine» (TrUsted Revocable Biometric IdentiTies), dont les objectifs généraux consistent à:

- développer une solution technologique renforçant le respect de la vie privée lors de l'authentification électronique de l'identité (eID) par la biométrie des empreintes digitales;
- démontrer l'efficacité et la sécurité de cette solution pour des applications commerciales de gestion de la carte d'identité électronique (eID) ainsi que ses avantages pour le citoyen en termes de renforcement de la protection de la vie privée et de la confiance de l'utilisateur dans la gestion de la carte d'identité électronique par l'utilisation des empreintes digitales.

L'analyse du CEPD s'est centrée sur certaines caractéristiques importantes du projet, notamment la protection du modèle biométrique par transformation cryptographique des informations de l'empreinte



Turbine - TrUsted Revocable Biometric IdentiTies

digitale en une clé **non inversible** (impossibilité de revenir à l'information biométrique d'origine), et la **révocabilité** de cette clé (possibilité de produire une nouvelle clé indépendante afin de délivrer de nouvelles identités biométriques). Par ailleurs, pendant la phase d'essai, le projet a testé l'application des caractéristiques en question dans des situations réelles.

Le CEPD a accueilli favorablement le projet, car il démontre que l'application de la «prise en compte du respect de la vie privée dès la conception» en tant que principe-clé de la recherche constitue un moyen efficace de garantir des solutions respectueuses de la vie privée.

3.6. Marché intérieur y compris données financières

3.6.1. Système d'information du marché intérieur

Dans son avis du 22 novembre 2011, le CEPD a proposé une série de recommandations visant à renforcer le cadre de protection des données pour le système d'information du marché intérieur (IMI). Le CEPD a soutenu une approche cohérente de la protection des données par l'établissement d'un système électronique pour l'échange d'informations, y compris de données à caractère personnel pertinentes.

Le CEPD a accueilli favorablement le fait que la Commission ait proposé un instrument juridique horizontal pour l'IMI sous la forme d'un règlement du Conseil et du Parlement visant à mettre clairement en évidence les questions les plus pertinentes en matière de protection des données de l'IMI. Le CEPD a mis en garde contre les risques liés à l'établissement d'un système électronique unique centralisé pour de multiples domaines de coopération administrative. Concernant le cadre juridique de l'IMI devant être établi dans la proposition de règlement, le CEPD a attiré l'attention sur deux défis majeurs: **la nécessité d'assurer la cohérence du cadre légal tout en respec-**

tant la diversité et la nécessité de trouver un équilibre entre flexibilité et sécurité juridique.

Le CEPD a reconnu le besoin de flexibilité nécessaire pour couvrir la coopération administrative dans les différents domaines politiques, mais a insisté pour que cette flexibilité soit accompagnée d'une sécurité juridique. Dans ce contexte, le CEPD a recommandé que les fonctionnalités de l'IMI déjà envisagées soient davantage clarifiées et que l'inclusion de nouvelles fonctionnalités soit accompagnée des garanties procédurales adéquates, telles que la préparation d'une évaluation de l'impact sur la protection des données ainsi que la consultation du CEPD et des autorités nationales chargées de la protection des données.

Dans l'avis, il est également demandé que les droits des personnes concernées soient renforcés et que la prolongation du délai de conservation actuel de six mois soit revue à moins qu'une justification adéquate ne puisse être donnée.

Enfin, le CEPD a accueilli favorablement les dispositions relatives à la supervision conjointe et a recommandé qu'elles soient encore renforcées afin de garantir une coopération efficace et active des autorités chargées de la protection des données impliquées.

3.6.2. Intégrité et transparence du marché de l'énergie

Le 21 juin 2011, le CEPD a publié un avis sur la proposition de règlement sur l'intégrité et la transparence du marché de l'énergie. Le principal objectif de la proposition est d'empêcher la manipulation des marchés et les opérations entre initiés sur le marché de l'énergie de gros, du gaz et de l'électricité. Le CEPD a fait des observations sur plusieurs aspects de la proposition, notamment ceux concernant la surveillance du marché et la reddition de comptes ainsi que les enquêtes et les mesures d'exécution.

La principale préoccupation du CEPD était que la proposition **manquait de clarté et de garanties adéquates pour la protection des données** en ce qui concerne les pouvoirs d'enquête accordés aux autorités de réglementation nationales. Le CEPD a recommandé par conséquent de clarifier:

- si les inspections **sur place** seraient limitées aux locaux commerciaux ou s'appliqueraient également aux propriétés privées de particuliers. Dans ce dernier cas, il conviendrait de justifier clairement la nécessité et la proportionnalité de

ce pouvoir et de demander un mandat judiciaire et des garanties supplémentaires;

- la **portée des pouvoirs** «de se faire remettre des enregistrements téléphoniques et des données échangées existants». La proposition devrait spécifier sans ambiguïté quels **enregistrements** peuvent être demandés et à qui. Le fait qu'aucune donnée ne peut être demandée aux prestataires de services de communications électroniques accessibles au public devrait être mentionné explicitement. Le règlement proposé devrait également clarifier si les autorités peuvent aussi demander les enregistrements privés de particuliers (par exemple, les messages envoyés à partir d'appareils portables personnels). Si c'était le cas, il conviendrait de justifier clairement la nécessité et la proportionnalité de ce pouvoir et la proposition devrait également nécessiter un mandat de la part d'une autorité judiciaire.

La reddition de comptes et la collecte de données concernant les transactions suspectes constituent un autre sujet sensible dans la proposition pour lequel le CEPD demande que soient clarifiées les dispositions pertinentes et les garanties adéquates, telles que les limitations strictes aux finalités et les périodes de conservation.



Le CEPD a examiné de près la proposition de règlement sur le marché de l'énergie.

3.6.3. Interconnexion des registres du commerce

Le 6 mai 2011, le CEPD a publié un avis sur une proposition de directive visant à modifier trois directives existantes sur l'interconnexion des registres du commerce. L'objectif est de favoriser et de renforcer la coopération transfrontalière et l'échange d'informations entre les registres du commerce dans l'Union européenne, augmentant ainsi la transparence et la fiabilité des informations disponibles par delà les frontières.

La principale préoccupation du CEPD est que le projet de proposition, tel que rédigé, laisserait aux actes délégués des questions clés telles que celles de la gouvernance, des rôles, des compétences et des responsabilités. Afin de **garantir une sécurité juridique** établissant qui est responsable de quoi, et afin d'assurer que des garanties adéquates pour la protection des données puissent être identifiées et mises en œuvre, le CEPD recommande que ces questions clés soient abordées dans la directive proposée.

3.6.4. Contrats de crédit relatifs aux biens immobiliers à usage résidentiel

Le 25 juillet 2011, le CEPD a adopté un avis sur une proposition de directive de la Commission sur les contrats de crédit relatifs aux biens immobiliers à usage résidentiel. Le prêt responsable est défini dans la proposition comme étant la précaution prise par les prêteurs et intermédiaires de prêter des montants que les consommateurs peuvent rembourser et qui sont adaptés à leurs besoins et à leur situation. Du point de vue de la proposition, le comportement irresponsable de certains acteurs du marché a été l'un des éléments clés de la crise financière. La proposition introduit donc des exigences prudentielles et de surveillance pour les prêteurs et des obligations et des droits pour les emprunteurs afin d'établir un cadre juridique clair qui devrait préserver le marché européen des crédits hypothécaires des effets perturbateurs expérimentés durant la crise financière.

Le CEPD s'est félicité que la proposition mentionne la directive 95/46/CE. Cependant, il a suggéré quelques modifications dans le texte afin de clarifier l'**applicabilité des principes de protection des données aux traitements**, notamment en ce qui concerne la consultation de la base de données sur la solvabilité qui est constituée dans la quasi-totalité des États membres.



Les contrats de crédit sont soumis à l'applicabilité des principes de protection des données.

3.6.5. Produits dérivés négociés de gré à gré, contreparties centrales et référentiels centraux

L'avis, publié par le CEPD le 19 avril 2011, mettait l'accent principalement sur les pouvoirs de recherche spécifiques accordés à l'Autorité européenne des marchés financiers (AEMF) aux termes du règlement proposé, à savoir **«exiger des enregistrements téléphoniques et d'échanges de données»**.

*L'avis met en évidence que les pouvoirs de recherche concernant directement les données relatives au trafic, compte tenu de leur nature potentiellement intrusive, doivent respecter les exigences de **nécessité et de proportionnalité**. Il est donc essentiel qu'ils soient clairement formulés en ce qui concerne leur champ d'application personnel et matériel ainsi que les circonstances et les conditions dans lesquelles ils peuvent être utilisés. Des garanties appropriées devraient également être fournies contre le risque d'abus.*

Le CEPD a estimé que ces exigences n'étaient pas remplies par le règlement proposé car le pouvoir considéré était **formulé de manière trop large**. En particulier, le **champ d'application personnel et matériel** du pouvoir, **les circonstances et les conditions** dans lesquelles il peut être utilisé

n'étaient pas suffisamment détaillés. Le CEPD a donc demandé plus de clarté et conseillé au législateur:

- de préciser clairement les catégories d'enregistrements téléphoniques et d'échanges de données que les référentiels centraux sont tenus de conserver et/ou de communiquer aux autorités compétentes;
- de limiter le pouvoir d'exiger l'accès aux enregistrements téléphoniques et d'échanges de données aux référentiels centraux seulement;
- d'énoncer explicitement que l'accès aux enregistrements téléphoniques et d'échanges de données directement auprès des sociétés de télécommunications est exclu.

Le CEPD a également recommandé de limiter l'exercice du pouvoir aux **infractions identifiées et graves** du règlement proposé et aux cas dans lesquels il existe un **motif raisonnable** de soupçonner une infraction. Il a suggéré en outre d'introduire **l'obligation d'autorisation judiciaire** préalable (au moins dans les cas où une telle autorisation est exigée en vertu de la législation nationale) et des garanties procédurales adéquates contre le risque d'abus.

3.6.6. Exigences techniques pour les virements et les prélèvements en euros

Le 23 juin 2011, le CEPD a adopté un avis sur une proposition de règlement de la Commission établissant des exigences techniques pour les virements et les prélèvements en euros, portant sur l'espace unique de paiements en euros (SEPA).

Le SEPA est un projet visant à instaurer un marché unique des paiements de détail en euros en surmontant les obstacles techniques, juridiques et commerciaux découlant de la période antérieure à l'introduction de la monnaie unique qu'est l'EURO. Dès que le SEPA sera achevé, il n'y aura plus de différence entre les paiements nationaux et transfrontaliers en euros.

L'introduction et le développement du SEPA impliquent plusieurs traitements de données: les noms, les numéros de compte bancaire et le contenu des contrats doivent être échangés directement entre les payeurs et les bénéficiaires et indirectement par l'intermédiaire de leurs prestataires de services de paiement respectifs afin de garantir le bon déroulement des transferts. La proposition prévoit aussi un nouveau rôle pour les autorités nationales chargées de contrôler le respect du règlement et de prendre toutes les mesures nécessaires pour garantir celui-ci. Si ce rôle est fondamental



L'introduction et le développement du SEPA impliquent plusieurs traitements de données.

pour garantir une mise en œuvre effective du SEPA, il est aussi susceptible d'accorder aux autorités de larges pouvoirs leur permettant de traiter ultérieurement les données à caractère personnel des individus, y compris le montant total des virements en euros entre les individus et les entités.

Le CEPD a donc recommandé quelques modifications au texte afin de **garantir que les échanges desdites données se conforment à la législation applicable** et notamment aux principes de nécessité, de proportionnalité et de limitation de la finalité.

3.6.7. Scanners corporels dans les aéroports

Le 17 octobre 2011, le CEPD a envoyé une lettre au vice-président de la Commission européenne Sim Kallas concernant trois propositions sur les normes de base communes en matière de sûreté de l'aviation civile en ce qui concerne l'utilisation de scanners de sécurité dans les aéroports de l'UE. La Commission a adopté les projets de mesures à l'aide de la procédure de «comitologie».

Dans ses observations, le CEPD a accueilli favorablement les garanties incluses dans les projets de mesures et le fait qu'il existe une approche de l'UE concernant les scanners de sécurité, étant donné que cela peut garantir une sécurité juridique ainsi qu'un niveau constant de protection des droits

fondamentaux. Cependant, il a remis en cause la **nécessité** et la **proportionnalité** de ces mesures, et a rappelé que **la législation en matière de protection des données était applicable**.

Le CEPD a également déploré que **des scanners corporels donnant une image détaillée du corps soient un jour autorisés**, surtout compte tenu du fait qu'un appareil moins intrusif pour la vie privée aurait pu être privilégié (c'est-à-dire, un scanner corporel montrant une silhouette à la place du corps humain).

3.7. Application transfrontalière de la loi

3.7.1. Directive relative à l'application des droits de propriété intellectuelle

Le 8 avril 2011, le CEPD a répondu à la consultation publique lancée par la Commission européenne sur l'application de la directive relative au respect des droits de propriété intellectuelle. Le CEPD a présenté une large vue d'ensemble des questions relatives à la protection des données qui peuvent se poser dans le contexte de l'application des droits de propriété intellectuelle sur l'internet. Le CEPD a souligné le fait que l'application des droits de propriété intellectuelle sur l'internet pose des défis majeurs et exige des garanties adéquates de



Le respect des droits de propriété intellectuelle sur l'internet requiert des garanties adéquates pour la protection des données.

protection des données. C'est le cas en particulier lors de la surveillance de l'activité sur internet destinée à trouver des contrevenants présumés ou lors de la collecte d'information sur les données à caractère personnel (par exemple le nom d'un abonné lié à une adresse IP concrète) auprès d'intermédiaires tels que les fournisseurs d'accès à internet.

Le CEPD a mis en avant l'importance de **trouver le bon équilibre entre le droit fondamental à la protection des données et le droit de propriété intellectuelle**. Il a estimé que les dispositions actuelles de la directive, fondées sur la recherche de l'équilibre compatible avec l'échelle commerciale de l'infraction, étaient appropriées bien qu'une clarification demeure nécessaire sur certains points.

Enfin, le CEPD a fait certaines recommandations visant à aider la Commission à adopter une vue plus prospective. En particulier, **la protection des données devrait être prise en compte dans l'évaluation de la mise en œuvre de la directive actuelle**, de son suivi et lors d'éventuelles modifications législatives.

3.7.2. Contrôle par les autorités douanières du respect des droits de propriété intellectuelle

Le 12 octobre 2011, le CEPD a adopté un avis sur la proposition de règlement concernant le contrôle, par les autorités douanières, du respect des droits de propriété intellectuelle. Le CEPD a accueilli favorablement le fait que la proposition de règlement fasse explicitement référence à l'applicabilité de la directive 95/46/CE et du règlement (CE) n° 45/2001 aux traitements de données à caractère personnel visés par le règlement.

Le CEPD a également mis en avant le droit à l'information des personnes concernées, la nécessité de concevoir un formulaire type de demande conforme à la protection des données, la définition d'une durée limite pour la conservation des données à caractère personnel communiquées par le titulaire du droit, au niveau national et à celui de la Commission, et la nécessité de clarifier la base juridique de la création d'une nouvelle base de données centrale de la Commission (COPIS).

3.7.3. Compétence judiciaire, reconnaissance et exécution des décisions en matière civile et commerciale

Le 20 septembre 2011, le CEPD a soumis des observations sur la proposition de règlement concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale. Le CEPD a souligné l'importance, dans le domaine de la protection des données également, de faciliter le règlement de litiges transfrontaliers. Il a insisté sur la nécessité de mener une réflexion plus approfondie sur certaines des questions soulevées dans la proposition, également dans le contexte de la révision en cours du cadre de protection des données dans l'UE:

- il convient notamment d'examiner de plus près la question de savoir si des règles juridictionnelles devraient protéger la partie la plus faible, également dans des procédures concernant la protection des données – comme c'est déjà le cas en matière d'emploi, d'assurance et de protection des consommateurs;
- en ce qui concerne le maintien de l'exequatur pour le respect de la vie privée, la diffamation, les droits ayant trait à la personnalité et la possibilité de contester la reconnaissance de décisions pour des raisons d'ordre public dans ces cas, le CEPD insiste sur la nécessité d'une interprétation stricte de ces exceptions;
- il n'est pas clairement établi si l'exception susmentionnée pour les droits à la vie privée est également censée couvrir des violations de règles juridiques pour le traitement de données à caractère personnel, comme prévu dans la directive de protection des données et, le cas échéant, dans quelle mesure. Cela peut créer des problèmes d'interprétation et ne contribuera pas à la sécurité juridique que la proposition vise à établir;
- une réflexion plus approfondie devrait être menée sur la façon de mieux aligner la compétence des tribunaux avec la compétence des autorités chargées de la protection des données.

3.7.4. Ordonnance européenne de saisie conservatoire des comptes bancaires

Le 13 octobre 2011, le CEPD a adopté un avis sur une proposition de règlement portant création d'une ordonnance européenne de saisie conservatoire des comptes bancaires, destinée à faciliter le recouvrement transfrontalier de créances en matière civile et commerciale. Le CEPD a noté avec satisfaction les efforts entrepris pour tenir compte des différents aspects de protection des données qui sont soulevés par la proposition d'instrument d'une OESC. Plus particulièrement, il a apprécié l'application du principe de nécessité et les références qui y sont faites.



Le recouvrement transfrontalier des dettes implique le traitement de données à caractère personnel.

Cependant, le CEPD a estimé que la proposition de règlement nécessitait des améliorations et des clarifications supplémentaires. Le CEPD a notamment recommandé :

- d'envisager d'inclure la possibilité pour le demandeur de demander le retrait des détails de son adresse, des informations communiquées au défendeur;
- de retirer les champs de données facultatives de l'annexe I du règlement (le numéro de téléphone et l'adresse électronique du défendeur) si le véritable besoin de ces données n'est pas démontré;
- de limiter les informations fournies par le demandeur aux informations nécessaires à l'identification du défendeur et à la détermination de son ou ses comptes bancaires.

3.8. Santé publique et consommateurs

3.8.1. Système de coopération en matière de protection des consommateurs

Le 4 mai 2011, le CEPD a rendu un avis législatif commentant le cadre juridique du système de coopération en matière de protection des consommateurs (SCPC). Le SCPC est un système de technologie de l'information conçu et exploité par la Commission. Le SCPC facilite la coopération entre les autorités compétentes des États membres de l'UE et la Commission dans le domaine de la protection des consommateurs. Dans le cadre de leur coopération, les autorités compétentes échangent des informations, y compris des données à caractère personnel.

Le CEPD a accueilli favorablement le fait que le règlement relatif au SCPC ait été complété au fil du temps par une décision de mise en œuvre et un ensemble de lignes directrices en matière de protection des données qui, conjointement, apportent de plus amples précisions sur le traitement même, ainsi que des garanties spécifiques quant à la protection des données.

Les principales recommandations de l'avis législatif sont notamment :

- en ce qui concerne la **période de conservation**, les demandes d'assistance mutuelle devraient être classées dans des délais bien précis. À moins qu'une enquête ou une mesure d'exécution ne soit en cours, les alertes devraient être retirées et supprimées dans un délai de six mois suivant leur publication. En outre, la Commission devrait préciser et réexaminer la finalité et la proportionnalité de la conservation de toutes les données liées à des affaires closes pendant une période supplémentaire de cinq ans;
- la Commission devrait réévaluer les mesures techniques et organisationnelles supplémentaires à prendre pour garantir que la protection de la vie privée et des données soit «conçue» dans l'architecture du SCPC («**prise en compte du respect de la vie privée dès la conception**») et que des contrôles adéquats soient mis en place pour veiller au respect de la protection des données et pour en apporter la preuve («**responsabilisation**»).

3.9. Questions diverses

3.9.1. Règlement portant réforme de l'OLAF

Le 1^{er} juin 2011, le CEPD a adopté un avis sur une proposition de règlement visant à modifier les règles actuelles relatives aux enquêtes menées par l'Office européen de lutte antifraude (OLAF). La proposition a pour objet d'augmenter l'efficacité, l'efficacité et la responsabilisation de l'OLAF, tout en préservant son indépendance en matière d'enquêtes.

Le CEPD a soutenu les objectifs des amendements proposés et a accueilli favorablement la proposition. Malgré l'impression générale positive, le CEPD a estimé que, du point de vue de la protection des données à caractère personnel, la proposition pourrait être améliorée sans compromettre les objectifs qu'elle poursuit.

Le CEPD a par conséquent émis un certain nombre de recommandations qui devraient être prises en compte en modifiant le texte. En particulier, la proposition devrait :

- mentionner clairement le **droit à l'information** des différentes catégories de personnes concernées, ainsi que le **droit d'accès et de rectification** des données par rapport à toutes les phases des enquêtes menées par l'OLAF;
- clarifier la relation entre le besoin de **confidentialité des enquêtes** et le régime de protection des données applicable lors des enquêtes;
- clarifier les principes généraux de protection des données sur la base desquels l'OLAF peut **transmettre et recevoir des informations**, notamment des données à caractère personnel, avec d'autres organes et agences de l'UE, et confier au directeur général la tâche d'assurer qu'une **vue d'ensemble stratégique et complète des différents traitements** de l'OLAF soit élaborée, gardée à jour et rendue transparente.

3.9.2. Règlement financier de l'UE

Le 15 avril 2011, le CEPD a adopté un avis sur la proposition de la Commission visant à réviser les règles financières régissant le budget annuel de l'Union européenne (règlement financier de l'UE). La proposition couvre plusieurs aspects qui entraînent le

traitement de données à caractère personnel par les institutions de l'UE, ainsi que par des entités au niveau des États membres.

Parmi les nouveaux éléments les plus importants introduits par la proposition figure la possibilité de publier des décisions sur les pénalités administratives et financières. Une telle publication impliquerait de divulguer d'une manière identifiable des informations à propos de la personne concernée. Le CEPD est d'avis que cette disposition, telle qu'elle est formulée, ne répond pas aux exigences de la législation en matière de protection des données.

Afin de mieux respecter les règles de protection des données, elle devrait être améliorée en indiquant explicitement la finalité de la divulgation, en assurant l'application cohérente de la possibilité de ce qui revient en fait à stigmatiser des personnes, et en utilisant des critères précis pour démontrer la nécessité de la divulgation.

Les recommandations du CEPD couvriraient également ce qui suit :

- **dénonciateurs**: le législateur devrait assurer la confidentialité de l'identité des dénonciateurs lors des enquêtes, excepté dans les cas où elle enfreint les règles nationales régissant les procédures judiciaires;
- **publication d'informations concernant les destinataires de fonds** en provenance du budget: le règlement devrait indiquer explicitement la finalité de la divulgation de l'information concernant les destinataires de fonds en provenance du budget et en expliquer la nécessité;
- **base de données centrale sur les exclusions**: la proposition prévoit la création d'une base de données contenant les détails de candidats individuels ou d'entreprises soumissionnaires exclus de la participation aux procédures de passation de marchés. L'accès à la base de données par les autorités de pays tiers devrait respecter les règles spécifiques de protection des données relatives aux transferts à des pays tiers.

3.9.3. Statistiques européennes de la sécurité face à la criminalité

Le 19 septembre 2011, le CEPD a adopté un avis sur la proposition de règlement de la Commission relatif aux statistiques européennes de la sécurité face à la criminalité. La finalité de la proposition est la

mise en œuvre, dans l'Union européenne, d'une nouvelle enquête sur la sécurité face à la criminalité. L'enquête inclurait des questions détaillées sur d'éventuels incidents de violence physique et sexuelle dont les répondants auraient pu être victimes, au sein ou en dehors du couple, sur des relations antérieures, sur leurs caractéristiques socio-démographiques et sur leurs sentiments de sécurité et leurs attitudes vis-à-vis de l'application de la loi et des précautions en matière de sécurité.

Le CEPD a déclaré mesurer l'importance de l'élaboration, de la production et de la diffusion de données statistiques. Il est cependant **préoccupé par les questions concernant les agressions physiques et sexuelles** et par la **possibilité d'identifier les victimes et agresseurs présumés**. Il a formulé plusieurs recommandations visant à réduire le risque d'identification directe ou indirecte inutile, à s'assurer que les catégories de données à caractère personnel qui doivent être collectées et traitées sont pertinentes et non excessives au regard de la finalité spécifique et à mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir la confidentialité et la sécurité des données à caractère personnel

jusqu'à ce que celles-ci soient rendues anonymes conformément aux principes de protection des données.

3.9.4. Transport

Le 5 octobre 2011, le CEPD a adopté un avis sur la proposition de la Commission visant à réviser la législation européenne relative aux tachygraphes, appareils utilisés dans les transports routiers pour surveiller les temps de conduite et de repos des conducteurs professionnels afin de vérifier le respect de la législation sociale dans le domaine. La révision a pour but de tirer parti des nouveaux développements technologiques en vue d'améliorer l'efficacité des tachygraphes numériques par rapport aux tachygraphes analogiques, notamment par l'utilisation de la géolocalisation et des installations de communication à distance. L'initiative affecte donc la **vie privée des conducteurs professionnels** de façon évidente puisqu'elle permet le contrôle permanent de leurs allées et venues, ainsi qu'une surveillance à distance par les autorités de contrôle qui auront un accès direct aux données à caractère personnel des conducteurs stockées dans le système.



L'introduction d'un nouveau tachygraphe numérique pourrait s'avérer très envahissante pour la vie privée.

Le CEPD a souligné que des **garanties spécifiques en matière de protection des données** sont nécessaires pour garantir un niveau satisfaisant de protection des données dans le système. Il a notamment recommandé que:

- l'installation et l'utilisation d'appareils dans le but direct et principal de permettre aux employeurs de **surveiller à distance et en temps réel les allées et venues de leurs employés** soient exclues;
- les **modalités générales du traitement des données à caractère personnel** dans les tachygraphes soient clairement énoncées dans la proposition, par exemple, le type de données enregistrées dans les tachygraphes et les équipements de géolocalisation, les destinataires et les délais de conservation des données;
- les **exigences de sécurité** pour le tachygraphe numérique établies dans la proposition soient davantage développées, notamment pour préserver la confidentialité des données, assurer l'intégrité des données et prévenir la fraude et la manipulation illégale;
- l'introduction de toute mise à jour technologique (par exemple, communication à distance ou systèmes de transport intelligents) dans les tachygraphes soit dûment appuyée par des **analyses d'impact sur la vie privée** afin d'évaluer les risques liés à la vie privée soulevés par l'utilisation de ces technologies.

Ces mesures de sauvegarde seront également pertinentes dans le contexte plus large des technologies de géolocalisation: en effet, si ces technologies peuvent aider à améliorer l'efficacité et la qualité des transports, elles impliquent également un risque de surveillance renforcée des conducteurs.

3.9.5. Politique agricole commune après 2013

Le 14 décembre 2011, le CEPD a adopté un avis sur les propositions législatives concernant la politique agricole commune après 2013. Le CEPD a observé que de nombreuses questions essentielles pour la protection des données n'étaient pas incluses dans les propositions, mais qu'elles seront régies par des actes délégués ou d'exécution. Le CEPD a recommandé qu'au moins les éléments suivants soient régis dans les propositions afin d'assurer la sécurité juridique:

- la **finalité spécifique** de chaque traitement devrait être explicitement décrite;
- les **catégories de données** devant être traitées devraient être prévues et précisées car, dans de nombreux cas, la portée du traitement n'était pas claire;
- les **droits d'accès** devraient être indiqués clairement, en particulier en ce qui concerne l'accès aux données par la Commission – il devrait être spécifié que la Commission ne peut traiter des données à caractère personnel 'qu'en cas de nécessité, par exemple à des fins de contrôle;
- des **périodes de conservation** maximales devraient être établies car dans certains cas, seules des périodes de conservation minimales sont mentionnées;
- les **droits des personnes concernées** devraient être précisés, notamment en ce qui concerne le droit à l'information des bénéficiaires et des tierces parties;
- **l'étendue et la finalité des transferts à des pays tiers** devraient aussi être précisées et respecter les exigences énoncées dans la législation relative à la protection des données.

Des **mesures de sécurité** devraient également être prévues, notamment en ce qui concerne les bases de données et systèmes informatiques. En outre, comme des **données relatives à des infractions ou suspicions d'infractions** peuvent être traitées (par exemple, en rapport avec une fraude), le traitement peut être soumis à un contrôle préalable par le CEPD ou par les autorités nationales chargées de la protection des données.

3.9.6. Contrôle destiné à garantir le respect de la politique de la pêche

Cet avis, publié le 28 octobre 2011, traitait de certains aspects techniques relatifs au règlement de la Commission instituant le régime européen de contrôle de la pêche. Le CEPD avait déjà rendu un avis en mars 2009 sur une proposition apparentée, mais il n'a toutefois pas été consulté par la Commission avant l'adoption du présent règlement.

Les activités des navires de pêche font l'objet d'une surveillance systématique et détaillée grâce à des moyens technologiques modernes, y compris des dispositifs de localisation par satellite et des bases



Les activités des navires de pêche font l'objet d'une surveillance systématique et détaillée utilisant des moyens technologiques avancés.

de données informatisées, traçant et conservant des données de localisation telles que la position géographique, le cap et la vitesse des navires de pêche. Toutes ces données sont systématiquement contrôlées par recoupement, analysées et vérifiées au moyen d'algorithmes informatisés et de mécanismes automatisés afin de repérer des incohérences ou des infractions présumées.

Tant que ces données concernent des personnes physiques identifiées ou identifiables (par exemple, le capitaine du navire, le propriétaire du navire ou les membres de l'équipage), un tel contrôle implique le **traitement de données à caractère personnel**. Il est dès lors important que le système de contrôle soit bien équilibré et que des protections adéquates soient mises en place afin d'éviter que les droits des personnes concernées ne soient indûment limités.

3.10. Accès du public aux documents contenant des données à caractère personnel

Dès le départ, le CEPD a abordé la relation parfois compliquée qui existe entre les règles de l'UE relatives à l'**accès du public aux documents** et les règles de l'UE relatives à la **protection des données**.

Il s'est d'abord attaqué à la question en donnant des conseils aux institutions de l'UE. En 2005, par exemple, le CEPD a publié un document de référence intitulé «Accès du public aux documents et protection des données», qui renfermait des lignes directrices à l'intention des institutions et organes de l'UE.

Une partie de l'analyse présentée dans ce document de référence n'est plus valide à la lumière de l'arrêt de la Cour européenne de justice dans l'affaire *Bavarian Lager* (voir le point 3.11.1 ci-dessous). Dès lors, le 24 mars 2011, le CEPD a publié un document de référence sur l'accès du public aux documents contenant des données à caractère personnel, **document destiné à servir de guide aux institutions européennes**. Le document présente la position renouvelée du CEPD sur le sujet suite à l'arrêt de la Cour européenne de Justice dans l'affaire *Bavarian Lager* portant sur la conciliation du droit fondamental à la protection de la vie privée et des données à caractère personnel avec le droit fondamental à l'accès aux documents et à la transparence.

En cas de divulgation de données à caractère personnel par les institutions européennes, une approche proactive permettrait de s'assurer que les personnes concernées sont bien informées et en mesure de faire valoir leurs droits dans le domaine de la protection des données. Cette approche serait également bénéfique pour les

institutions, car elle permettrait de réduire les charges administratives des responsables du traitement des données et de ceux chargés du traitement des demandes d'accès du public.

Le CEPD encourage l'administration européenne à développer des **politiques internes claires** en la matière, incluant la création d'une présomption de publicité pour certaines données à caractère personnel utilisées dans des cas précis (par exemple, documents contenant des données à caractère personnel portant uniquement sur les activités professionnelles de la personne concernée). Le CEPD souligne qu'un changement des règles sur l'accès du public aux documents est nécessaire, et il encourage le Conseil et le Parlement à accélérer le processus de révision en cours.

3.11. Affaires judiciaires

3.11.1. Participation du CEPD à des procédures judiciaires

L'année 2011 a été chargée pour le CEPD à l'égard de la participation à des procédures devant les tribunaux européens. Les agents du CEPD ont présenté la position du CEPD lors d'audiences devant les tribunaux dans quatre affaires, dont trois ont déjà fait l'objet d'un arrêt du tribunal.

Dans l'affaire *M^{me} V. contre Parlement européen* (affaire F-46/09), le CEPD a été invité à intervenir par le Tribunal de la fonction publique. L'affaire concernait le transfert présumé illégal de données médicales entre les services médicaux de la Commission et le Parlement européen. Le CEPD a plaidé en faveur de la demanderesse, arguant que le transfert était contraire aux règles de protection des données car il n'était pas nécessaire et qu'il ne reposait pas sur une base juridique appropriée. Dans son jugement du 5 juillet 2011, le Tribunal de la fonction publique s'est prononcé en faveur de la demanderesse, suivant le raisonnement du CEPD.

Les trois autres affaires concernaient la relation entre les règles de l'UE relatives à l'accès du public aux documents et les règles de l'UE relatives à la protection des données. Comme indiqué dans le point 3.10, le CEPD a été impliqué dans la question. Les trois affaires peuvent être considérées comme le suivi juridique de l'arrêt déterminant rendu par la Cour de justice dans l'affaire *Bavarian Lager* le

29 juin 2010 (affaire C-28/08 P). Le CEPD a expliqué sa position au cours des trois audiences, comme il est précisé dans le document de référence complémentaire du 24 mars 2011.

Dans son arrêt du 7 juillet 2011, *Valero Jordana contre Commission* (affaire T-161/04), le Tribunal a considéré que la Commission avait eu tort de ne pas évaluer la demande d'accès public à certaines données à caractère personnel au titre des règles de protection des données. Cette conclusion était conforme aux arguments présentés au Tribunal par le CEPD.

Dans son arrêt du 23 novembre 2011, *Dennekamp contre Parlement européen* (affaire T-82/09), le Tribunal a conclu que le demandeur, un journaliste demandant les noms des membres du Parlement européen affiliés à un régime de pension complémentaire, n'avait pas démontré la nécessité de rendre les données publiques. Le CEPD avait défendu l'avis contraire, considérant que pour réaliser un équilibre entre les différents intérêts en jeu, les données auraient dû être divulguées au journaliste.

La troisième affaire, *Egan et Hackett contre Parlement européen* (affaire T-190/10), n'a pas, au moment de la rédaction du présent rapport, fait l'objet d'un arrêt du Tribunal. Cette affaire concernait une demande d'accès aux noms des assistants des membres du Parlement européen.

Outre ces quatre affaires, le CEPD est intervenu dans l'affaire *Commission contre Autriche* (affaire C-614/10), une procédure d'infraction contre l'Autriche concernant le manque d'indépendance de l'autorité autrichienne de protection des données. Le CEPD a présenté un mémoire en intervention, soutenant la conclusion de la Commission selon laquelle la façon dont l'autorité autrichienne de protection des données est intégrée dans la structure institutionnelle de l'Autriche ne garantit pas suffisamment son indépendance.



Dans ses interventions, le CEPD vise à clarifier la question de la protection des données.

Enfin, l'ENISA a porté devant le Tribunal une affaire contre une décision rendue par le CEPD au sujet d'une réclamation (affaire T-345/11). La demande a été déclarée manifestement irrecevable pour des raisons de procédure.

3.11.2. Jurisprudence en matière de protection des données

Les tribunaux européens ont rendu plusieurs autres arrêts pertinents pour la protection des données. Trois décisions de la Cour de justice sont exposées brièvement ci-dessous.

L'affaire *Deutsche Telekom* (affaire C-543/09) a soulevé des questions quant à savoir si, en vertu de la directive «Vie privée et communications électroniques» révisée, une entreprise attribuant des numéros de téléphone à ses abonnés était autorisée à fournir des données concernant ces abonnés à d'autres entreprises dont les activités consistaient à fournir des services d'annuaire et de renseignements sans un renouvellement du consentement des personnes concernées. Dans son arrêt du 5 mai 2011, la Cour a considéré que, les abonnés ayant déjà été correctement informés de cette possibilité, le renouvellement du consentement n'était pas nécessaire.

Dans son arrêt dans l'affaire *ASNEF et FECEMD* du 24 novembre 2011 (affaires jointes C-648/10 et C-469/10), la Cour de justice a répondu à un tribunal espagnol qui avait demandé des éclaircissements sur une disposition de la directive relative à la protection des données autorisant le traitement des données à caractère personnel si ce traitement servait un intérêt légitime et n'était pas contrebalancé par l'intérêt des personnes concernées impliquées. Dans le droit espagnol, cela n'était possible qu'à l'égard des données à caractère personnel déjà rendues publiques. Selon la Cour, cette restriction nationale n'est pas conforme à la directive, qui a un effet direct sur la question.

Le 24 novembre 2011, la Cour de justice a rendu un arrêt préjudiciel dans une affaire belge, concernant l'obligation d'un fournisseur de services internet (Scarlet Extended) de surveiller le comportement sur Internet de ses clients afin de prévenir la violation de droits de propriété intellectuelle (affaire C-70/10). La Cour a conclu que l'obligation constituait une obligation générale de surveillance, interdite en vertu des règles de l'UE relatives au commerce électronique. La Cour a également noté qu'une telle obligation ne réalisait pas un juste équilibre entre le respect des droits de propriété intellectuelle et

plusieurs droits et liberté fondamentaux définis dans la charte des droits fondamentaux, dont le droit à la protection des données.

3.12. Développements technologiques futurs

Dans ce que l'on appelle «société de l'information» ou «monde numérique», les citoyens, les clients, les administrations et les entreprises interagissent plus que jamais grâce à la technologie. La technologie facilite la production, l'échange et le stockage d'informations (y compris les données à caractère personnel) et rend les barrières traditionnelles, telles que l'emplacement géographique, la langue ou même les coûts d'infrastructure, de moins en moins pertinentes.

En outre, les nouveaux développements technologiques brouillent progressivement les frontières entre le monde numérique et le monde réel (dans le secteur numérique, les données existent mais pas les personnes concernées, les responsables du traitement des données ni les sous-traitants); les deux mondes vont bientôt converger en une réalité unique avec des règles communes. La technologie devient de plus en plus accessible et facile d'utilisation, et ceux qui l'utilisent ne sont pas seulement les personnes concernées mais souvent également les responsables du traitement des données.

À partir de 2012, le CEPD prévoit que les six sujets suivants revêtiront une importance particulière:

- **La multiplication des traitements effectués de façon dématérialisée ('Cloud')**. Le paradigme des services informatiques hébergés existe depuis plusieurs années. À une échelle suffisante, les services informatiques hébergés apportent à présent des avantages notables en matière de réduction des coûts, convainquant les entreprises, les organisations gouvernementales et les citoyens d'y déplacer leurs traitements de données. Ils entraînent néanmoins de nouveaux défis du point de vue de la protection des données, tels que, par exemple: i) une perte de contrôle des responsables du traitement des données sur les traitements de données en raison de la complexité des cas qui se présentent, ii) une délocalisation des données et un enchevêtrement de juridictions différentes en liaison avec le manque d'harmonisation des lois relatives à la protection des données au niveau international, iii) une augmentation du nombre d'acteurs participant aux traitements de données et une dilution de leurs responsabilités, iv) un traitement massif de données

effectué par des individus agissant en tant que responsables du traitement des données sans bien connaître leurs obligations et v) des défis considérables en matière de sécurité et d'application des droits des personnes concernées.

Les coûts liés à la capacité de stockage, à la puissance de traitement et à la bande passante du réseau continuent de chuter dans toutes les formes d'informatique dématérialisée (en tant qu'infrastructure, plateforme ou service) à un point tel que le lien traditionnel entre le volume des données et le coût de l'infrastructure associée sera bientôt brisé, c'est-à-dire que les coûts d'infrastructure baissent et les barrières à l'entrée concernant les traitements massifs de données disparaissent. Ce phénomène permettra aux personnes physiques et aux petites entreprises d'effectuer des traitements massifs de données que, jusqu'à présent, seuls les gouvernements et les grandes entreprises pouvaient se permettre.

•L'augmentation des traitements effectués sur les dispositifs mobiles intelligents. Les possibilités qu'offrent les dispositifs mobiles intelligents se développent également à un rythme accéléré. Les dispositifs d'aujourd'hui sont toujours allumés et capables de partager, modifier et traiter des informations en temps réel. Les dispositifs de nouvelle génération disposeront de davantage de puissance, de meilleures interfaces, d'une connectivité accrue et d'une plus grande capacité de stockage, et ils seront intégrés de manière homogène dans le «nuage». En 2012, les processeurs quadricœurs deviendront courants dans les dispositifs mobiles intelligents, les réseaux LTE¹³ seront déployés, les dispositifs se connecteront aux services informatiques hébergés pour traiter nos commandes vocales, la réalité augmentée continuera de se développer et les interfaces biométriques, telles que la reconnaissance faciale ou vocale, deviendront la norme.

Outre les capacités améliorées des nouveaux dispositifs, les usagers disposeront de toute la puissance de calcul des services informatiques hébergés, conditionnés dans un kit intégré facile d'utilisation. Les personnes physiques seront capables de générer des informations et de les télécharger dans les services informatiques hébergés à une échelle sans précédent. Elles traiteront continuellement leurs

propres données à caractère personnel ainsi que celles d'autres personnes.

• L'IPv6. Les dernières adresses IPv4 restantes (le schéma d'adressage du réseau actuellement utilisé dans l'internet) ont été attribuées en 2011, et l'attention se tourne à présent vers l'IPv6. Cette nouvelle norme offre notamment un espace d'adresses IP pratiquement illimité et elle permet par conséquent d'allouer un identifiant unique à chaque dispositif connecté au réseau (par exemple, dispositifs RFID utilisant l'IP). Les adresses IP ne seront plus une ressource rare et il sera plus économique d'attribuer un identifiant unique qu'une adresse dynamique.

Dans ce contexte, la résolution adoptée lors de la conférence internationale sur la vie privée à Mexico¹⁴ concernant l'IPv6 est pertinente. Cette résolution exige que les identifiants uniques ne soient pas utilisés sans le consentement des utilisateurs finaux et que les utilisateurs finaux soient autorisés à utiliser des adresses IPv6 temporaires et instables (adresses dynamiques) par défaut. Il convient en outre de tenir compte des questions de sécurité que peut soulever le passage de l'IPv4 à l'IPv6.

• De nouvelles interfaces homme-machine deviendront disponibles. Les tablettes et les téléphones intelligents actuels ont rendu la communication entre les êtres humains et les machines plus facile. Bientôt, ces interfaces seront incorporées dans d'autres dispositifs tels que les systèmes de sécurité, les voitures, les télévisions et les systèmes de jeux. Les interfaces tactiles, portables, visuelles et vocales feront partie de notre vie quotidienne. Des systèmes d'information conçus pour aider les êtres humains seront capables de détecter et d'interpréter les visages, les mouvements, les voix, les comportements et même l'état de santé. En effet, des systèmes intelligents seront bientôt capables de surveiller l'état physique et même psychologique des êtres humains en se fondant sur des schémas comportementaux. Une application de services de santé électronique, surveillant les patients à distance pour qu'ils puissent rester à domicile au lieu d'être hospitalisés, présente des avantages pour l'individu et peut potentiellement générer des économies de coûts, mais elle ne devrait pas être mise en œuvre aux dépens du droit à la protection des données et de la vie privée.

Ces développements auront une influence énorme d'un point de vue social, et la protection des données devrait notamment jouer un rôle croissant

¹³ La norme LTE est une norme de communication sans fil de données à haut débit pour les téléphones mobiles et les terminaux. Elle est fondée sur les technologies de réseau GSM/EDGE et UMTS/HSPA, accroissant la capacité et la vitesse à l'aide de nouvelles techniques de modulation. La norme est élaborée par le 3GPP (*3rd Generation Partnership Project*). Elle permet des vitesses allant jusqu'à 300 Mbit/s.

¹⁴ Voir également le point 4.6 du présent rapport annuel.

pour vérifier que des garanties appropriées sont prévues et que le principe de prise en compte du respect de la vie privée dès la conception est appliqué lors de la mise en œuvre de ces technologies. Il est possible de trouver des solutions qui permettent d'obtenir une pleine fonctionnalité tout en préservant la vie privée des personnes physiques si les systèmes sont bien conçus dès le début.

• **Les réseaux intelligents.** Diverses technologies de réseau émergentes commencent à prendre forme, par exemple: le V2G (*Vehicle to Grid* - du véhicule au réseau), les systèmes de gestion des pannes (*Outage Management Systems - OMS*) ou les microréseaux. En particulier, les entreprises de services publics (eau et électricité principalement) ont déjà commencé à déployer des systèmes de comptage faisant appel à des technologies de pointe qui fourniront des informations bien plus détaillées concernant les modes de consommation au fournisseur de services publics et finalement aussi au consommateur. Ces informations permettront de mieux prévoir les demandes des consommateurs et de mieux adapter le réseau, et l'on peut espérer qu'elles renforceront l'efficacité d'utilisation des ressources rares telles que l'eau ou l'énergie, notamment par l'automatisation des réseaux de distribution.

Cependant, la notion de réseau intelligent est large et peut avoir de lourdes conséquences, car les dispositifs intelligents se connectent au réseau et échangent des informations. Outre les avantages économiques possibles, il est également évident qu'une quantité inégalée d'informations concernant le comportement des individus seront transmises et traitées par une foule d'acteurs.

Par conséquent, afin de préserver le droit à la protection des données des personnes physiques, ces traitements de données doivent être équilibrés et les principes de protection des données, tels que la proportionnalité, la nécessité ou la légitimité, doivent être appliqués correctement.

• **Des problèmes de sécurité accrus** rendront la cybersécurité plus importante que jamais. Même si la valeur totale de l'économie cybercriminelle n'est pas encore connue, la plus récente estimation des pertes subies par les seules entreprises au niveau mondial s'élève à quelque 750 milliards d'euros par an.¹⁵ Le nombre de délits informatiques augmente et les activités criminelles se sophistiquent et s'internationalisent de plus en plus. Il apparaît clairement que des

groupes criminels organisés se développent, avec la création de nouveaux groupes issus des pirates informatiques et de la cyberculture et même avec la participation de certains gouvernements.

Il convient d'accorder une attention particulière aux diverses règles juridiques afin de garantir l'adoption de mesures de sécurité appropriées pour protéger les données à caractère personnel, ainsi qu'à l'harmonisation de ces mesures et des procédures de notification des violations de données aux autorités compétentes et aux personnes concernées. En particulier, il convient de noter que le nouveau règlement général relatif à la protection des données proposé par la Commission étendra l'obligation de notifier les violations de données à tous les responsables du traitement des données¹⁶.

Les systèmes d'information deviennent progressivement des éléments essentiels de nos vies quotidiennes, et les personnes physiques doivent compter sur une technologie et des systèmes qu'ils ne comprennent pas complètement. Il faut donc que des tierces parties leur fournissent des mécanismes d'assurance capables de garantir la confidentialité et la sécurité de ces systèmes d'information. Dans ce contexte, on peut prévoir une croissance continue de l'activité de certification et également des procédures prévoyant une responsabilisation en matière de bonnes pratiques.

3.13. Priorités pour 2012

En janvier 2012, le CEPD publiera son sixième inventaire public en tant que conseiller sur les propositions législatives européennes, définissant ses priorités dans le domaine de la consultation pour l'année à venir. Le CEPD doit relever le défi consistant à remplir un rôle sans cesse croissant dans la procédure législative, tout en garantissant une contribution qualitative élevée et appréciée au processus législatif, 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:

- Il existe une tendance croissante à doter les autorités administratives, à la fois au niveau de

¹⁵ http://ec.europa.eu/home-affairs/policies/crime/crime_cybercrime_en.htm

¹⁶ La directive 2002/58, telle que modifiée par la directive 2009/136, établit uniquement l'obligation de notifier les violations de données à caractère personnel pour les fournisseurs de services de communications électroniques.

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.

- 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 partie 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 pendant la procédure législative, en raison des conséquences graves que ces échanges peuvent avoir sur la protection de la vie privée des citoyens, par exemple en facilitant la surveillance de leur vie.
- Ces dernières années ont été caractérisées par d'importants développements technologiques, essentiellement en raison de l'utilisation généralisée de l'internet et des technologies de géolocalisation. De tels développements ont des répercussions importantes sur les droits des citoyens en matière de protection de la vie privée et des données.

De tels 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 le CEPD va recevoir un nombre croissant de demandes de conseils concernant des propositions de mesures législatives.

Eu égard à ces circonstances, le CEPD a recensé les questions d'importance stratégique formant la pierre angulaire de son travail consultatif pour 2012, sans omettre toutefois d'autres procédures législatives touchant à la protection des données à caractère personnel.

Le CEPD s'engage dès lors à consacrer des ressources considérables en 2012 à l'analyse des propositions d'importance stratégique. Il a en outre recensé plusieurs initiatives de moindre importance stratégique qui peuvent néanmoins être pertinentes pour la protection des données. Le fait que ces initiatives figurent dans l'inventaire du CEPD implique qu'elles seront régulièrement surveillées, mais pas qu'elles feront systématiquement l'objet d'un avis ou d'observations formelles du CEPD.

Les principales priorités du CEPD, telles que définies dans son inventaire, sont les suivantes:

- a. **Vers un nouveau cadre juridique** de la protection des données
 - Révision du cadre de l'UE pour la protection des données
- b. Développements technologiques et stratégie numérique, droits de propriété intellectuelle et internet
 - Cadre paneuropéen pour l'identification, l'authentification et la signature électroniques
 - Contrôle de l'internet (notamment l'application des droits de propriété intellectuelle et les procédures de retrait)
 - Services d'informatique dématérialisée
 - «Santé électronique»
- c. Développement de l'espace de liberté, de sécurité et de justice
 - UE-PNR (données des dossiers des passagers)
 - UE-SSFT (système européen de surveillance du financement du terrorisme)
 - Contrôles aux frontières
 - Révision de la directive sur la conservation des données
 - Négociations sur les accords avec les pays tiers en matière de protection des données
- d. Réforme du secteur financier
 - Réglementation et supervision des marchés et acteurs financiers

4

COOPÉRATION

4.1. Groupe de travail «Article 29»

Le groupe de travail «Article 29» est l'organe consultatif indépendant institué par l'article 29 de la directive sur la protection des données (95/46/CE). Il fournit à la Commission européenne des 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.¹⁷

Ses missions, définies à l'article 30 de la directive, peuvent être résumées de la façon suivante:

- apporter l'expertise de chaque État membre à la Commission européenne sur les questions liées à la protection des données;
- promouvoir l'application uniforme des principes généraux de la directive dans tous les États membres au moyen d'une coopération entre les autorités de surveillance de la protection des données;
- donner à la Commission des conseils sur toute mesure affectant les droits et libertés des

¹⁷ Le groupe de travail est composé de représentants des autorités nationales de contrôle de chaque État membre, d'un représentant de l'autorité créée pour les institutions et les organismes de l'Union (c'est-à-dire le CEPD) et d'un représentant de la Commission. Cette dernière assure également le secrétariat du groupe. Les autorités nationales de contrôle de l'Islande, de la Norvège et du Liechtenstein (partenaires EEE) sont représentées en tant qu'observatrices.

personnes physiques à l'égard du traitement des données à caractère personnel;

- formuler des recommandations, à l'intention du public en général et des institutions de l'UE en particulier, sur des questions concernant la protection des personnes à l'égard du traitement des données à caractère personnel dans l'UE.

Membre du groupe de travail «Article 29» depuis début 2004, le CEPD considère ce groupe comme une plateforme très importante pour la coopération avec les autorités nationales de contrôle. Il est également évident que le groupe de travail devrait jouer un rôle central dans l'application cohérente de la directive et dans l'interprétation de ses principes généraux.

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

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

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

- l'avis 9/2011 sur la proposition révisée des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID) (WP 180);
- l'avis 10/2011 sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des **données des dossiers passagers** pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (WP 181);
- l'avis 15/2011 sur la définition du **consentement** (WP 187);
- l'avis 16/2011 sur le code de bonnes pratiques de l'AEEP et de l'IAB en matière de publicité comportementale en ligne (WP 188).

Le groupe de travail a également fait valoir sa position sous forme de lettres au sujet de plusieurs questions, parmi lesquelles la mise en œuvre du programme de surveillance du financement du terrorisme (TFTP) et le cadre d'autoréglementation en

matière de publicité comportementale en ligne (PCL) élaboré par le secteur.

Le CEPD a participé activement aux activités du groupe «Article 29» dans différents domaines. Il s'est particulièrement impliqué dans les activités de plusieurs sous-groupes, notamment le sous-groupe «technologie», le sous-groupe «frontières, voyages et application de la loi» (*BTLE - Border Travel and Law Enforcement*) et le sous-groupe «dispositions essentielles», qui a pour objectif de fournir une interprétation commune des dispositions essentielles de la directive 95/46/CE. Dans le cadre de ce dernier sous-groupe, le CEPD a été rapporteur pour avis sur la notion de **consentement** (avis 15/2011). Le CEPD s'est aussi fortement impliqué dans les activités du sous-groupe sur «l'avenir de la vie privée» concernant l'initiative de la Commission en vue d'un nouveau cadre juridique de protection des données.

Le CEPD coopère également avec les autorités nationales de contrôle 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). Cette coopération se fait au cas par cas.



Les défis technologiques ont fait partie des thèmes stratégiques principaux du groupe de travail Article 29 en 2011.

La coopération directe avec les autorités nationales est un élément qui revêt une importance croissante dans le contexte de l'élaboration de systèmes internationaux à grande échelle, tels qu'Eurodac, qui nécessitent une approche coordonnée de la supervision (voir les points 4.2 et 4.3).

4.2. Supervision conjointe d'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.¹⁸

En 2011, le groupe de coordination du contrôle d'Eurodac, composé de représentants des autorités nationales chargées de la protection des données et du CEPD, a fondé ses activités sur le programme de travail 2010-2011, adopté début 2010.

Le groupe a organisé deux réunions à Bruxelles, une en juin et une en octobre 2011. La réunion d'octobre était la première réunion entièrement organisée par le CEPD. Les participants l'ont considérée comme une réussite en ce qui concerne l'organisation et les résultats.

4.2.1 Rapport sur la suppression préalable des données

L'une des principales réalisations du groupe en 2011 a été l'inspection conjointe sur la suppression préalable des données. Par «suppression préalable des données», on entend la suppression de données renfermées dans l'unité centrale avant la fin de leur délai de conservation, par exemple si une personne quitte l'UE, devient citoyenne d'un État membre ou obtient un permis de séjour. La suppression de ces personnes de la base de données préserve leurs droits et accroît la qualité des données. L'un des objectifs de cet exercice était de présenter l'état d'avancement des règles relatives à la suppression préalable des

¹⁸ L'Islande, la Norvège et la Suisse et, depuis l'entrée en vigueur d'un protocole à cet effet le 1er avril 2011, le Liechtenstein.

données dans les États membres et d'étudier s'il est nécessaire de proposer d'autres solutions.

Le rapport final confirme que de nombreux États membres ont déjà mis en œuvre des procédures adéquates. Ceux qui ne l'ont pas encore fait ne rencontrent généralement que très peu, voire pas, de cas où une suppression préalable des données serait nécessaire. Le rapport encourage à créer de telles procédures lorsqu'elles n'existent toujours pas, à mieux informer les personnes concernées et à travailler vers de meilleures statistiques sur le phénomène.

Le rapport a été adressé aux principaux acteurs institutionnels de l'UE, ainsi qu'aux organisations internationales concernées.

4.2.2 Nouvel exercice pour 2012: empreintes digitales illisibles

Comme la réforme du règlement Eurodac n'a pas progressé en 2011, le groupe a dû adapter son programme de travail en conséquence en reportant plusieurs points. À la suite de cette adaptation, une nouvelle inspection conjointe sur la question des empreintes digitales illisibles est prévue pour 2012.

Le traitement des données biométriques, telles que les empreintes digitales, présente des difficultés particulières et crée des risques qui doivent être pris en considération. Dans ce contexte, le problème de «l'enregistrement impossible» - la situation où il s'avère, pour une raison ou une autre, que les empreintes digitales d'une personne ne sont pas utilisables - est l'un des principaux risques.

Le principal objectif de l'exercice est d'examiner les procédures actuellement appliquées dans tous les États membres lorsqu'une telle situation se présente et de déterminer s'il est nécessaire de proposer de nouvelles solutions. De façon analogue à l'exercice concernant la suppression préalable des données, cette enquête devrait surtout être considérée comme un exercice exploratoire, susceptible d'entraîner ultérieurement:

- le recensement de bonnes pratiques (sous la forme de caractéristiques techniques, de lignes directrices internes ou de pratiques administratives) et un encouragement à les utiliser largement;
- toute recommandation supplémentaire si l'exercice révèle des lacunes dans le système actuel.

4.2.3. Questionnaire de l'audit de sécurité coordonné

Au cours des deux réunions d'Eurodac de 2011, les préparatifs en cours en vue de l'audit de sécurité coordonné ont été examinés. Sur la base de la méthodologie utilisée dans un audit national, des efforts sont réalisés afin d'élaborer un cadre commun de méthodologie d'audit de sécurité susceptible d'aider les autorités nationales et, dans le même temps, de garantir des résultats cohérents et utiles à Eurodac en général. Les travaux dans ce domaine se poursuivront en 2012 en vue de l'adoption d'un cadre commun avant la fin de l'année.

4.2.4 Système d'information sur les visas

La création du système d'information sur les visas (VIS), en octobre 2011, a donné lieu à une discussion informelle au sein du groupe concernant sa supervision. Le groupe a convenu qu'une approche progressive et pragmatique devrait être mise en place avant la fin de l'année 2012. Cela signifie qu'une partie importante de l'ordre du jour des prochaines réunions d'Eurodac sera consacrée, même de façon informelle, au VIS.

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

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

Le SID enregistre des informations relatives aux produits de base, aux moyens de transport, aux personnes et aux entreprises, aux marchandises et aux liquidités détenues, saisies ou confisquées afin d'aider à prévenir, à rechercher et à poursuivre les opérations qui sont contraires aux réglementations douanière ou agricole (ancien premier pilier de l'UE) ou les infractions graves aux lois nationales (ancien troisième pilier de l'UE). 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° 766/2008¹⁹ - 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:

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

En 2011, le CEPD a organisé deux réunions du groupe de coordination du contrôle du SID (en juin et décembre). Les réunions ont regroupé les représentants des autorités nationales chargées de la protection des données, ainsi que des représentants de l'autorité de contrôle commune des douanes et du secrétariat chargé de la protection des données.

Lors de la réunion de juin, le groupe a élu M. Giovanni Buttarelli, contrôleur adjoint, président, et M. Gregor König, représentant autrichien et président de l'autorité de contrôle commune des douanes, vice-président. Le groupe a également examiné et adopté un programme de travail définissant ses activités pour 2011 et 2012, et a confirmé son intention de coopérer pleinement avec l'autorité de contrôle commune des douanes dans les domaines d'intérêt commun. Lors de la réunion de décembre, le groupe a examiné les documents qui orienteront ses premières inspections sur l'accès au système et les droits des personnes concernées, qui seront réalisées en 2012.

¹⁹ 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

4.4. Coopération policière et judiciaire: coopération avec les autorités de contrôle communes et le GTPJ

Le CEPD coopère également avec les autorités chargées du contrôle d'organes ou de systèmes d'information à grande échelle de l'UE, comme les autorités de contrôle communes d'Europol et d'Eurojust et les autorités de contrôle communes pour le système d'information Schengen (SIS) et les aspects de l'ancien troisième pilier du système d'information douanier (SID). Cette coopération prend la forme d'échanges d'informations réciproques sur des points présentant un intérêt commun, comme dans les cas où le CEPD et les autorités de contrôle communes (ACC) contrôlent chacune des parties différentes d'un même système.

En 2011, cette coopération a principalement porté sur le SID. Étant donné que le CEPD et l'ACC du SID partagent un rôle de contrôle pour le même système, il est logique de coordonner autant que possible leurs activités. Ainsi, le CEPD a invité des représentants de l'ACC à participer aux réunions organisées sur le contrôle coordonné du SID (voir le

point 4.3). Dans cet esprit, les représentants du CEPD ont été invités aux parties des réunions des ACC où des points d'intérêt commun étaient examinés.

Le CEPD participe également aux réunions et aux activités du groupe de travail sur la police et la justice (GTPJ). En 2011, le GTPJ a travaillé sur plusieurs questions telles que l'utilisation de profils ADN par les forces de l'ordre (y compris l'échange d'ADN par l'intermédiaire de la passerelle d'Interpol), l'établissement d'une politique commune de contrôle et l'évaluation des risques à l'égard du traitement des données à caractère personnel dans le domaine de l'application de la loi en Europe.

En 2011, le GTPJ a également abordé le sujet de son propre avenir au vu de l'implication croissante du groupe «Article 29» dans des domaines traditionnellement traités par le GTPJ. Lors de la conférence européenne (voir le point 4.5. Conférence européenne ci-dessous), le GTPJ a reçu pour mission d'œuvrer en faveur de l'intégration de ses compétences et de son expertise liées à l'UE dans le groupe de travail «Article 29» qui, à son tour, a été invité à préciser le statut de son sous-groupe sur l'application de la loi et les possibilités pour les États non membres de l'UE de participer aux activités de ce dernier.



L'utilisation de profils ADN par les forces de l'ordre a figuré à l'ordre du jour du GTPJ.

4.5. Conférence européenne

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

En 2011, la Conférence européenne des commissaires à la protection des données a eu lieu à Bruxelles, le 5 avril 2011. Le format pour la réunion était exceptionnel: la conférence était organisée par le CEPD, en étroite coopération avec le groupe de travail «Article 29» qui s'était également réuni le matin même.

La conférence a comporté des sessions consacrées à plusieurs questions variées, parmi lesquelles on peut citer:

- une vue d'ensemble des développements juridiques: traité de Lisbonne, cadre juridique de l'UE, Convention 108, lignes directrices de l'OCDE, etc.;
- le rôle du groupe de travail «Article 29»; et
- le contrôle de l'espace de liberté, de sécurité et de justice.

Le futur cadre de protection des données était alors encore en cours d'élaboration par la Commission européenne. Ce cadre a constitué un thème central des discussions et a donné lieu à l'adoption d'une résolution sur la nécessité d'un cadre complet de protection des données.

4.6. Conférence internationale

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

La 33^e conférence annuelle des commissaires à la vie privée et à la protection des données s'est tenue du 1^{er} au 3 novembre 2011 à Mexico et s'intitulait

«Privacy: The Global Age» (Vie privée: l'ère mondiale). La conférence visait à examiner des moyens permettant de renforcer les relations et les instruments nécessaires à la protection des données des personnes physiques au-delà des frontières nationales.

Le 31 octobre, une pré-conférence intitulée «Privacy as Freedom» (le respect de la vie privée comme liberté) a également eu lieu à Mexico, suivie le 1^{er} novembre de deux manifestations organisées par l'Organisation de coopération et de développement économiques et le commissaire à l'information et à la protection de la vie privée de l'Ontario, Canada. La conférence a permis aux acteurs européens de la protection des données de rencontrer leurs homologues du Canada, des États-Unis, d'Amérique latine, d'Australie, de Nouvelle Zélande, de la Chine et du Japon, pour n'en nommer que quelques-uns.

La session de clôture a été l'occasion de la présentation officielle de la «déclaration de Mexico», élaborée par l'autorité d'accueil avec la participation des autres délégations. Cette déclaration appelle les parties concernées à coopérer efficacement pour affronter les nouveaux défis, et notamment la mise en application efficace de la protection des données dans un monde caractérisé par une circulation massive des données à caractère personnel.

L'une des principales réalisations de la conférence a été l'initiative adoptée en vue de renforcer la coopération mondiale entre les commissaires à la vie privée et à la protection des données. Un comité exécutif a été créé – sous la présidence du président du groupe de travail «Article 29» et avec des participants du monde entier – afin de conférer une plus grande pérennité à la conférence internationale entre ses réunions annuelles. Une attention particulière sera accordée à la coopération mondiale pour l'application des législations protégeant la vie privée, et une réunion à part sur les questions de mise en application est prévue en mai 2012, à Montréal.

Peter Hustinx, contrôleur, et Giovanni Buttarelli, contrôleur adjoint, faisaient partie des orateurs et ont animé des sessions de la conférence.

La 34^e conférence internationale aura lieu en Uruguay, en octobre 2012.

5

INFORMATION ET COMMUNICATION

5.1. Introduction

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

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

5.2. Caractéristiques de la communication

La politique de communication du CEPD est conçue en fonction de caractéristiques particulières pertinentes du point de vue de l'âge, de la taille et des compétences de l'institution ainsi que des besoins de ses parties prenantes. Le CEPD personnalise les outils pour les adapter aux publics concernés, ces outils devant pouvoir être adaptés à un certain nombre de contraintes et d'exigences.

5.2.1. Principaux publics et groupes cibles

Les politiques et les activités de communication de la majorité des autres institutions et organes de l'UE sont conduites à un niveau général pour s'adresser à l'ensemble des citoyens de l'Union. Le champ d'action direct du CEPD est plus restreint. Il s'adresse avant tout aux parties prenantes du CEPD - les 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 homologues du secteur de la protection des données. Il n'est donc pas nécessaire que la politique de communication du CEPD suive une stratégie de «communication de masse». Au contraire, la sensibilisation des citoyens de l'UE aux questions liées à la protection des données, au niveau des États membres, repose sur une approche plus indirecte passant par exemple par les autorités nationales chargées de la protection des données.

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

5.2.2. Politique linguistique

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

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

Depuis 2010, le CEPD transmet ses messages dans ses communiqués de presse et ses autres activités de communication en au moins trois langues: l'anglais, le français et l'allemand. L'objectif général est d'atteindre le public le plus large possible.

5.3. Relations avec les médias

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

5.3.1. Communiqués de presse

En 2011, le service de presse a publié 12 communiqués de presse. La plupart de ces communiqués concernaient le travail du CEPD dans le domaine de la consultation et, plus spécifiquement, les **nouveaux avis législatifs** présentant un intérêt immédiat pour le grand public. Ils couvraient des thèmes tels que la stratégie européenne de réforme en matière de protection des données, le guide de bonnes pratiques sur la protection des données et la transparence, le système de l'Union européenne relatif aux dossiers passagers, le règlement financier de l'UE, l'évaluation de la directive sur la conservation des données, la publicité comportementale en ligne, l'appareil de contrôle dans le domaine des transports par route, la neutralité de l'internet et le système d'information du marché intérieur.

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

5.3.2. Interviews

En 2011, le CEPD a accordé 14 interviews directes à des journalistes de la presse écrite, de la radiotélévision et des médias électroniques en Europe, un grand nombre de demandes émanant de la presse allemande, autrichienne, néerlandaise et française, ainsi que de la presse spécialisée de l'UE.

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

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 des thèmes plus spécifiques qui ont fait la une des journaux en 2011,

comme l'accord entre l'UE et les États-Unis sur les transferts de données, la révision du cadre juridique européen de protection des données, les préoccupations de vie privée dans le contexte des réseaux sociaux, l'établissement de profils de consommateurs, les droits des citoyens numériques, ainsi que la conservation et la sécurité des données.

5.3.3. Conférence de presse

Le 15 juin 2011, le CEPD a organisé une conférence de presse au Parlement européen, à Bruxelles, afin de présenter son rapport annuel 2010 et de décrire les principaux aspects de ses activités en 2010 du point de vue de ses tâches de supervision, de consultation et de coopération (voir le point 5.7.1.).

La conférence de presse a permis à Peter Hustinx, Contrôleur, et à Giovanni Buttarelli, Contrôleur adjoint, d'aborder le contexte dynamique actuel de la protection des données dans l'UE et les défis à venir et de répondre aux questions posées par les journalistes.

5.3.4. Demandes formulées par les médias

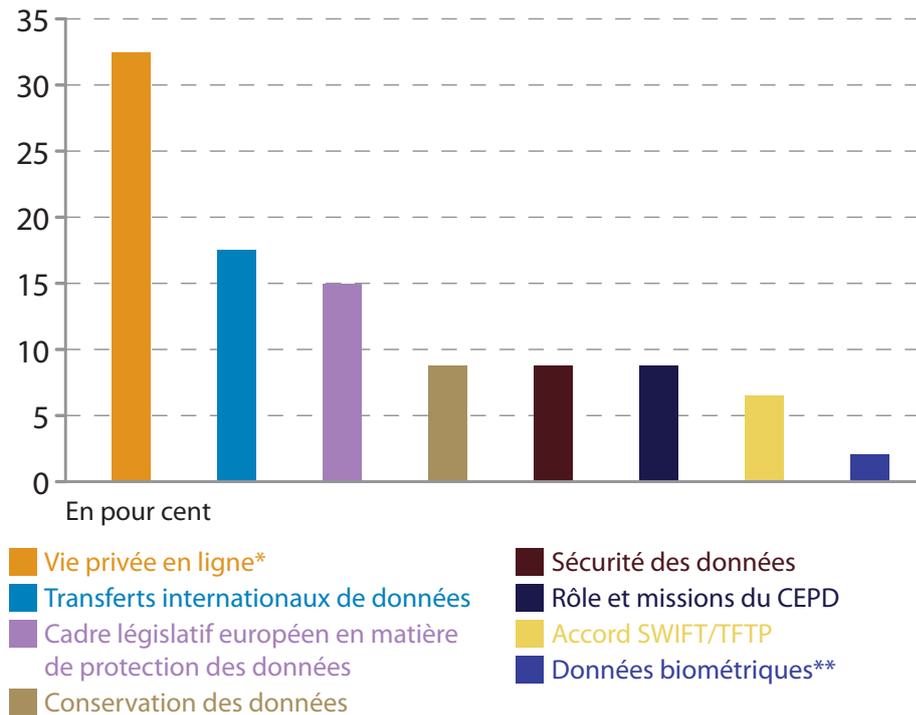
En 2011, le CEPD a reçu quelque 46 demandes écrites formulées par les médias qui comprenaient des demandes de commentaires et des demandes de clarification, de position ou d'information. En 2011, l'attention des médias s'est portée principalement sur la question de la vie privée en ligne, notamment en ce qui concerne les nouvelles applications en ligne comme les applications de géolocalisation, les moteurs de recherche et - le domaine arrivant en tête du nombre de demandes - les réseaux sociaux.

Parmi les autres dossiers intéressant les médias, on peut citer les transferts internationaux de données, la révision du cadre juridique de l'Union en matière de protection des données, la directive sur la conservation des données, la sécurité des données et les dispositions relatives aux violations de données, ainsi que l'utilisation des données des dossiers passagers et leur transfert aux États-Unis.



Peter Hustinx et Giovanni Buttarelli ont présenté le rapport annuel 2010 du CEPD au cours d'une conférence de presse.

Principaux sujets des demandes émanant de la presse en 2011



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

** y compris le système d'information Schengen.

5.4. Demandes d'informations et de conseils

Le nombre de demandes d'information ou d'aide présentées par les citoyens a augmenté de 39 % entre 2010 et 2011 (196 demandes contre 141 en 2010). Cette évolution est liée à la meilleure visibilité du CEPD dans le domaine de la protection des données, qui a été renforcée au moyen de divers outils d'information et de communication.

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

La plus grande catégorie de demandes reçues en 2011 concernait des plaintes des citoyens de l'UE concernant des questions pour lesquelles le CEPD

n'est pas compétent. Elles portaient la plupart du temps sur des violations présumées de la protection des données par les pouvoirs publics, par des entreprises publiques ou privées et par des services et technologies en ligne, comme les jeux de hasard en ligne, les blogs, les services de géolocalisation, les réseaux sociaux et les outils de messagerie. Les autres sujets concernés étaient par exemple la sécurité des données bancaires, le droit d'accès aux documents détenus par les administrations nationales, la diffusion de données à caractère personnel à des tierces parties sans le consentement de la personne concernée et des demandes d'appel contre la décision d'une autorité nationale chargée de la protection des données. Lorsque ces types de plaintes ne relèvent pas de la compétence du CEPD, une réponse est envoyée 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.

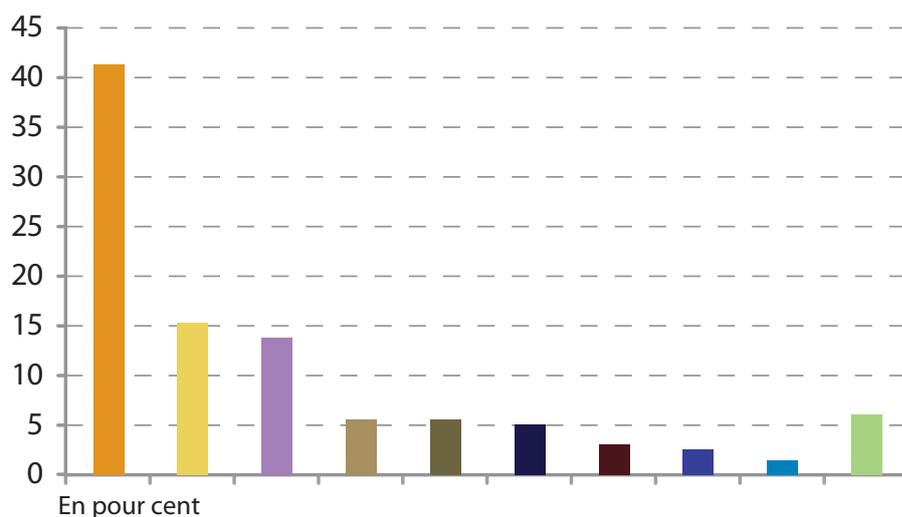
La deuxième catégorie de demandes reçues en 2011 concernait la législation relative à la protection des données dans les États membres de l'UE et/ou sa mise en œuvre au niveau national. Dans de tels cas, le CEPD conseille à la personne de contacter l'autorité chargée de la protection des données

concernée et, le cas échéant, l'unité de protection des données de la Commission européenne.

La troisième catégorie de demandes d'informations concernait les questions de protection des données au sein de l'administration de l'UE, telles que les activités de traitement des institutions, organes et agences de l'UE.

Les autres catégories de demandes d'informations incluaient des demandes concernant les activités, le rôle et les missions du CEPD, la protection des données dans la législation de l'UE, la vie privée en ligne, le transfert international de données, les systèmes d'information à grande échelle tels que le VIS, le SIS et Eurodac, et la révision du cadre de l'UE pour la protection des données.

Principaux domaines de demandes d'information émanant du public en 2011



- Réclamations pour lesquelles le CEPD n'est pas compétent
- Législation nationale de protection des données
- Problèmes de protection des données dans l'administration de l'UE
- Missions et activités du CEPD
- Droit européen de la protection des données
- Vie privée en ligne
- Transferts internationaux de données
- Systèmes d'information à grande échelle (SIS, VIS, Eurodac)
- Réforme du cadre législatif européen en matière de protection des données
- Autres

5.5. Visites d'étude

Dans le cadre des efforts fournis pour renforcer la visibilité de la protection des données et l'interaction avec le monde universitaire, le CEPD accueille régulièrement des groupes spécialisés dans les domaines du droit européen, de la protection des données et/ou de la sécurité des technologies de l'information. En 2011, le bureau du CEPD a accueilli quatre groupes d'étudiants venus de différents pays. En décembre 2011, par exemple, le CEPD a accueilli un groupe d'étudiants en droit allemand et européen de l'université de Cologne en Allemagne, a présenté son rôle et ses activités et a évoqué les questions de protection des données au niveau de

l'UE. D'autres groupes de visiteurs sont également venus de l'institut de droit scientifique et technologique de Taipei à Taïwan, de l'université technologique de Nanyang à Singapour et de l'université Pierre Mendès France de Grenoble en France.

Pour atteindre un public plus large, le bureau du CEPD a également accueilli quatre groupes ou associations s'intéressant aux questions de protection des données et de la vie privée: des membres de l'église évangélique allemande, l'association des jeunes européens de Bordeaux en France, le collège de Police (*Politieacademie*) aux Pays-Bas et la sous-commission «communication» des stagiaires de la Commission européenne.

5.6. Outils d'information en ligne

5.6.1. Site internet

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

Évolution du site internet

La principale modification apportée au site internet en 2011 est une plateforme électronique pour le dépôt des réclamations. Le formulaire de réclamation en ligne facilite le processus de dépôt des réclamations et accélère leur traitement par les services du CEPD.

Comme annoncé dans le rapport annuel 2010, une rubrique «kit presse» a également été créée sur le site internet afin de fournir aux professionnels des médias des informations et des ressources pertinentes qu'ils pourront utiliser dans leurs articles et reportages.

Entre septembre et novembre 2011, une enquête en ligne a été réalisée sur la qualité du site internet du CEPD. En général, les avis sur le site internet étaient positifs: la majorité des personnes ont trouvé le contenu du site internet satisfaisant. Elles ont également estimé que les informations étaient exactes, actualisées et faciles à comprendre. Bien que le site ait été considéré comme plutôt facile à utiliser, des améliorations supplémentaires seront apportées à la fonction «recherche avancée» et au registre en 2012.

De plus, une refonte des rubriques «supervision» et «consultation» est prévue afin d'améliorer les options de recherche et la navigation dans les catégories thématiques. D'autres améliorations incluront la création d'un Coin des délégués à la protection des données et l'application d'une caractéristique de flux RSS.

Trafic et navigation

Une analyse des données relatives au trafic et à la navigation montre que le site internet a accueilli au

total 65 599 visiteurs uniques en 2011, dont plus de 6 000 par mois en janvier, mai et juin.

Après la page d'accueil, les pages les plus régulièrement consultées étaient les pages «Presse et actualités», «Supervision» et «Consultation», même si les pages «Publications» et «Événements» étaient également populaires. Les statistiques montrent également que la plupart des visiteurs accèdent au site internet par l'intermédiaire d'une adresse directe, d'un onglet, d'un lien dans un courrier électronique ou d'un lien sur un autre site (portail Europa ou site internet d'une autorité nationale chargée de la protection des données). Rares sont les visiteurs qui utilisent les liens des moteurs de recherche.

5.6.2. Newsletter

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

Quatre numéros de la newsletter du CEPD ont été publiés en 2011, soit en moyenne un tous les trois mois. Le nombre d'abonnés est passé de 1 500 fin 2010 à environ 1 750 avant la fin 2011. 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.

5.7. Publications

5.7.1. Rapport annuel

Le rapport annuel constitue une publication essentielle du CEPD. Il présente un aperçu des activités du CEPD au cours de l'année concernée dans les principaux domaines opérationnels que sont la supervision, la consultation et la coopération, et fixe les principales priorités pour l'année suivante. Il décrit en outre les réalisations en termes



Rapport annuel 2010 du CEPSD

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 CEPSD.

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 de la protection des données, les groupes d'intérêt et ONG actifs dans ce domaine, ainsi que les journalistes et toute personne recherchant des informations sur la protection des données à caractère personnel au niveau de l'UE.

Le contrôleur et le contrôleur adjoint ont présenté le rapport annuel 2010 du CEPSD à la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen, le 15 juin 2011. Les caractéristiques essentielles du rapport ont également été présentées lors de la conférence de presse qui a eu lieu le même jour.

5.7.2. Publications thématiques

Les travaux préparatoires sur des fiches d'information thématiques portant sur des questions de protection des données d'importance stratégique pour le CEPSD ont commencé. L'objectif est de publier des informations ciblées qui serviront d'orientation au grand public et aux autres parties intéressées. La première série de fiches d'information couvrira des sujets tels que les violations de données, la

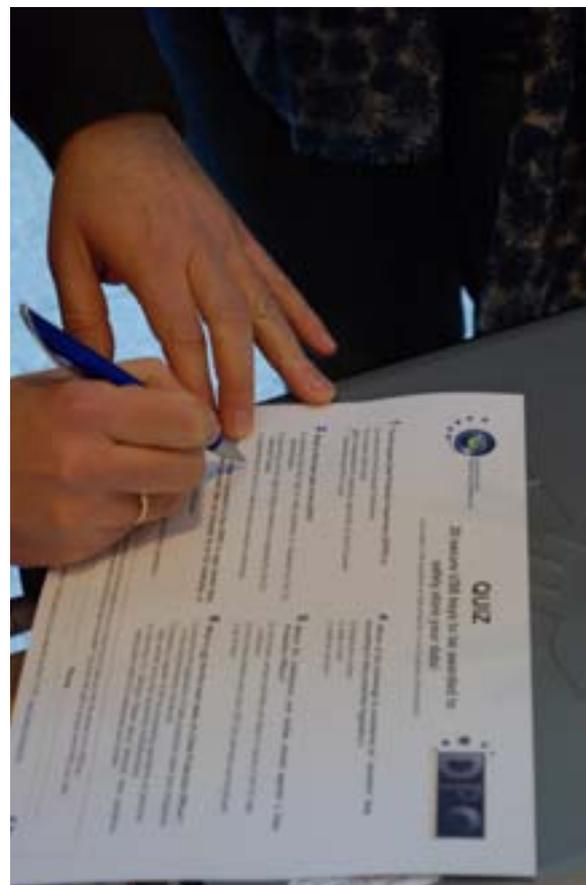
protection de la vie privée dans les communications électroniques, l'accord SWIFT/TFTP et les données des dossiers passagers (données PNR).

5.8. Actions de sensibilisation

Le CEPSD tient 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.

5.8.1. Journée de la protection des données 2011

Les États membres du Conseil de l'Europe et les institutions et organes de l'Union européenne ont célébré le 28 janvier 2011 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.



Visiteur remplissant un quiz au stand d'information du CEPSD pendant la Journée de la protection des données 2011.

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

Le CEPD a renouvelé cette activité spécifique en 2011 tout en consacrant davantage d'efforts à la sensibilisation du personnel des institutions européennes. Un message vidéo du contrôleur et du contrôleur adjoint a également été diffusé aux parties prenantes institutionnelles et mis à disposition sur le site internet du CEPD, en version courte et en version longue, afin de présenter le rôle du CEPD et de décrire les défis de l'année.

Le CEPD a également pris part à diverses manifestations organisées à l'occasion de la Journée de la protection des données, telles que la conférence

internationale «Ordinateurs, vie privée et protection des données», 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. Pour cette quatrième édition internationale, le thème de la conférence était «European Data Protection: In Good Health?» (La protection des données européenne est-elle en bonne santé?). La conférence s'est déroulée du 25 au 27 janvier 2011, avec deux manifestations d'une journée sur la «santé électronique» et la surveillance et une table ronde sur les scanners corporels. Les membres du secrétariat du CEPD ont participé à des tables rondes et Peter Hustinx a prononcé les remarques de clôture de la conférence.

5.8.2. Journée portes ouvertes de l'UE 2011

Le 7 mai 2011, le CEPD a participé, comme chaque année, à la Journée portes ouvertes des institutions européennes organisée au Parlement européen à Bruxelles. La Journée portes ouvertes de l'Union européenne offre au CEPD une excellente occasion de sensibiliser le public à la nécessité de protéger la vie privée et les informations à caractère personnel.



Visiteurs jouant avec une caméra thermique au stand du CEPD pendant la Journée portes ouvertes de l'UE 2011 au Parlement européen.

Des membres du personnel du CEPD étaient présents pour répondre aux questions des visiteurs au stand du CEPD, dans le bâtiment principal du Parlement européen. Comme lors de la Journée de la protection des données, un quiz sur la protection de la vie privée et des données au niveau de l'Union a été distribué aux visiteurs, ainsi que différents supports d'information. L'installation d'une caméra thermique reliée à un grand écran a été l'une des principales attractions du stand. Bien que n'ayant pas de lien direct avec le traitement des données à caractère personnel, cette attraction a permis de sensibiliser les citoyens, d'une manière originale et amusante, au risque potentiel que représentent les nouvelles technologies pour la vie privée.

6

ADMINISTRATION, BUDGET ET PERSONNEL

6.1. Introduction

L'entrée en vigueur du traité de Lisbonne a eu des répercussions directes sur les activités et les tâches du CEPD. Le traité confère une plus grande importance à la protection des données dans les institutions et organes de l'UE, ce qui a augmenté la charge de travail de l'institution et, à son tour, celle de l'unité Ressources humaines, budget et administration (HRBA).

La croissance modérée du tableau des effectifs du CEPD prévue ces dernières années n'a pas permis d'assumer ces nouvelles tâches et responsabilités, et il a fallu engager plusieurs agents contractuels et agents temporaires et négocier le détachement d'experts de la protection des données des autres institutions de l'Union européenne et autorités chargées de la protection des données des États membres pour aider le CEPD à faire face à l'accroissement de sa charge de travail.

En 2011, une gestion plus stratégique et efficace des priorités et des ressources a été établie. Une telle gestion revêt une importance particulière en des temps d'austérité et de consolidation budgétaire. Une révision stratégique du CEPD a été entreprise au cours de l'année, et un groupe de travail «révision stratégique» a été créé, avec des représentants de toutes les équipes et sous la présidence du directeur du CEPD. En octobre 2011, une conférence interne a permis aux différentes équipes du CEPD de réfléchir à leurs missions, valeurs et objectifs respectifs, et de définir ceux du CEPD pour les années à venir. Cette conférence sera suivie en 2012 par une consultation externe

des parties prenantes, au moyen d'enquêtes en ligne, de groupes thématiques et d'ateliers. Les résultats seront présentés à l'occasion d'une conférence publique.

En 2011, les efforts visant à améliorer l'efficacité ont produit des résultats tangibles, tels que l'accès au catalogue des formations de la Commission européenne par l'intermédiaire du système Syslog Formation, l'adoption de manuels internes détaillés traitant du recrutement de plusieurs catégories de personnel et un nouveau mécanisme de contrôle budgétaire qui a entraîné une hausse importante du taux d'exécution du budget.

Les améliorations apportées à l'efficacité de la fonction RH se poursuivront en 2012, lorsqu'il sera possible d'accéder aux systèmes Sysper (système de gestion des dossiers du personnel) et MIPS (une application destinée à coordonner les missions). Ces systèmes faciliteront l'accomplissement de certaines tâches administratives courantes et libéreront des ressources pour mieux positionner l'équipe des ressources humaines en tant que partenaire stratégique fiable du conseil d'administration du CEPD.

6.2. Budget

Le budget alloué au CEPD en 2011 s'élevait à 7 564 137 euros, ce qui correspondait à une hausse de 6,47 % par rapport à l'année précédente. Cependant, étant donné le développement global de l'institution et l'accroissement de sa charge de travail, cela a représenté une croissance modérée.

Cette modeste augmentation du budget a été essentiellement absorbée par la ligne budgétaire consacrée aux salaires qui, en termes monétaires, est le poste le plus important du budget du CEPD. Une part importante du budget a été consacrée à la traduction, dans toutes les langues officielles, des avis du CEPD sur des propositions législatives. Une fois traduits, les avis peuvent être publiés au *Journal officiel de l'Union européenne*, à proximité des textes législatifs de l'UE et de la jurisprudence de la Cour européenne de justice, garantissant que les opinions du CEPD sont faciles d'accès pour les praticiens comme pour les tribunaux. Les autres documents adoptés par le CEPD (par exemple, les avis de contrôle préalable) sont traduits dans les langues de travail du CEPD (anglais, français et allemand).

La déclaration d'assurance (DAS) 2010 de la Cour des comptes européenne n'a pas fait état de préoccupations concernant le CEPD ni émis de recommandations à son intention. Néanmoins, dans le cadre d'une gestion financière saine et en vue d'améliorer la fiabilité et la qualité des données financières du CEPD:

- a) un nouveau système de vérification financière interne, incluant des listes de vérification pour tous les niveaux de transactions financières, a été introduit dans le flux de travail financier;
- b) un rapport trimestriel sur l'exécution du budget, y compris un suivi de la consommation budgétaire ligne par ligne, a été mis en œuvre;

c) de nouveaux formulaires de mission ont été adoptés pour permettre un meilleur contrôle et une transparence accrue;

d) des lignes directrices concernant les marchés de faible valeur ont été élaborées; et

e) de nouveaux tableaux de rapports financiers ont été créés.

À la suite à ces initiatives, le taux d'exécution du budget du CEPD s'est considérablement amélioré: de 76 % en 2010 à près de 85 % en 2011.

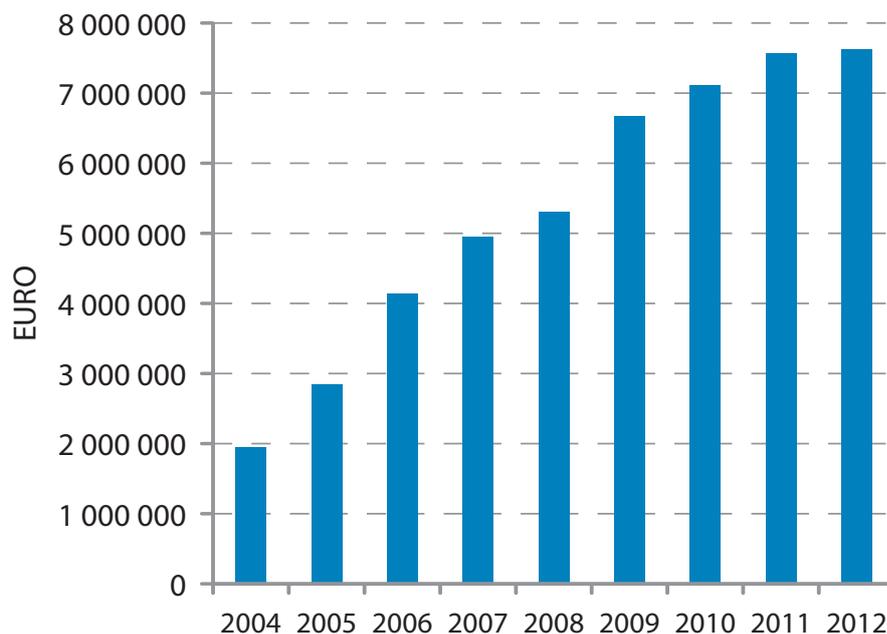
En 2011, la Commission européenne a continué d'apporter une assistance dans le domaine financier, notamment en ce qui concerne les services comptables - le comptable de la Commission est également le comptable du CEPD. En l'absence de règles spécifiques, le CEPD applique le règlement intérieur de la Commission pour l'exécution du budget.

6.3. Ressources humaines

6.3.1. Recrutement

Le nombre croissant des tâches et la visibilité accrue du CEPD entraînent progressivement un accroissement de la charge de travail et une expansion des activités qui doivent être gérés du point de vue des ressources humaines.

Évolution du budget du CEPD entre 2004 et 2012



Grâce à un accord de niveau de service avec l'Office européen de sélection du personnel (EPSO), un concours général sur la protection des données a été organisé en 2009 afin de recruter du personnel très spécialisé. Trois listes de réserve ont été publiées à l'été 2010 pour les grades AD9, AD6 et AST3, avec une validité de trois ans. À présent, 82 % des lauréats des trois listes ont été recrutés. Le recrutement au titre de la liste AST3 est ouvert à toutes les institutions de l'UE.

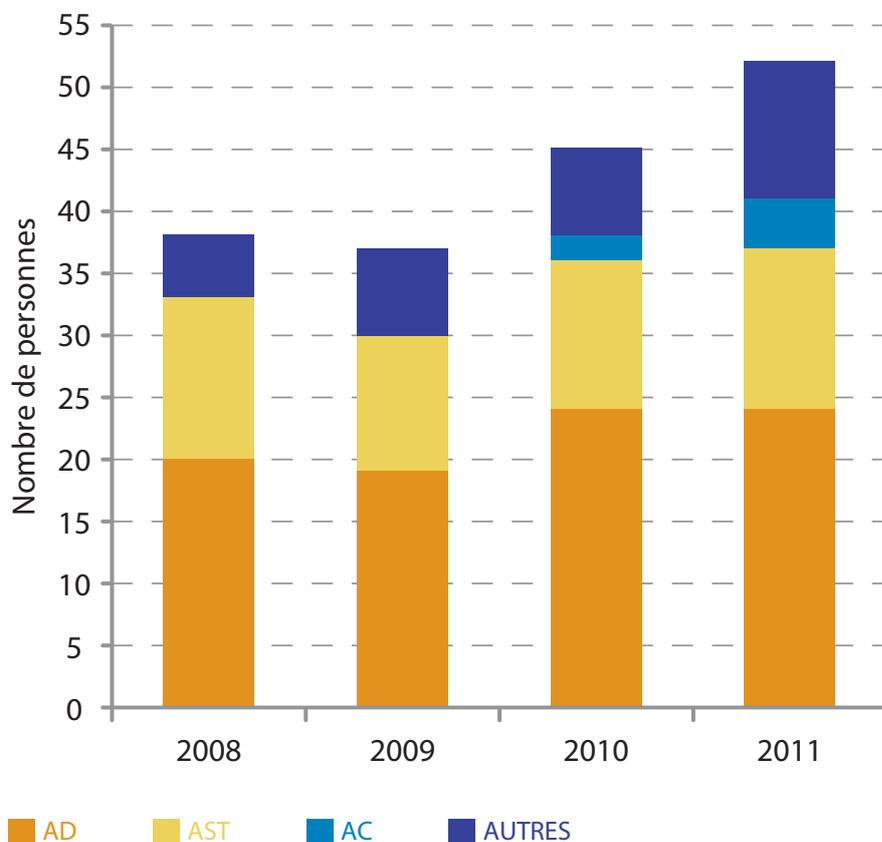
Après la publication de ces listes en 2010, le CEPD s'est lancé dans une grande opération de recrutement et a organisé des entretiens avec les candidats des listes de réserve et des fonctionnaires d'autres institutions, conformément à l'article 29 du statut du personnel. Cet effort de recrutement s'est poursuivi en 2011. Avant 2011, les nouveaux-venus étaient principalement sélectionnés à partir des listes de concours de l'EPSO. En 2011, le CEPD a commencé à recevoir 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.

Afin de traiter plus efficacement le nombre accru de demandes et de garantir un processus de recrutement équitable et professionnel, l'équipe des ressources humaines a publié plusieurs manuels de recrutement concernant toutes les catégories de personnel, définissant les procédures que le personnel des ressources humaines et les gestionnaires doivent suivre pendant le processus de recrutement.

Outre les fonctionnaires, le CEPD a recruté trois agents contractuels et l'ancien délégué à la protection des données du Conseil a été détaché auprès du CEPD, ce qui a renforcé l'unité 'Supervision'. Afin de couvrir des besoins temporaires en 2011, deux membres du personnel intérimaires et un contractant externe chargé de la maintenance et du développement du site internet du CEPD ont été embauchés. Au total, le CEPD a recruté 14 nouveaux collègues en 2011.

La procédure destinée à pourvoir le poste de directeur du secrétariat du CEPD, entamée fin 2010, a été menée à bien. À la suite d'une procédure de recrutement interinstitutionnel, le directeur a été sélectionné et nommé en mars 2011.

Évolution des effectifs du CEPD par catégorie



6.3.2. Programme de stages

Un programme de stages a été créé en 2005 afin d'offrir aux jeunes ayant un diplôme universitaire la possibilité de mettre en pratique leurs connaissances académiques, et d'acquérir ainsi une expérience pratique en participant aux activités quotidiennes du CEPD. Cela donne également à l'institution l'occasion d'accroître sa visibilité auprès des jeunes citoyens de l'UE, et notamment auprès des étudiants universitaires et des jeunes diplômés spécialisés dans la protection des données.

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, le CEPD peut également accueillir des stagiaires non rémunérés souhaitant acquérir de l'expérience dans le domaine de la protection des données, dans le cadre de leurs études ou de leur carrière professionnelle. Les critères sont définis dans la nouvelle décision adoptée par le CEPD le 25 octobre 2011, qui contient les règles régissant le programme de stages. Dans la nouvelle décision, une attention particulière est accordée aux aspects liés à la protection des données afin de mieux informer les candidats de leurs droits.

Tous les stagiaires, rémunérés ou non, contribuent à la fois au travail théorique et pratique, tout en acquérant une expérience directe utile.

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

6.3.3. 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 a permis au CEPD de bénéficier de leurs compétences et de leur expérience professionnelle et d'accroître sa visibilité au niveau national. À son tour, ce programme permet aux END de se familiariser avec les

questions de protection des données au niveau de l'UE. Un manuel interne régissant leur procédure de sélection a été publié en 2011.

6.3.4. Organigramme

L'organigramme du CEPD est resté inchangé entre sa création en 2004 et 2009, après quoi la première réorganisation a eu lieu avec la création du poste de directeur à la tête du secrétariat.

En 2010, l'organigramme du CEPD a connu un profond changement avec la réorganisation du personnel en cinq secteurs, avec des responsables de secteurs nommés à un niveau de management intermédiaire.

L'effort de recrutement considérable qui a suivi la publication des listes de réserve du concours de l'ESPO a entraîné une croissance substantielle de ces secteurs. Pour cette raison, en juin 2011, les trois plus grands secteurs du CEPD, à savoir «supervision et mise en application», «politique législative et consultation» et «ressources humaines, budget et administration», ont été transformés en unités.

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

6.3.5. Conditions de travail

Le régime d'horaire flexible a été introduit au CEPD en 2005 et est très apprécié du personnel. De nombreux collègues profitent de cette occasion pour équilibrer leur vie professionnelle et personnelle de façon équitable.

En 2011, la décision concernant l'horaire flexible a été révisée afin de rationaliser et simplifier la procédure et de garantir le traitement équitable de tout le personnel. En outre, la nouvelle décision harmonise les règles applicables au CEPD avec celles qui sont en place à la Commission européenne, afin de faciliter l'introduction du module de gestion du temps Sysper II en 2012.

En 2011, deux membres du personnel (un de l'unité des ressources humaines et un du comité du personnel) ont été nommés «personnes de confiance». Ces personnes sont à la disposition de tout le personnel pour discuter d'éventuelles affaires de harcèlement. Les deux fonctionnaires ont suivi une formation spécifique organisée par la Commission pour les préparer à traiter d'éventuels dossiers et à mettre en œuvre une politique spécifique contre le harcèlement.

6.3.6. Formation

Le système Syslog Web Formation a été mis en œuvre au CEPD en 2011. Ce système, qui permet d'accéder électroniquement au catalogue des formations de la Commission européenne, a entraîné une amélioration considérable de l'efficacité et de la rapidité de l'organisation des formations. En conséquence, l'essentiel du budget de formation a été consommé en 2011 (88 % du budget total, 102 499 euros).

| | |
|--|---------|
| Cours de formation générale (à la Commission, y compris des cours de langue) | 21,75 % |
| Cours de formation de l'EEA | 48,70 % |
| Cours de formation externes | 17,55 % |

Le taux élevé d'exécution du budget de formation indique la réussite de la réorganisation du CEPD et soutient l'objectif déclaré du conseil d'administration de l'institution de satisfaire les besoins du personnel du CEPD et de faire du CEPD un employeur attractif pour les fonctionnaires des autres institutions de l'UE.

L'EEA a organisé un cours spécialement conçu, intitulé «First steps in management» (premiers pas dans le management), à l'intention de 16 administrateurs du CEPD. Le cours était conçu pour transmettre des connaissances sur la gestion, en mettant l'accent sur les bases de la gestion d'équipe, de la diversité et de la communication. Le cours a permis au personnel de mieux comprendre les difficultés rencontrées par les cadres intermédiaires et de se préparer à assumer de futures responsabilités de management. En raison de son succès, le cours sera à nouveau organisé en 2012.

En 2011, les cadres intermédiaires du CEPD nommés en 2010 et 2011 ont suivi un cours spécifique de formation au management et ont également bénéficié d'un programme d'accompagnement professionnel individuel et collectif proposé par le coordinateur de l'accompagnement professionnel de la Commission européenne. Cela a permis au directeur et aux chefs d'unité et de secteur de mieux fonctionner, en tant que gestionnaires individuels et en tant qu'équipe de gestion, avec pour résultat une amélioration tangible de la planification, de la coordination et de la mise en œuvre des politiques décidées par le conseil d'administration de l'institution.

Le CEPD a continué à participer à divers comités interinstitutionnels, qui facilitent le regroupement des besoins de formation et permettent de réaliser des

économies d'échelle dans un domaine où toutes les institutions de l'UE ont des besoins essentiellement similaires. Le sixième amendement au protocole sur les cours de langue a été signé en décembre 2011. Il s'agit d'un domaine où les demandes de formation ont également connu une hausse importante.

À la demande du coordinateur des formations, le CEPD a mis à jour sa décision relative aux formations en octobre 2011, permettant au personnel du CEPD de se voir offrir davantage de possibilités de formation.

6.3.7. 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 RH, budget et administration, qui leur remettent le guide administratif du CEPD et leur communiquent les informations concernant les procédures propres au CEPD.

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

En 2011, plusieurs activités sociales destinées au personnel du CEPD ont été organisées en étroite collaboration avec le comité du personnel de l'institution, et chaque manifestation a bénéficié d'un taux de participation élevé.

6.4. Fonctions de contrôle

6.4.1. Contrôle interne

Le système de contrôle interne, en vigueur depuis 2006, gère le risque de non-réalisation des objectifs. En 2011, des efforts considérables ont été réalisés pour mettre en œuvre les normes de contrôle

interne (NCI). La liste des actions a été élargie afin de garantir un contrôle interne plus efficace des processus en place. Par exemple, une action de sensibilisation à l'éthique, une harmonisation des titres de tout le personnel, un programme de par-rainage, une adaptation du nouveau flux de travail financier, un plan de continuité des opérations et une mise à jour du guide des missions ont tous été adoptés en relation avec le système de contrôle interne. Une décision mise à jour sur les normes de contrôle interne sera adoptée en 2012 pour simplifier l'approche, augmenter l'appropriation et renforcer l'efficacité de ces normes.

Le CEPD a pris acte du rapport d'activités annuel et de la déclaration d'assurance jointe signée par l'ordonnateur délégué. D'une manière générale, le CEPD estime que les systèmes de contrôle interne en place fournissent une assurance raisonnable quant à la légalité et à la régularité des opérations dont l'institution est responsable.

6.4.2. Audit interne

Le service d'audit interne (SAI) de la Commission agit également en tant qu'auditeur du CEPD. En janvier 2011, le service d'audit interne a effectué une visite d'évaluation des risques en vue d'élaborer sa stratégie d'audit du CEPD pour la période allant de 2011 à 2013. Il a soigneusement contrôlé toutes les procédures du CEPD, élaboré un profil de risque et défini des domaines déclenchant les visites d'audit.

En juillet 2011, le service d'audit interne a effectué, à la demande du CEPD, une visite spécifiquement consacrée à l'évaluation des risques informatiques. Comme le CEPD occupe une partie des locaux du Parlement européen et qu'il s'appuie sur l'infrastructure informatique de ce dernier, les travaux avec les services de l'information et des technologies du Parlement européen se poursuivront en 2012.

Enfin, un audit a été réalisé en novembre 2011 concernant les avis de contrôle préalable, les mesures administratives et les inspections. Le rapport de cet audit sera disponible en 2012.

Concernant le suivi des deux audits d'évaluation des risques, six recommandations n'ont pas encore été appliquées. Trois d'entre elles devraient être appliquées début 2012 et les trois autres seront traitées plus tard, en 2012 ou 2013, car elles concernent des projets à long terme tels que l'élaboration d'un système de gestion des dossiers (pour plus de détails, consulter le point 6.6.3) ou une politique de gestion des risques.

Comme les deux organisations partagent un intérêt commun en matière d'audits en ce qui concerne le respect de la protection des données, le CEPD a présenté un mémorandum d'accord au service d'audit interne afin de permettre aux deux organisations de jouer leur rôle le plus efficacement possible. Le mémorandum d'accord sera conclu en 2012, dans le plein respect des droits, des obligations et de l'indépendance définis dans l'acte de constitution de chaque organisation.

6.4.3. 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 des recettes et dépenses du CEPD 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 2010, le CEPD a répondu de façon satisfaisante aux questions posées par la Cour.

6.4.4. Sécurité

En 2011, d'importantes ressources dans le domaine de la sécurité ont été consacrées au système interne de gestion des dossiers du CEPD, qui sera spécialement conçu pour le CEPD et mis en œuvre en 2012, une attention particulière étant accordée aux mesures de sécurité à mettre en place. Le contrat avec la société qui développe le système a été signé en décembre 2011 avec l'aide du Parlement européen.

Bien qu'elle ne soit pas encore finalisée, la visite d'évaluation des risques informatiques réalisée par l'auditeur interne du CEPD en juillet 2011 a déjà suscité certaines initiatives, telles que la création d'un comité de pilotage informatique qui s'est réuni pour la première fois en janvier 2012.

Le CEPD a également adopté un plan de continuité des activités (PCA) concernant les conditions de santé et de sécurité des personnes et des lieux en 2011. En 2012, après avoir emménagé dans ses nouveaux locaux, le CEPD élaborera un nouveau plan en étroite collaboration avec d'autres institutions.

Compte tenu du fait qu'il leur était nécessaire d'accéder à des informations classifiées de l'UE (ICUE)

pour pouvoir s'acquitter de leurs fonctions, plusieurs membres du personnel du CEPD ont reçu une habilitation de sécurité officielle, accordée par leur autorité nationale de sécurité. Cela permet au CEPD d'effectuer des inspections de sécurité sur des systèmes d'information à grande échelle ou d'autres sites importants et sensibles.

Des avis ont régulièrement été transmis au sujet des activités du CEPD, y compris une introduction aux missions et au mandat du CEPD présentée par les responsables locaux de sécurité (LSO) et les responsables de la sécurité informatique au niveau local (LISO) de la Commission européenne.

6.5. Infrastructure

Sur la base de l'accord de coopération administrative décrit ci-dessous, les bureaux du CEPD sont situés dans les locaux du Parlement européen, qui assiste en outre le CEPD dans les domaines des technologies de l'information (TI) et de l'infrastructure.

En raison d'un manque d'espace récurrent dans le bâtiment où le CEPD est situé et de l'expiration imminente du contrat de location du bâtiment qu'occupe le CEPD (Montoyer 63), le Parlement européen a créé un comité du bâtiment, auquel le CEPD a participé, afin de choisir un nouveau bâtiment pour accueillir les bureaux du CEPD.

Le nouveau bâtiment a été choisi en 2011 et le déménagement est prévu pour mi-2012. Un groupe de travail nommé 'EDPS by design' a été créé. Sa mission consiste à «analyser et développer tous les aspects liés à la conception et au déménagement dans un nouveau bâtiment (par exemple, planification, distribution de l'espace, questions relatives aux technologies de l'information, à court terme comme à long terme, questions liées à la sécurité ou à la protection des données, etc.) courant 2012, de manière à ce que le déménagement soit un succès et que les activités de l'institution soient aussi peu perturbées que possible.»

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

6.6. Environnement administratif

6.6.1. Assistance administrative et coopération interinstitutionnelle

Le CEPD bénéficie de la coopération interinstitutionnelle dans de nombreux domaines en vertu de l'accord conclu en 2004 avec les secrétaires généraux de la Commission, du Parlement et du Conseil, accord qui a été prorogé pour une durée de trois ans en 2006 et de deux ans en 2010 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. Cette coopération est essentielle pour le CEPD car elle renforce son efficacité et lui permet de réaliser des économies d'échelle.

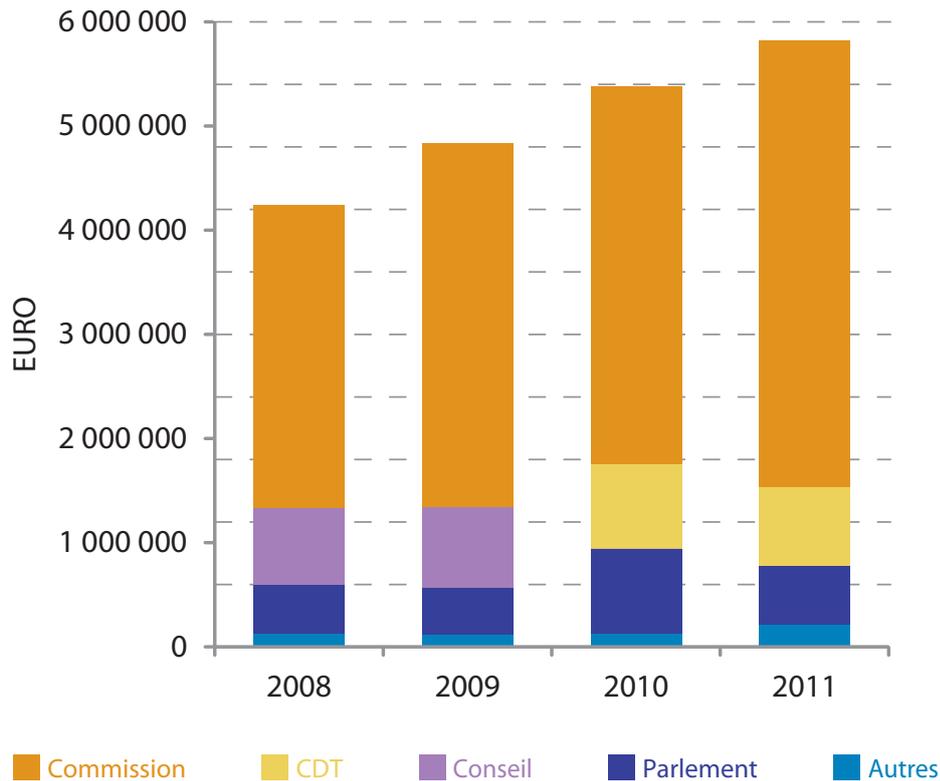
En 2011, la coopération interinstitutionnelle étroite s'est poursuivie avec diverses directions générales de la Commission (DG «Personnel et administration», DG «Budget», service d'audit interne, DG «Éducation et culture»), l'Office des paiements (PMO), l'École européenne d'administration (EEA), le Centre 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 de nombreux cas, cette coopération se fait au moyen d'accords de niveau de service, qui sont régulièrement mis à jour. Le CEPD a également continué de participer aux appels d'offres interinstitutionnels, accroissant ainsi son efficacité dans de nombreux domaines administratifs et évoluant vers plus d'autonomie.

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.

6.6.2. Règlement intérieur

L'adoption du règlement intérieur pour le bon fonctionnement du CEPD a eu lieu en 2011. Lorsque les dispositions de ce règlement concernent des

Exécution du budget du CEPD via la coopération interinstitutionnelle



domaines pour lesquels le CEPD bénéficie de l'assistance de la Commission ou du Parlement européen, elles sont semblables à celles de ces institutions moyennant quelques adaptations liées à la spécificité des services du CEPD.

En 2011, la réunion des directeurs (qui réunit les chefs d'unité ou de secteur et le directeur) a entamé des discussions sur l'adoption d'un règlement intérieur d'une portée plus générale, et une première proposition a été présentée au conseil d'administration du CEPD. Le CEPD prévoit d'adopter ce règlement en 2012, avec une version révisée du code de bonne conduite du CEPD.

6.6.3. Gestion des documents

Le CEPD a sélectionné et acquis un système de gestion des documents et des dossiers intégrant la gestion des dossiers. Ce processus a été mené à bien avec l'aide des services de l'information et des technologies du Parlement européen.

Les travaux visant à adapter et à configurer ce système pour qu'il réponde aux besoins particuliers du CEPD ont commencé à la fin de l'année. Les bases de données actuelles du CEPD ont été harmonisées dans la perspective de la migration vers le nouveau système.

6.6.4. Planification

Au cours de l'année 2011, des améliorations ont été apportées à la planification et au contrôle des activités au sein du CEPD. Trois niveaux de planification ont été mis en place: un plan stratégique (sur 3 à 5 ans), un plan de gestion annuel et une planification détaillée des activités:

- a) Plan stratégique

Un des premiers résultats de la révision stratégique a été la création d'un plan stratégique précis et détaillé. Cette planification stratégique permettra au conseil d'administration de gérer ses ressources plus efficacement à moyen terme.
- b) Plan de gestion

Le plan de gestion annuel expose la planification détaillée pour l'année, sur la base des objectifs et activités mentionnés dans le plan stratégique sur trois ans.
- c) Planification hebdomadaire des activités

Une planification hebdomadaire exacte des activités est effectuée pour garantir que le CEPD respecte ses obligations juridiques et ses délais. La planification garantit également une coopération efficace entre les différentes équipes du CEPD.

7

DÉLÉGUÉ À LA PROTECTION DES DONNÉES DU CEPD

7.1. Le DPD du CEPD

En 2010, l'équipe du DPD était constituée de deux DPD (un DPD et un DPD adjoint), désignés par le CEPD en septembre 2010. À la suite au départ du DPD en mars 2011, le CEPD a décidé de nommer le DPD adjoint - qui a suivi avec succès le programme de certification en 2010 - DPD faisant fonction. Le DPD faisant fonction a été nommé DPD en décembre 2011, après avoir été nommé à un poste AD.

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

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 DPD²⁰.

7.2. Le registre des traitements

L'année 2011 a été consacrée à la révision de toutes les notifications de traitement au sein du CEPD et à de nouvelles notifications. Sept notifications ont été considérablement révisées afin de tenir compte des nouvelles procédures mises en place au sein du CEPD à la suite de sa réorganisation interne, notamment en ce qui concerne les procédures de gestion des ressources humaines. Huit nouvelles notifications ont été requises, principalement dans les équipes des ressources humaines et de la communication. Une notification concernant la façon dont le CEPD traite les réclamations déposées a également été traitée. Ces notifications ont trait à l'article 25 du règlement (CE) n° 45/2001.

Dans le même temps, le DPD a traité les notifications présentées au CEPD en vertu de l'article 27, paragraphe 2, du règlement (CE) n° 45/2001 conformément aux lignes directrices du CEPD. Parmi les 17 notifications existantes fondées sur l'article 25 du règlement, neuf faisaient l'objet d'une notification en vertu de l'article 27 du règlement (CE) n° 45/2001 et 89 % de ces dernières concernaient des questions de ressources humaines.

Le principal objectif du DPD pour 2012 est de demander les notifications de tous les traitements qui figurent dans l'inventaire qui n'ont pas encore été établies par les personnes responsables du traitement.

²⁰ 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

7.3. Enquête 2011 du CEPD

En mars 2011, le directeur du CEPD a adressé au contrôleur une lettre exposant tous les travaux réalisés dans le but de respecter le règlement (CE) n° 45/2001. Le CEPD a tenu compte de ces documents dans son enquête 2011. Le plan d'action 2010, qui a été mis en œuvre à 95 %, a reçu un accueil positif. Le CEPD a souligné que toutes les notifications en vertu de l'article 27 avaient été clôturées.

7.4. Information et sensibilisation

Le DPD accorde une grande importance à la sensibilisation 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 reprend des informations de base sur le rôle et les activités du DPD, a été actualisée de sorte que le public peut consulter le registre actualisé et toutes les notifications dans leur nouvelle version.

Par ailleurs, le DPD participe aux **réunions du réseau des DPD**, qui sont une occasion unique de développer des réseaux, d'aborder des problèmes communs et d'échanger les bonnes pratiques.

En ce qui concerne la **communication interne**, l'intranet du CEPD offre 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 a été complétée par une liste détaillée de déclarations de confidentialité concernant les traitements du CEPD, permettant à tous les membres du personnel de faire valoir leurs droits (articles 11 et 12 du règlement (CE) n° 45/2001) en les informant à ce sujet.

Dans le cadre de la sensibilisation, le DPD a également réalisé une présentation intitulée «Initiation au règlement (CE) n° 45/2001», destinée aux nouveaux arrivants et aux fonctionnaires ne disposant pas d'expérience en matière de protection des données. Son objectif était de permettre aux membres du personnel de se familiariser avec les questions de protection des données, ainsi qu'avec les missions et valeurs du CEPD.

8

PRINCIPAUX OBJECTIFS POUR 2012

Les objectifs suivants ont été sélectionnés pour 2012. Les résultats obtenus figureront dans le rapport annuel de 2013.

8.1. Supervision et mise en application

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

- **Sensibilisation**

Le CEPD consacrera du temps et des ressources à donner des orientations aux institutions et agences de l'UE. Ces orientations sont nécessaires pour faciliter une réorientation vers une plus grande responsabilisation des institutions et agences. Elles prendront la forme de documents thématiques concernant les procédures administratives standard et des thèmes horizontaux tels que l'e-monitoring, les transferts et les droits des personnes concernées. Des formations et ateliers destinés aux DPD/CPD seront également organisés, à la demande d'une institution ou agence spécifique ou à l'initiative du CEPD lorsque celui-ci aura repéré un besoin. Le site internet du CEPD sera développé afin de fournir des informations utiles aux DPD. Le registre public des notifications de contrôle préalable sera également rendu accessible selon une taxonomie thématique.

- **Contrôles préalables**

Le CEPD continue à recevoir des notifications *ex-post* concernant soit des procédures administratives standard soit des traitements déjà en vigueur. En 2012, le CEPD prendra des mesures afin de définir les procédures appropriées pour gérer de telles notifications et de garantir que de telles notifications de contrôle *ex-post* ne sont autorisées que dans des circonstances exceptionnelles et justifiées. Le suivi des recommandations formulées dans les avis de contrôle préalable est un élément essentiel de la stratégie de mise en application du CEPD. Le CEPD continuera d'insister sur la mise en œuvre des recommandations contenues dans les avis de contrôle préalable et veillera à leur suivi adéquat.

- **Bilans généraux**

En 2011, le CEPD a entamé un bilan général donnant des indicateurs du respect de certaines obligations par les institutions et organes (désignation d'un DPD, adoption de règles d'application, niveau de notifications au titre de l'article 25, niveau de notifications au titre de l'article 27, etc.). Le CEPD rédigera un rapport sur la base des informations reçues de la part de ces institutions et organes. Le rapport mettra l'accent sur les progrès accomplis dans la mise en œuvre du règlement, mais il soulignera également les lacunes constatées. En 2012, l'enquête 2011 sera complétée par un exercice particulier concernant le statut des DPD. Cet exercice visera également à apporter un soutien à la fonction de DPD dans le cadre du principe de responsabilisation. En 2012, le CEPD lancera en outre une enquête spécialement conçue pour la Commission,

dans l'objectif de recueillir directement des informations auprès des diverses directions générales.

- **Visites**

En se fondant sur les indicateurs de l'enquête 2011, le CEPD a sélectionné les institutions et agences où il effectuera des visites (6 visites prévues). Ces visites sont suscitées par un manque apparent d'engagement, par un manque de communication de la part de la direction ou si une institution ou une agence est en dessous de la référence définie pour un groupe de pairs.

- **Inspections**

Les inspections constituent un instrument capital qui permet au CEPD de surveiller et de garantir l'application du règlement. Il est essentiel que leur nombre augmente, non seulement en tant qu'instrument de répression mais aussi en tant qu'instrument d'information sur les questions de protection des données et le CEPD. Les inspections se multiplieront en 2012 en raison de la création d'inspections plus légères et plus ciblées en sus des inspections intégrales. Certaines institutions ou certains organes traitent des données à caractère personnel dans le cadre de leurs activités principales; la protection des données constitue dès lors un élément essentiel. Ces organes seront recensés et feront l'objet de contrôles ciblés (sur support papier) ou d'inspections ciblées. En 2012, des inspections générales concernant des systèmes d'information à grande échelle sont également prévues. Ces systèmes sont sélectionnés sur la base de l'obligation juridique. Le CEPD effectuera également des inspections thématiques dans des domaines où il a donné des conseils et où il souhaite effectuer un contrôle dans la pratique, par exemple le système de télévision en circuit fermé (CCTV).

8.2. Politique législative et consultation

Les principaux objectifs du CEPD pour son rôle consultatif sont définis dans l'inventaire et le mémo joint, qui sont publiés sur son site internet. Le CEPD devra relever le défi consistant à remplir un rôle sans cesse croissant dans la procédure législative, tout en garantissant une contribution qualitative élevée et appréciée au processus législatif, à partir de ressources limitées. Eu égard à ces circonstances, le CEPD a relevé les questions d'importance stratégique formant la pierre angulaire de son travail consultatif pour 2012, sans omettre toutefois

d'autres procédures législatives touchant à la protection des données.

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

Le CEPD accordera la priorité aux travaux sur un cadre juridique de la protection des données dans l'UE. Il rendra un avis sur les propositions législatives relatives au cadre, et il participera aux débats dans les étapes suivantes de la procédure législative lorsque cela s'avérera nécessaire et approprié.

- **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 2012. 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 et la «santé électronique». En outre, le CEPD renforcera son savoir-faire technologique et participera à des recherches sur des technologies permettant de renforcer la protection de la vie privée.

- **Développement de l'espace de liberté, de sécurité et de justice**

L'espace de liberté, de sécurité et de justice demeurera l'un des domaines politiques clés traités par le CEPD. Parmi les propositions à venir dans le domaine, on peut citer le système de surveillance du financement du terrorisme (SSFT) de l'UE et les frontières intelligentes. En outre, le CEPD continuera de suivre la révision de la directive relative à la conservation des données. Il suivra également de près les négociations d'accords en matière de protection des données avec les pays tiers.

- **Réforme du secteur financier**

Le CEPD continuera 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.

- **Autres initiatives**

Le CEPD suivra également des propositions dans d'autres domaines politiques ayant des répercussions importantes sur la protection des données. Il continuera d'être disponible pour des consultations formelles et informelles sur des propositions affectant le droit à la protection de la vie privée et des données.

8.3. Coopération

Le CEPD continuera d'assumer ses responsabilités dans le domaine de la supervision conjointe. En outre, il se rapprochera des autorités nationales chargées de la protection des données et des organisations internationales.

- **Supervision conjointe**

Le CEPD jouera son rôle dans la supervision conjointe d'Eurodac, du système d'information douanier et du système d'information sur les visas (VIS). La supervision conjointe du système d'information sur les visas, qui est opérationnel depuis octobre 2011, n'en est encore qu'à ses débuts. Après des discussions informelles dans le cadre des réunions de coordination du contrôle d'Eurodac, l'objectif pour 2012 est d'établir progressivement la supervision dans ce domaine. Une fois lancé, le système SIS II fera également l'objet d'une supervision conjointe. Le lancement est prévu pour 2013 et les préparatifs seront suivis de près. Le CEPD effectuera également des inspections des unités centrales de ces systèmes lorsque ce sera nécessaire ou que la loi l'exigera.

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

Comme auparavant, le CEPD contribuera activement aux activités et au succès du groupe de travail «Article 29» sur la protection des données, en assurant cohérence et synergie entre le groupe de travail et les positions du CEPD conformément à leurs priorités respectives et en entretenant une relation constructive avec les autorités nationales chargées de la protection des données. En tant que rapporteur de certains dossiers particuliers, il dirigera et préparera l'adoption des avis du groupe «Article 29».

- **Protection des données au sein des organisations internationales**

Les organisations internationales ne sont généralement pas soumises à la législation relative à la protection des données dans leur pays d'accueil.

Cependant, elles ne disposent pas toutes de règles appropriées en matière de protection des données. Le CEPD se rapprochera des organisations internationales en organisant un atelier visant à accroître la sensibilisation et à diffuser les bonnes pratiques.

8.4. Autres domaines

- **Information et communication**

Le CEPD continuera de développer et d'améliorer ses activités d'information, de communication et de presse en mettant plus particulièrement l'accent sur la sensibilisation, les publications et l'information en ligne. Il commencera également à mettre en œuvre la révision de sa stratégie de l'information et de la communication, après avoir consulté ses principales parties prenantes. La réorganisation de certaines parties importantes du site internet du CEPD est prévue afin de rendre le site internet plus convivial et de faciliter la recherche et la navigation dans les informations disponibles.

- **Organisation interne**

La révision stratégique du CEPD se poursuivra tout au long de l'année 2012, avec une consultation externe des parties prenantes au moyen d'enquêtes en ligne, d'entretiens, de groupes thématiques et d'ateliers. Les premiers résultats de la révision entamée en 2011 ont abouti aux décisions d'élaborer une approche plus stratégique des activités de supervision et de consultation et de créer un nouveau secteur politique «technologies de l'information» en 2012. Une fois la révision terminée et les résultats analysés, le CEPD finalisera sa stratégie à moyen terme et élaborera les indicateurs de performance clés (KPI) nécessaires à l'évaluation des éléments essentiels de cette stratégie.

- **Gestion des ressources**

Les travaux visant à développer un système de gestion des dossiers spécialement conçu pour le CEPD se poursuivront en 2012. Les applications informatiques fondées sur des accords de niveau de service dans le domaine des ressources humaines seront également encore développées, notamment avec la mise en œuvre du système Sysper II, qui sera terminée en 2012, et avec l'introduction du système MIPS.

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 ⁽²¹⁾.

Depuis l'entrée en vigueur du traité de Lisbonne, le 1^{er} 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.

D'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

²¹ JO L 8 du 12.1.2001, p. 1.

traité de Lisbonne et l'abolition de la structure en piliers - qui rendent les références aux «institutions communautaires» et au «droit communautaire» désormais obsolètes - le règlement couvre en principe toutes les institutions et tous les organes de l'Union européenne, sauf disposition contraire spécifique dans d'autres actes législatifs de l'Union. Les conséquences précises de ces changements font encore l'objet d'un examen et pourraient nécessiter une clarification supplémentaire.

Les définitions et la teneur du règlement s'inspirent très largement des principes de la directive 95/46/CE. On pourrait dire que le règlement (CE) n° 45/2001 constitue la mise en œuvre de cette directive au niveau européen. Il traite ainsi des principes généraux tels que le traitement loyal et licite, la proportionnalité et la compatibilité d'utilisation, les catégories particulières de données sensibles, l'information de la personne concernée, les droits de la personne concernée, les obligations des responsables du traitement - en tenant compte, le cas échéant, des circonstances propres au niveau de l'UE-, ainsi que du contrôle, de l'exécution et des recours. Un chapitre particulier est consacré à la protection des données à caractère personnel et de la vie privée dans le cadre des réseaux internes de télécommunications. Ce chapitre constitue 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. Des travaux importants ont donc été accomplis pour mettre en œuvre le règlement, même en l'absence d'un organe de contrôle. Ces délégués peuvent d'ailleurs être mieux placés pour fournir des conseils ou intervenir à un stade précoce et pour contribuer à la mise au point de bonnes pratiques. Les délégués à la protection des données ayant l'obligation formelle de coopérer avec le CEPD, il s'est formé un réseau très important et fort apprécié, qu'il convient de développer encore (voir 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 les responsables du traitement et les personnes concernées, effectuer des contrôles préalables lorsque les traitements présentent des risques particuliers, etc. Le règlement habilite le CEPD à obtenir accès à toutes les informations utiles et aux locaux 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 dans le 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

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

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

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

Article 46 — Fonctions

Le Contrôleur européen de la protection des données:

- a) entend et examine les réclamations et informe la personne concernée des résultats de son examen dans un délai raisonnable;
- b) effectue des enquêtes, soit de sa propre initiative, soit sur la base d'une réclamation et informe les personnes concernées du résultat de ses enquêtes dans un délai raisonnable;
- c) contrôle et assure l'application du présent règlement et de tout autre acte communautaire relatifs à la protection des personnes physiques à l'égard du traitement de données à caractère personnel par une institution ou un organe communautaire, à l'exclusion de la Cour de justice des Communautés européennes dans l'exercice de ses fonctions juridictionnelles;

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

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

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

ii) coopère également avec les organes de contrôle de la protection des données institués en vertu du titre VI du traité sur l'Union européenne en vue notamment d'améliorer la cohérence dans l'application des règles et procédures dont ils sont respectivement chargés d'assurer le respect;

g) participe aux activités du groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive 95/46/CE;

h) détermine, motive et rend publiques les exceptions, garanties, autorisations et conditions mentionnées à l'article 10, paragraphe 2, point b), à l'article 10, paragraphes 4, 5 et 6, à l'article 12, paragraphe 2, à l'article 19 et à l'article 37, paragraphe 2;

i) tient un registre des traitements qui lui ont été notifiés en vertu de l'article 27, paragraphe 2, et enregistrés conformément à l'article 27, paragraphe 5, et fournit les moyens d'accéder aux registres tenus par les délégués à la protection des données en application de l'article 26;

j) effectue un contrôle préalable des traitements qui lui ont été notifiés;

k) établit son règlement intérieur.

Article 47 — Compétences

1. Le Contrôleur européen de la protection des données peut:

- a) conseiller les personnes concernées dans l'exercice de leurs droits;
- b) saisir le responsable du traitement en cas de violation alléguée des dispositions régissant le traitement des données à caractère personnel et, le cas échéant, formuler des propositions tendant à remédier à cette violation et à améliorer la protection des personnes concernées;
- c) ordonner que les demandes d'exercice de certains droits à l'égard des données soient satisfaites lorsque de telles demandes ont été rejetées en violation des articles 13 à 19;
- d) adresser un avertissement ou une admonestation au responsable du traitement;
- e) ordonner la rectification, le verrouillage, l'effacement ou la destruction de toutes les données lorsqu'elles ont été traitées en violation des dispositions régissant le traitement de données à caractère personnel et la notification de ces mesures aux tiers auxquels les données ont été divulguées;
- f) interdire temporairement ou définitivement un traitement;
- g) saisir l'institution ou l'organe concerné et, si nécessaire, le Parlement européen, le Conseil et la Commission;
- h) saisir la Cour de justice des Communautés européennes dans les conditions prévues par le traité;
- i) intervenir dans les affaires portées devant la Cour de justice des Communautés européennes.

2. Le Contrôleur européen de la protection des données est habilité à:

- a) obtenir d'un responsable du traitement ou d'une institution ou d'un organe communautaire l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires à ses enquêtes;
- b) obtenir l'accès à tous les locaux dans lesquels un responsable du traitement ou une institution ou un organe communautaire exerce ses activités s'il existe un motif raisonnable de supposer que s'y exerce une activité visée par le présent règlement.

Annexe C — Liste des abréviations

| | | | |
|----------|---|-------|--|
| ACAC | Accord commercial anti-contrefaçon | ENISA | Agence européenne chargée de la sécurité des réseaux et de l'information |
| SID | Système d'information douanier | CEDH | Convention européenne des droits de l'homme |
| CC | Cour des comptes | DPE | Décision de protection européenne |
| CdR | Comité des régions | EPSO | Office européen de sélection du personnel |
| CPAS | Comité de préparation pour les affaires sociales | ERCEA | Agence exécutive du Conseil européen de la recherche |
| DAS | Déclaration d'assurance | UE | Union européenne |
| DG INFSO | Direction générale de la société de l'information et des médias | RAPS | Système d'alerte précoce et de réaction |
| DG MARKT | Direction générale du marché intérieur et des services | FRA | Agence des droits fondamentaux de l'Union européenne |
| DIGIT | Direction générale de l'informatique | RH | Ressources humaines |
| APD | Autorité chargée de la protection des données | SAI | Service d'audit interne |
| CPD | Coordinateur de la protection des données | TIC | Technologies de l'information et de la communication |
| DPD | Délégué à la protection des données | IMI | Système d'information sur le marché intérieur |
| EEA | École européenne d'administration | OIM | Organisation internationale pour les migrations |
| AESA | Agence européenne de la sécurité aérienne | SSI | Stratégie de sécurité intérieure |
| CE | Communautés européennes | TI | Technologies de l'information |
| BCE | Banque centrale européenne | CCR | Centre commun de recherche |
| ECDC | Centre européen pour la prévention et de contrôle des maladies | ORC | Opération de retour conjointe |
| CJE | Cour de justice européenne | ACC | Autorité de contrôle commune |
| AEE | Agence européenne pour l'environnement | CGAM | Comité de gestion du régime commun d'assurance maladie |
| EFSA | Autorité européenne de sécurité des aliments | LIBE | Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen |
| BEI | Banque européenne d'investissement | RLSI | Responsable local de la sécurité informatique |
| DEE | Décision d'enquête européenne | RLS | Responsable local de la sécurité |

| | |
|---------|--|
| OHMI | Office de l'harmonisation dans le marché intérieur |
| OLAF | Office européen de lutte antifraude |
| PNR | Dossier passager (<i>Passenger Name Record</i>) |
| R&D | Recherche et développement |
| RFID | Identification par radiofréquence |
| SIS | Système d'information Schengen |
| END | Expert national détaché |
| CSO | Centre de service et d'opération |
| s-TESTA | Services télématiques transeuropéens sécurisés entre administrations |
| SSFT | Système européen de surveillance du financement du terrorisme |
| SWIFT | Société de télécommunications interbancaires mondiales |
| TFTP | Programme de surveillance du financement du terrorisme |
| TFUE | Traité sur le fonctionnement de l'Union européenne |
| TURBINE | TrUsted Revocable Biometrics IdeNtitiEs |
| HCR | Haut commissariat des Nations unies pour les réfugiés |
| VIS | Système d'information sur les visas |
| OMD | Organisation mondiale des douanes |
| WP 29 | Groupe de travail «Article 29» sur la protection des données |
| GTPJ | Groupe de travail sur la police et la justice |

Annexe D — Liste des délégués à la protection des données

| ORGANISATION | NAME | E-MAIL |
|---|------------------------------|---|
| Parlement européen (PE) | Jonathan STEELE | 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 des Communautés européennes (CURIA) | Valerio Agostino PLACCO | Dataprotectionofficer@curia.europa.eu |
| Cour des comptes européenne | Johan VAN DAMME | Data-Protection@eca.europa.eu |
| Comité économique et social européen (CESE) | Maria ARSENE | Data.Protection@eesc.europa.eu |
| Comité des régions (CdR) | Rastislav SPÁC | Data.Protection@cor.europa.eu |
| Banque européenne d'investissement (EIB) | Jean-Philippe MINNAERT | Dataprotectionofficer@eib.org |
| Service européen pour l'action extérieure (SEAE) | Ingrid HVASS | Ingrid.HVASS@eeas.europa.eu |
| Médiateur européen | Loïc JULIEN | 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) | Ignacio DE MEDRANO CABALLERO | DataProtectionOfficer@oami.europa.eu |
| Agence des droits fondamentaux de l'Union européenne (FRA) | Nikolaos FIKATAS | Nikolaos.Fikatas@fra.europa.eu |
| Agence européenne des médicaments (EMA) | Alessandro SPINA | Data.Protection@emea.europa.eu |
| Office communautaire des variétés végétales (OCVV) | 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 travail (Eurofound) | Markus GRIMMEISEN | mgr@eurofound.europa.eu |
| Observatoire européen des drogues et des toxicomanies (EMCDDA) | Ignacio Vázquez MOLINÍ | Ignacio.Vazquez-Molini@emcdda.europa.eu |

>>>

| ORGANISATION | NAME | E-MAIL |
|--|-------------------------|--|
| Autorité européenne de sécurité des aliments (EFSA) | Claus RÉUNIS | Dataprotectionofficer@efsa.europa.eu |
| Agence européenne pour la sécurité maritime (AESM) | Malgorzata NESTEROWICZ | Malgorzata.Nesterowicz@emsa.europa.eu |
| Centre européen pour le développement de la formation professionnelle (Cedefop) | Spyros ANTONIOU | Spyros.Antoniou@cedefop.europa.eu |
| Agence exécutive Éducation, audiovisuel et culture (EACEA) | Hubert MONET | eacea-data-protection@ec.europa.eu |
| Agence européenne pour la sécurité et la santé au travail (OSHA) | Eusebio RIAL GONZALES | rial@osha.europa.eu |
| Agence communautaire de contrôle des pêches (ACCP) | Rieke ARNDT | cfca-dpo@cfca.europa.eu |
| Centre satellitaire de l'Union européenne (EUSC) | 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 (ASG) | 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 pour la prévention et le contrôle des maladies (ECDC) | 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 | Francesca.Pavesi@easa.europa.eu |
| Agence exécutive pour la compétitivité et l'innovation (EACI) | Elena FIERRO SEDANO | Elena.Fierro-Sedano@ec.europa.eu |
| Agence européenne du réseau transeuropéen de transport (AE RTE-T) | Zsófia SZILVÁSSY | Zsofia.Szilvassy@ec.europa.eu |
| Autorité bancaire européenne (EBA) | Joseph MIFSUD | Joseph.MIFSUD@eba.europa.eu |
| Agence européenne des produits chimiques (ECHA) | Alain LEFÈBVRE | 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 (ESRB) | Frederik MALFRÈRE | DPO@ecb.int |

>>>

| ORGANISATION | NAME | E-MAIL |
|---|--------------------|----------------------------------|
| Fusion à des fins énergétiques (Entreprise commune pour ITER et le développement de l'énergie de fusion) | Radoslav HANAK | Radoslav.Hanak@f4e.europa.eu |
| Entreprise commune Sesar (SESAR) | Daniella PAVKOVIC | Daniella.Pavkovic@sesarju.eu |
| Entreprise commune Artemis | Anne SALAÜN | Anne.Salaun@artemis-ju.europa.eu |
| Entreprise commune Clean Sky | Silvia POLIDORI | Silvia.Polidori@cleansky.eu |
| Initiative Médicaments innovants (IMI) | Estefania RIBEIRO | Estefania.Ribeiro@imi.europa.eu |
| Entreprise commune Piles à combustible et hydrogène | Nicolas BRAHY | Nicolas.Brahy@fch.europa.eu |
| Autorité européenne des assurances et des pensions professionnelles (EIOPA) | Catherine COUCKE | catherine.coucke@eiopa.europa.eu |
| Collège européen de police (CEPOL) | Leelo KILG | leelo.kilg@cepol.europa.eu |
| Institut européen d'innovation et de technologie (EIT) | Roberta MAGGIO | roberta.maggio@eit.europa.eu |
| Agence européenne de défense (EDA) | Alain-Pierre LOUIS | alain-pierre.louis@eda.europa.eu |
| ENIAC Joint Undertaking | Marc JEUNIAUX | Marc.Jeuniaux@eniac.europa.eu |

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

Procédures de passation de marchés publics- ACCP

Avis du 21 décembre 2011 sur la notification d'un contrôle préalable concernant les procédures de passation de marchés publics à l'Agence communautaire de contrôle des pêches (dossier 2011-0890)

Système de vidéosurveillance - CCE

Lettre du 20 décembre 2011 sur la notification d'un contrôle préalable concernant le système de vidéosurveillance à la Cour des comptes européenne (CCE) (dossier 2011-0989)

Rapport de retour d'information à 360 ° pour les cadres

Avis du 20 décembre 2011 sur la notification d'un contrôle préalable concernant le «rapport de retour d'information à 360 ° pour les cadres», Comité des régions (dossier 2011-0926)

Évaluations du personnel - Eurofound

Avis du 19 décembre 2011 sur la notification en vue d'un contrôle préalable concernant les rapports de stage, les évaluations du personnel et les promotions à la Fondation européenne pour l'amélioration des conditions de vie et de travail (Eurofound) (dossier 2011-0628)

Interventions de la Chambre d'écoute dans le cadre de la réorganisation de l'organigramme de l'OLAF

Avis du 16 décembre 2011 sur la notification en vue d'un contrôle préalable concernant des interventions de la Chambre d'écoute dans le cadre de la réorganisation de l'organigramme de l'Office européen de lutte antifraude (OLAF) (dossier 2011-1021)

Procédure relative aux commissions d'invalidité - Cour de Justice

Avis du 15 décembre 2011 sur la notification d'un contrôle préalable à propos du dossier «Procédure relative aux commissions d'invalidité» (dossier 2011-0655)

Évaluations du personnel - Agence européenne des produits chimiques

Avis du 15 décembre 2011 sur la notification d'un contrôle préalable concernant les évaluations du personnel à l'Agence européenne des produits chimiques (ECHA) (dossier 2011-0945)

Évaluations du personnel - ACER

Avis du 15 décembre 2011 sur la notification d'un contrôle préalable concernant les rapports de stage et les évaluations du personnel, y compris l'évaluation du directeur de l'Agence de coopération des régulateurs de l'énergie (ACER) (dossier 2011-0953)

Rapports de stage, évaluations du personnel et reclassification - Agence exécutive du CER

Avis du 15 décembre 2011 sur la notification d'un contrôle préalable concernant l'évaluation annuelle et le stage, la reclassification et l'évaluation de la capacité à travailler dans une troisième langue à l'Agence exécutive du CER (dossier 2011-0955/0956/0963)

Évaluations du personnel - Agence exécutive du réseau transeuropéen de transport

Avis conjoint du 14 décembre 2011 sur les notifications de contrôle préalable concernant les évaluations du personnel de l'Agence exécutive du réseau transeuropéen de transport (TEN-T EA) (dossier 2011-0990)

Procédure de retraite anticipée sans réduction des droits à pension - OCVV

Avis du 13 décembre 2011 sur la notification en vue d'un contrôle préalable concernant la procédure de retraite anticipée sans réduction des droits à pension, l'Office communautaire des variétés végétales (OCVV) (dossier 2011-0304)

Transmission des rapports d'inspection - EFCA

Avis conjoint du 30 novembre 2011 concernant deux notifications de contrôle préalable concernant la transmission des rapports d'inspection relatifs au plan de déploiement commun (PDC) pour le thon rouge et la transmission des rapports d'inspection (OPANO/CPANE), l'Agence européenne de contrôle des pêches (EFCA) (dossiers 2011-0615 et 2011-0636)

Procédures de passation de marchés et contrats de marchés liés - OCVV

Avis du 30 novembre 2011 sur la notification d'un contrôle préalable concernant des procédures de passation de marchés et les contrats de marchés qui leur sont liés à l'Office communautaire des variétés végétales (OCVV) (dossier 2011-0740)

«E-recruitment for the Graduate Recruitment and Development Programme» - BEI

Lettre du 24 novembre 2011 sur la notification d'un contrôle préalable concernant «E-recruitment for the Graduate Recruitment and Development Programme» à la Banque Européenne d'Investissement (BEI) (dossier 2009-0761)

Sélection d'experts – ERA

Avis du 22 novembre 2011 sur les notifications de contrôle préalable concernant les appels à candidatures visant à établir des listes d'experts indépendants potentiels chargés d'assister les travaux des groupes de travail de l'Agence ferroviaire européenne dans les domaines de la sécurité ferroviaire et de l'interopérabilité ferroviaire (dossiers joints 2011-0667/0668)

Évaluation des propositions et gestion des subventions - AECER

Avis du 21 novembre 2011 sur la notification d'un contrôle préalable concernant l'évaluation des propositions et la gestion des subventions à l'Agence exécutive du Conseil européen de la recherche (AECER) (dossier 2011-0845)

Recrutement de personnel et sélection et recrutement de stagiaires - Piles à combustible et Hydrogène

Avis du 15 novembre 2011 sur les notifications en vue d'un contrôle préalable concernant la sélection et le recrutement de personnel et de stagiaires, Piles à combustible et Hydrogène (EC PCH) (dossiers 2011- 0833 et 2011-0834)

Procédures de sélection des agents contractuels - Commission européenne

Lettre du 11 novembre 2011 sur la notification d'un contrôle préalable concernant des procédures de sélection des agents contractuels dans les services de la Commission européenne (dossier 2011-0820)

Système de vidéosurveillance - ECHA

Lettre du 25 octobre 2011 sur la notification d'un contrôle préalable sur le système de vidéosurveillance à l'Agence européenne des produits chimiques (ECHA) (dossier 2011-0012)

Politique de «retour au travail» - EU-OSHA

Avis du 24 octobre 2011 sur la notification en vue d'un contrôle préalable concernant la politique de «retour au travail» à l'Agence européenne pour la sécurité et la santé au travail (EU-OSHA) (dossier 2011-752)

Sélection de conseillers confidentiels et politique anti-harcèlement

Avis du 21 octobre 2011 sur les notifications de contrôle préalable concernant «la politique anti-harcèlement» et «la sélection de conseillers confidentiels» à certaines agences de l'UE (dossier 2011-0483)

Recrutement du personnel - Cour de justice

Lettre du 21 octobre 2011 sur la notification d'un contrôle préalable des traitements de données relatifs au «recrutement du personnel» à la Cour de justice de l'Union européenne (dossier 2011-0388)

Période probatoire à l'OCVV

Avis du 19 octobre 2011 sur une notification pour contrôle préalable concernant l'évaluation et les rapports de la période probatoire à l'Office communautaire des variétés végétales (dossier 2011-298)

Unité de coopération opérationnelle virtuelle, courtier d'assistance mutuelle et système d'information douanier - OLAF

Avis commun du 17 octobre 2011 sur les notifications de contrôle préalable concernant l'unité de coopération opérationnelle virtuelle, le courtier d'assistance mutuelle et le système d'information douanier (dossiers joints 2010-0797, 2010-0798, 2010-0799)

Sélection des participants aux actions (internes ou externes) de formation et de perfectionnement - Commission européenne

Avis du 17 octobre 2011 sur la notification d'un contrôle préalable concernant la «sélection des participants aux actions (internes ou externes) de formation et de perfectionnement» (dossier 2011-0627)

Mobilité interne des membres du personnel - EACEA

Avis du 17 octobre 2011 sur la notification d'un contrôle préalable concernant la «mobilité interne des membres du personnel de l'EACEA» (dossier 2011-0672)

Curriculum vitae électronique

Avis du 4 octobre 2011 sur la notification d'un contrôle préalable reçue du délégué à la protection des données du Parlement européen concernant le curriculum vitae électronique (dossier 2011-568)

Procédure de sélection pour le poste de membre du conseil d'administration - EFSA

Avis du 3 octobre 2011 sur une notification en vue d'un contrôle préalable concernant la «procédure de sélection pour le poste de membre du conseil d'administration de l'Autorité européenne de sécurité des aliments (EFSA)» (dossier 2011-0575)

Sélection et recrutement d'END, de stagiaires et d'agents temporaires - Eurofound

Avis du 27 septembre 2011 sur la notification d'un contrôle préalable concernant la sélection et le recrutement d'END, de stagiaires et d'agents temporaires (dossiers 2011-0645/646/647)

PMO – Mise en place d'indicateurs de production individuels

Avis du 23 septembre 2011 sur la notification d'un contrôle préalable concernant la mise en place d'indicateurs de production individuels (dossier 2011-368)

Base de données de la cartographie des compétences et aspirations du personnel de la DG INFSO

Avis du 23 septembre 2011 sur la notification en vue d'un contrôle préalable concernant la base de données de la cartographie des compétences et aspirations du personnel de la DG INFSO (dossier 2011-0614)

Projet «IDEAS-Exclusion d'experts par les proposant» - ERCEA

Avis du 21 septembre 2011 sur la notification en vue d'un contrôle préalable concernant le projet «IDEAS-Exclusion d'experts par les proposant»,

l'Agence exécutive du Conseil européen de la recherche (ERCEA) (dossier 2010-661)

Détermination et paiement de traitements et d'indemnités

Avis du 19 septembre 2011 sur la notification d'un contrôle préalable concernant le traitement de données à caractère personnel par les services de la Fondation européenne pour l'amélioration des conditions de vie et de travail (Eurofound) en vue de «la détermination et du paiement de traitements et d'indemnités» (dossier 2011-644)

Enquêtes administratives et procédures disciplinaires - Cour de Justice

Avis du 12 septembre 2011 sur la notification mise à jour concernant les enquêtes administratives et procédures disciplinaires au sein de la Cour de Justice de l'UE (dossier 2011-0806)

Perfectionnement des cadres de la DG Traduction

Avis du 9 septembre 2011 sur la notification en vue d'un contrôle préalable concernant le retour d'information en vue du perfectionnement des cadres de la DGT (dossier 2011-0511)

Sélection et recrutement d'experts nationaux détachés à Fusion for Energy

Avis du 9 septembre 2011 sur les notifications de contrôle préalable concernant les traitements de données ayant trait à la sélection et au recrutement d'experts nationaux détachés (END) à Fusion for Energy (F4E) (dossier 2011-0340)

Experts Nationaux Détachés

Lettre du 9 septembre 2011 sur la notification de contrôle préalable concernant des traitements de données relatifs aux «Experts Nationaux Détachés» (END) (dossier 2011-0557)

Système de contrôle d'accès physique de la Commission (PACS)

Avis du 8 septembre 2011 sur le «système de contrôle d'accès physique (PACS): Projet de sécurisation PSG globale» de la Commission (dossier 2011-0427)

Procédure de sélection d'agents temporaires

Avis du 29 juillet 2011 sur la notification d'un contrôle préalable sur les traitements liés à la procédure de sélection d'agents temporaires, organisée par la Commission européenne (CE) pour des «postes autres qu'encadrement ou conseil sans concours de l'EPSO» (dossier 2011-0559)

Échange électronique d'informations sur la sécurité sociale

Avis du 28 juillet 2011 sur la notification d'un contrôle préalable concernant le système d'échange électronique d'informations sur la sécurité sociale («EESSI») (dossier 2011-0016)

Demandes de travail à temps partiel - OCVV

Avis du 28 juillet 2011 sur une notification de contrôle préalable concernant les demandes de travail à temps partiel à l'Office communautaire des variétés végétales (dossier 2011-0299)

Procédure de mobilité

Avis du 27 juillet 2011 sur la notification d'un contrôle préalable à propos du dossier «Procédure de mobilité» (dossier 2011-648)

Comité exécutif et groupe consultatif technique de Fusion for Energy

Avis du 26 juillet 2011 sur les notifications de contrôle préalable reçues du délégué à la protection des données de Fusion for Energy concernant les appels à manifestation d'intérêt pour la nomination d'experts externes au sein du comité exécutif et du groupe consultatif technique de Fusion for Energy (dossiers conjoints 2011-0363 et 2011-0364)

Étude de reconnaissance des empreintes digitales des enfants de moins de 12 ans

Avis du 25 juillet 2011 sur une notification de contrôle préalable concernant l'«étude de reconnaissance des empreintes digitales des enfants de moins de 12 ans» (dossier 2011-0209)

Gestion des crèches du Parlement à Bruxelles

Avis du 25 juillet 2011 sur la notification d'un contrôle préalable à propos du dossier «Gestion des crèches du Parlement à Bruxelles» (dossier 2010-0385)

Système de contrôle de l'accès

Avis du 15 juillet 2011 sur une notification de contrôle préalable concernant le système de contrôle de l'accès au site Ispra du CCR (dossier 2010-0902)

Traitement de données dans le cadre d'enquêtes administratives et de procédures disciplinaires - AESA

Lettre du 13 juillet 2011 sur la notification d'un contrôle préalable concernant le traitement de données dans le cadre d'enquêtes administratives et de procédures disciplinaires (EA&PD) à l'Agence européenne de la sécurité aérienne (AESA) à la lumière des lignes directrices du CEPD relatives aux EA&PD (dossier 2011-0558)

Congés de maladie à l'OHMI

Avis du 12 juillet 2011 sur la notification d'un contrôle préalable concernant le contrôle et la gestion des congés de maladie à l'Office d'harmonisation dans le marché intérieur (dossier 2010-0263)

Agents intérimaires - Comité des régions

Lettre du 30 juin 2011 sur la notification d'un contrôle préalable concernant des traitements de données relatifs aux agents intérimaires au Comité des régions (dossier 2010-0796)

Traitement de données dans le cadre d'enquêtes administratives et de procédures disciplinaires

Avis du 22 juin 2011 sur des notifications de contrôle préalable concernant le dossier «Traitement de données dans le cadre d'enquêtes administratives et de procédures disciplinaires» dans plusieurs agences de l'UE (dossier 2010-0752)

Système de gestion de la qualité et des contrôles de qualité ex post - OHMI

Avis du 9 juin 2011 sur la notification d'un contrôle préalable au sujet du système de gestion de la qualité et des contrôles de qualité ex post de l'Office de l'harmonisation dans le marché intérieur (OHMI) (dossier 2010-0869)

Sélection des stagiaires - OCVV

Lettre du 1^{er} juin 2011 sur une notification de contrôle préalable concernant le traitement des données en relation avec la sélection des stagiaires à l'OCVV (dossier 2011-0214)

Procédure de sélection des END au CCR

Avis du 30 mai 2011 sur la notification d'un contrôle préalable concernant la «procédure de sélection des END au CCR» (dossier 2008-0141)

Évaluation du personnel au CEDEFOP

Avis du 24 mai 2011 sur la notification d'un contrôle préalable concernant l'évaluation du personnel au Centre européen pour le développement de la formation professionnelle (dossier 2010-0620)

Procédure de certification - OCVV

Avis du 19 mai 2011 sur la notification d'un contrôle préalable concernant la procédure de certification à l'Office communautaire des variétés végétales (dossier 2011-0055)

Système de coopération en matière de protection des consommateurs («SCPC»)

Avis du 4 mai 2011 sur la notification d'un contrôle préalable relatif au système de coopération en matière de protection des consommateurs («SCPC») (dossier 2009-0019)

Procédures de passation des marchés publics - EACEA

Avis du 29 avril 2011 sur la notification d'un contrôle préalable concernant les procédures de passation des marchés publics à l'Agence exécutive «Éducation, audiovisuel et culture» (dossier 2011-0135)

Procédures de passation de marché et d'octroi de subvention, y compris les appels à manifestation d'intérêt - AEE

Avis du 18 avril 2011 sur la notification d'un contrôle préalable concernant le dossier: «Procédures de passation de marché et d'octroi de subvention, y compris les appels à manifestation d'intérêt» à l'Agence environnementale européenne (dossier 2011-0103)

Sélection des membres du comité scientifique consultatif du Comité européen du risque systémique - BCE

Avis du 13 avril 2011 sur la notification d'un contrôle préalable à propos de la «sélection des membres du comité scientifique consultatif du Comité européen du risque systémique» à la Banque centrale européenne (dossier 2011-0101)

«Politique anti-harcèlement et la création d'un réseau interagences de conseillers confidentiels» et «la sélection de conseillers confidentiels»

Avis du 11 avril 2011 sur les notifications de contrôle préalable concernant «la politique anti-harcèlement et la création d'un réseau interagences de conseillers confidentiels» et «la sélection de conseillers confidentiels» (dossier 2011-0151)

Sélection et recrutement de fonctionnaires, agents temporaires et agents contractuels - F4E

Lettre du 7 avril 2011 sur une notification d'un contrôle préalable concernant la sélection et le recrutement de fonctionnaires, agents temporaires et agents contractuels à Fusion for Energy (F4E) (dossier 2010-0454)

«Gestion des congés» et «gestion des congés de convenance personnelle et des congés sans rémunération» - OCVV

Avis conjoint du 28 mars 2011 sur deux notifications de contrôles préalables concernant la «gestion des congés» et la «gestion des congés de convenance personnelle et des congés sans rémunération» à l'Office communautaire des variétés végétales (dossiers 2010-0073/0075)

Sélection et désignation des membres du comité scientifique et des groupes scientifiques - EFSA

Avis du 21 mars 2011 sur la notification d'un contrôle préalable concernant «la sélection et la désignation des membres du comité scientifique et des groupes scientifiques de l'EFSA» (dossier 2010-0980)

Gestion des dossiers de recrutement des agents temporaires - CCR

Avis du 9 mars 2011 sur une notification de contrôle préalable concernant la gestion des dossiers de recrutement des agents temporaires du Centre commun de recherche (CCR) (dossier 2008-0143)

Rapports de performance et de comptabilité analytique - OHMI

Avis du 2 mars 2011 sur la notification d'un contrôle préalable concernant «les rapports de performance et de comptabilité analytique» (dossier 2009-0771)

Traitement des données dans le cadre de la sélection et du recrutement de stagiaires - ERA

Lettre du 2 mars 2011 concernant la notification de contrôle préalable relatif au traitement des données dans le cadre de la sélection et du recrutement de stagiaires à l'ERA (dossier 2010-0313)

CRIS – Suivi de la disponibilité des experts en mission dans le contexte du CC - CE

Avis du 23 février 2011 sur la notification d'un contrôle préalable concernant le «CRIS – Suivi de la disponibilité des experts en mission dans le contexte du CC» (dossier 2010-0465)

Traitement des données relatives à la santé sur le lieu de travail

Avis du 11 février 2011 sur les notifications d'un contrôle préalable concernant «Le traitement des données relatives à la santé sur le lieu de travail» (dossier 2010-0071)

Traitements «points d'écoute/procédures informelles» - EMA

Avis du 7 février 2011 sur une notification de contrôle préalable concernant les traitements «points d'écoute/procédures informelles» (gestion des cas de harcèlement psychologique ou sexuel) (dossier 2010-0598)

Évaluation du directeur de l'OEDT

Avis du 26 janvier 2011 sur la notification d'un contrôle préalable concernant la période probatoire, la période probatoire de gestion et l'évaluation annuelle des performances du directeur de l'Observatoire européen des drogues et des toxicomanies (dossier 2010-0895)

Annexe F — Liste des avis et observations formelles sur des propositions législatives

Avis sur des propositions législatives

Politique agricole commune après 2013

Avis du 14 décembre 2011 sur les propositions législatives sur la politique agricole commune après 2013

Utilisation et transfert des données des dossiers passagers au ministère américain de la sécurité intérieure

Avis du 9 décembre 2011 sur la proposition de décision du Conseil relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers (données PNR) au ministère américain de la sécurité intérieure

Système d'information du marché intérieur («IMI»)

Avis du 22 novembre 2011 sur la proposition de la Commission de règlement du Parlement européen et du Conseil concernant la coopération administrative par l'intermédiaire du système d'information du marché intérieur («IMI»)

Régime communautaire de contrôle afin d'assurer le respect des règles de la politique commune de la pêche

Avis du 28 octobre 2011 sur le règlement d'exécution (UE) n° 404/2011 de la Commission du 8 avril 2011 portant modalités d'application du règlement (CE) n° 1224/2009 du Conseil instituant un régime communautaire de contrôle afin d'assurer le respect des règles de la politique commune de la pêche

Paquet législatif relatif aux victimes de la criminalité

Avis du 17 octobre 2011 sur le paquet législatif relatif aux victimes de la criminalité, incluant une proposition de directive établissant des normes minimales concernant les droits, le soutien et la protection des victimes de la criminalité et une proposition de règlement relatif à la reconnaissance mutuelle des mesures de protection en matière civile

Ordonnance européenne de saisie conservatoire des comptes bancaires

Avis du 13 octobre 2011 sur une proposition de règlement du Parlement européen et du Conseil portant création d'une ordonnance européenne de saisie conservatoire des comptes bancaires, destinée à faciliter le recouvrement transfrontalier de créances en matière civile et commerciale

Contrôle par les autorités douanières du respect des droits de propriété intellectuelle

Avis du 12 octobre 2011 sur la proposition de règlement du Parlement européen et du Conseil concernant le contrôle, par les autorités douanières, du respect des droits de propriété intellectuelle

Neutralité du Net

Avis du 7 octobre 2011 sur la neutralité du net, la gestion du trafic et la protection de la vie privée et des données à caractère personnel

Appareil de contrôle dans le domaine des transports par route

Avis du 5 octobre 2011 sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (CEE) n° 3821/85 du Conseil concernant l'appareil de contrôle dans le domaine des transports par route et modifiant le règlement (CE) n° 561/2006 du Parlement européen et du Conseil

Statistiques européennes de la sécurité face à la criminalité

Avis du 19 septembre 2011 sur la proposition de règlement du Parlement européen et du Conseil relatif aux statistiques européennes de la sécurité face à la criminalité

Contrats de crédit relatifs aux biens immobiliers à usage résidentiel

Avis du 25 juillet 2011 sur la proposition de directive du Parlement européen et du Conseil sur les contrats de crédit relatifs aux biens immobiliers à usage résidentiel

Données PNR - Australie

Avis du 15 juillet 2011 sur la proposition de décision du Conseil relative à la conclusion de l'accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au service australien des douanes et de la protection des frontières

Migration

Avis du 7 juillet 2011 sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions sur la migration

Exigences techniques pour les virements et les prélèvements en euros

Avis du 23 juin 2011 sur la proposition de règlement du Parlement européen et du Conseil établissant des exigences techniques pour les virements et les prélèvements en euros et modifiant le règlement (CE) n° 924/2009

Intégrité et transparence du marché de l'énergie

Avis du 21 juin 2011 sur la proposition de règlement du Parlement européen et du Conseil concernant l'intégrité et la transparence du marché de l'énergie

Enquêtes effectuées par l'Office européen de lutte antifraude (OLAF)

Avis du 1^{er} juin 2011 sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (CE) n° 1073/1999 relatif aux enquêtes effectuées par l'Office européen de lutte antifraude (OLAF) et abrogeant le règlement (EURATOM) n° 1074/1999

Rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant la directive sur la conservation des données (directive 2006/24/CE)

Avis du 31 mai 2011 sur le rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant la directive sur la conservation des données (directive 2006/24/CE)

Interconnexion des registres centraux, du commerce et des sociétés

Avis du 6 mai 2011 sur la proposition de directive du Parlement européen et du Conseil modifiant les directives 89/666/CEE, 2005/56/CE et 2009/101/CE en ce qui concerne l'interconnexion des registres centraux, du commerce et des sociétés

Système de coopération en matière de protection des consommateurs («SCPC»)

Avis du 5 mai 2011 sur le système de coopération en matière de protection des consommateurs («SCPC») et sur la recommandation de la Commission 2011/136/UE concernant les lignes directrices régissant l'application de règles relatives à la protection des données au système de coopération en matière de protection des consommateurs (SCPC)

Produits dérivés négociés de gré à gré, contreparties centrales et référentiels centraux

Avis du 19 avril 2011 sur la proposition de règlement du Parlement européen et du Conseil sur les produits dérivés négociés de gré à gré, les contreparties centrales et les référentiels centraux

Règles financières applicables au budget annuel de l'Union

Avis du 15 avril 2011 sur la proposition de règlement du Parlement européen et du Conseil relatif aux règles financières applicables au budget annuel de l'Union

Données des dossiers passagers

Avis du 25 mars 2011 sur l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière

Turbine (TrUsted Revocable Biometric IdeNtitiEs)

Avis du 1^{er} février 2011 sur un projet de recherche financé par l'Union européenne en vertu du septième programme-cadre (7PC) de recherche et de développement technologique - Turbine (TrUsted Revocable Biometric IdeNtitiEs)

Approche globale de la protection des données à caractère personnel dans l'Union européenne

Avis du 14 janvier 2011 sur la communication de la Commission intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne»

Observations formelles sur des propositions législatives

Proposition modifiée de règlement (CE) n° 1073/1999 relatif à l'OLAF

Lettre du 19 décembre 2011 concernant un nouvel article et un nouveau considérant dans la proposition modifiée de règlement (CE) n° 1073/1999 relatif à l'OLAF

Programme «Droits et citoyenneté»

Lettre du 19 décembre 2011 sur la proposition de règlement du Parlement européen et du Conseil établissant, pour la période 2014-2020, le programme «Droits et citoyenneté»

Mise en œuvre du système d'appel d'urgence paneuropéen harmonisé embarqué à bord des véhicules (appels «eCall»)

Commentaires du CEPD du 12 décembre 2011 sur la recommandation de la Commission et l'évaluation d'impact qui l'accompagne concernant la mise en œuvre du système d'appel d'urgence paneuropéen harmonisé embarqué à bord des véhicules (appels «eCall»)

Commentaires du CEPD sur diverses propositions législatives concernant certaines mesures restrictives à l'encontre de l'Afghanistan, de la Syrie et de la Birmanie/Myanmar

Lettre du 9 décembre 2011 au président du Conseil de l'Union européenne sur diverses propositions législatives concernant certaines mesures restrictives à l'encontre de l'Afghanistan, de la Syrie et de la Birmanie/Myanmar

Commentaires du CEPD sur une proposition de directive relative à l'efficacité énergétique

Lettre du 27 octobre 2011 à M. Günther H. Oettinger, commissaire chargé de l'énergie, sur une proposition de directive du Parlement européen et du Conseil relative à l'efficacité énergétique et abrogeant les directives 2004/8/CE et 2006/32/CE

Système européen de surveillance du financement du terrorisme (SSFT)

Commentaires sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions du 13 juillet 2011, intitulée «Options envisageables pour la création d'un système européen de surveillance du financement du terrorisme»

Vers une politique de l'UE en matière pénale: assurer une mise en œuvre efficace des politiques de l'UE au moyen du droit pénal

Commentaires du CEPD du 24 octobre 2011 sur la communication de la Commission européenne intitulée «Vers une politique de l'UE en matière pénale: assurer une mise en œuvre efficace des politiques de l'UE au moyen du droit pénal»

Normes de base communes dans le domaine de la sûreté de l'aviation civile

Commentaires du 17 octobre 2011 sur les projets de propositions de règlement de la Commission et de règlement d'exécution de la Commission sur des normes de base communes dans le domaine de la sûreté de l'aviation civile concernant l'utilisation de scanners corporels dans les aéroports de l'Union européenne

Commentaires du CEPD sur la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale

Lettre du 20 septembre 2011 à M^{me} Viviane Reding, vice-présidente de la Commission européenne, sur une proposition de règlement du Parlement européen et du Conseil concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale

Commentaires du CEPD sur le paquet anticorruption

Lettre du CEPD du 6 juillet 2011 sur la communication de la Commission intitulée «La lutte contre la corruption dans l'Union européenne» et la décision de la Commission instituant un mécanisme de suivi de l'Union européenne en matière de lutte contre la corruption aux fins d'une évaluation périodique

Directive relative au respect des droits de propriété intellectuelle

Réponse du CEPD du 8 avril 2011 à la consultation de la Commission sur son rapport relatif à l'application de la directive relative au respect des droits de propriété intellectuelle

Diverses propositions législatives concernant certaines mesures restrictives, à l'encontre de l'Iran, en République de Guinée-Bissau, en Côte d'Ivoire, en Biélorussie, en Tunisie, en Lybie et en Égypte

Lettre du CEPD du 16 mars 2011 concernant les diverses propositions législatives concernant certaines mesures restrictives, à l'encontre de l'Iran, en République de Guinée-Bissau, en Côte d'Ivoire, en Biélorussie, en Tunisie, en Lybie et en Égypte.

Annexe G — Discours du contrôleur et du contrôleur adjoint en 2011

En 2011, le contrôleur et le contrôleur adjoint ont continué de consacrer beaucoup de temps et d'efforts à l'explication de leur mission et à la sensibilisation à la protection des données en général, ainsi qu'à un certain nombre de questions particulières, à l'occasion de discours et de contributions similaires devant différentes institutions et dans divers États membres.

Parlement européen

| | |
|-------------|---|
| 12 janvier | Contrôleur, Commission JURI, groupe de travail sur le droit administratif (Bruxelles) |
| 26 janvier | Contrôleur, Commission JURI, données sensibles sur l'internet (Bruxelles) |
| 14 mars | Contrôleur adjoint, Commission ITRE, projet de règlement sur l'ENISA (Bruxelles) |
| 31 mars | Contrôleur, ETICA, éthique et gouvernance des TIC futurs et émergents (Bruxelles) (*) |
| 13 avril | Contrôleur, Commission LIBE, accès du public aux documents (Bruxelles) (*) |
| 27 avril | Contrôleur, Conférence JURI sur le droit administratif (León) |
| 15 juin | Contrôleur et contrôleur adjoint, Commission LIBE, rapport annuel 2010 (Bruxelles) (**) |
| 4 octobre | Contrôleur, Commission LIBE, cyber-attaques contre les systèmes d'information (Bruxelles) (*) |
| 10 novembre | Contrôleur, Commission LIBE, charte européenne des droits fondamentaux (Bruxelles) (*) |

Conseil

| | |
|------------|---|
| 17 janvier | Contrôleur, Groupe de travail sur la protection des données et l'échange d'informations (Bruxelles) |
|------------|---|

| | |
|----------------------|---|
| 27 janvier | Contrôleur, Représentation permanente de la Pologne, Journée de la protection des données (Bruxelles) |
| 1 ^{er} mars | Contrôleur adjoint, Groupe de travail sur le règlement ENISA (Bruxelles) (*) |
| 4 mai | Contrôleur adjoint, Groupe de travail sur la protection des données et l'échange d'informations (Bruxelles) (*) |
| 16 juin | Contrôleur et contrôleur adjoint, Conférence internationale sur la protection des données (Budapest) (*) |
| 23 juin | Contrôleur adjoint, Groupe de travail sur les questions générales relatives aux données PNR de l'UE (Bruxelles) |
| 21 septembre | Contrôleur, Conférence internationale sur la protection des données (Varsovie) |
| 18 novembre | Contrôleur adjoint, Conférence ministérielle sur l'administration en ligne (Poznań) (*) |
| 23 novembre | Contrôleur adjoint, Groupe de travail sur les statistiques de la sécurité face à la criminalité (Bruxelles) (*) |

Commission européenne

| | |
|--------------|--|
| 28 janvier | Contrôleur, Réunion conjointe de haut niveau sur la protection des données (Bruxelles) (*) |
| 22 juin | Contrôleur, Conférence sur la conservation des données (Bruxelles) |
| 22 juin | Contrôleur adjoint, Groupe européen d'éthique (GEE) (Bruxelles) |
| 15 septembre | Contrôleur, Secrétaire général et directeurs généraux |
| 28 septembre | Contrôleur adjoint, CE-Etsi sur les normes dans le nuage (*) |
| 20 octobre | Contrôleur adjoint, Sixième symposium sur la sécurité (Bruxelles) (*) |

Autres institutions et organes de l'Union européenne

| | |
|------------|---|
| 11 janvier | Contrôleur adjoint, Comité économique et social européen (Bruxelles) |
| 28 janvier | Contrôleur et contrôleur adjoint, Journée de la protection des données (Bruxelles) (**) |
| 7 février | Contrôleur, École européenne d'administration, Erasmus (Bruxelles) |
| 9 février | Contrôleur adjoint, Comité économique et social européen (Bruxelles) (*) |
| 28 mars | Contrôleur, École européenne d'administration, Erasmus (Bruxelles) |
| 8 juin | Contrôleur adjoint, Atelier pour les délégués à la protection des données (Bruxelles) |
| 13 octobre | Contrôleur, Directeurs des agences européennes (Helsinki) |
| 20 octobre | Contrôleur adjoint, École européenne d'administration, Erasmus (Bruxelles) |

Conférences internationales

| | |
|--------------|---|
| 27 janvier | Contrôleur, Ordinateurs, vie privée et protection des données (Bruxelles) |
| 27 janvier | Contrôleur adjoint, Ordinateurs, vie privée et protection des données (Bruxelles) (*) |
| 10 mars | Contrôleur, Sommet mondial sur la vie privée de l'IAPP (Washington DC) |
| 5 avril | Contrôleur et contrôleur adjoint, Autorités européennes chargées de la protection des données (Bruxelles) |
| 12 juillet | Contrôleur, Privacy Laws & Business (Cambridge) |
| 1er novembre | Contrôleur et contrôleur adjoint, Commissaires à la vie privée et à la protection des données (Mexico) |
| 21 novembre | Contrôleur adjoint, Conseil de l'Europe sur les droits de l'enfant (2012-2015) (Monaco) (*) |

30 novembre Contrôleur, IAPP Europe (Paris)

2 décembre Contrôleur adjoint, Conseil consultatif professionnel et scientifique international (ISPAC) de l'ONU et CNPDS sur la cybercriminalité (Courmayeur) (*)

6 décembre Contrôleur, Protection des données et vie privée dans l'UE (Bruxelles)

Autres événements

19 janvier Contrôleur, Institut Boltzmann pour les droits de l'homme (Vienne)

26 janvier Contrôleur, Association GSM (Bruxelles)

3 février Contrôleur adjoint, Forum FIDE sur la protection des données dans l'UE (Madrid)

10 février Contrôleur, Centre de politique européenne (Bruxelles)

11 février Contrôleur, Université de Louvain, faculté de droit (Louvain)

17 février Contrôleur, Centre d'étude des politiques européennes (Bruxelles)

21 février Contrôleur, Sénat du parlement néerlandais (La Hague)

23 février Contrôleur, Conférence INET de l'Internet Society (Francfort) (**)

24 février Contrôleur, Conférence sur la protection des données (Édimbourg)

24 février Contrôleur adjoint, Atelier du CRID sur l'informatique dématérialisée (Bruxelles)

2 mars Contrôleur, Sécurité informatique et protection de la vie privée dans les communications électroniques (Copenhague)

21 mars Contrôleur adjoint, Justice et protection des citoyens (Bruxelles)

23 mars Contrôleur, Atelier «principes relatifs au respect de la vie privée» (Copenhague)

| | | | |
|----------|--|--------------|---|
| 24 mars | Contrôleur, Séminaire d'experts sur la justice en ligne, bureau de la Saxe (Bruxelles) (*) | 8 juin | Contrôleur adjoint, Forum PSC Europe, conférence sur la vidéosurveillance (Bruxelles) (*) |
| 29 mars | Contrôleur adjoint, Table ronde numérique d'EUROISPA (Bruxelles) | 15 juin | Contrôleur, Séminaire européen sur la biométrie (Bruxelles) |
| 30 mars | Contrôleur, Audition à la chambre des députés italienne (Rome) (*) | 28 juin | Contrôleur, L'internet des objets (Bruxelles) |
| 8 avril | Contrôleur adjoint, Cour de cassation italienne, droit pénal et l'internet (Rome) | 5-6 juillet | Contrôleur adjoint, Consent Social Networking Summit (Göttingen) (*) |
| 14 avril | Contrôleur, Forum «ordinateurs et protection des données» (Copenhague) | 7 juillet | Contrôleur, Université d'Édimbourg, école de droit (*) |
| 3 mai | Contrôleur, Conseil de l'Europe, accès du public aux documents (Bruxelles) | 19 septembre | Contrôleur, FD Blueprint, examen de la protection des données (Bruxelles) |
| 5 mai | Contrôleur, C-PET, relations entre l'UE et les États-Unis (Washington DC) | 20 septembre | Contrôleur, Droit des médias et protection des données (Londres) |
| 6 mai | Contrôleur, Conférence RISE sur la biométrie (Washington DC) | 27 septembre | Contrôleur, 10e anniversaire de l'EPOF (Bruxelles) |
| 9 mai | Contrôleur adjoint, Université de Rome, droits fondamentaux au sein de l'UE (Rome) | 28 septembre | Contrôleur, RIM, sécurité de l'information (Berlin) |
| 12 mai | Contrôleur, Clyde & Co, séminaire sur la protection des données (Londres) | 29 septembre | Contrôleur, Centre pour la réforme européenne (Bruxelles) |
| 12 mai | Contrôleur adjoint, Forum bancaire européen (Bruxelles) | 4 octobre | Contrôleur, Sommet du Conseil européen de Lisbonne, agenda numérique (Bruxelles) |
| 17 mai | Contrôleur, Journée européenne de la protection des données (Berlin) | 28 octobre | Contrôleur, Protection des données dans la procédure pénale (Madrid) |
| 20 mai | Contrôleur adjoint, AIDP, respect de la vie privée sur le lieu de travail (Cagliari) | 9 novembre | Contrôleur, Conférence NAID-ARMA (Londres) |
| 25 mai | Contrôleur adjoint, Phase de responsabilisation III (Madrid) | 18 novembre | Contrôleur adjoint, Lobbying, transparence et institutions de l'UE (Bruxelles) |
| 26 mai | Contrôleur adjoint, ISMS Forum, flux transfrontaliers de données (Madrid) | 25 novembre | Contrôleur, Conférence sur les analyses d'impact sur la vie privée (Berlin) |
| 26 mai | Contrôleur, Biometrics Institute Australia (Sydney) (*) et (**) | 10 décembre | Contrôleur, Felix Meritis, Bescherming Burgerrechten (Amsterdam) |
| 27 mai | Contrôleur, Data Protection Intensive (Londres) | | |

(*) Texte disponible sur le site internet du CEPD

(**) Vidéo disponible sur le site internet du CEPD

Annexe H — Composition du secrétariat du CEPD



Le Contrôleur et le Contrôleur adjoint en compagnie de la majorité de leur personnel.

Directeur, chef du Secrétariat

Christopher DOCKSEY

• Supervision et mise en application

| | |
|--|--|
| Sophie LOUVEAUX <i>Chef d'unité a.i.</i> | Pierre VERNHES Conseiller juridique |
| Laurent BESLAY (*) <i>Coordinateur sécurité et technologie</i> | Jaroslav LOTARSKI <i>Coordinateur réclamations</i> |
| Maria Verónica PEREZ ASINARI <i>Coordinateur consultations</i> | Athena BOURKA <i>Expert national détaché</i> |
| Bart DE SCHUITENEER <i>Conseiller Technologies Local Security Officer/LISO</i> | Raffaele DI GIOVANNI BEZZI <i>Conseiller juridique</i> |
| Elisabeth DUHR <i>Expert national détaché</i> | Delphine HAROU <i>Conseiller juridique</i> |
| John-Pierre LAMB (*) <i>Expert national détaché</i> | Ute KALLENBERGER <i>Conseiller juridique</i> |
| Xanthi KAPSOSIDERI <i>Conseiller juridique</i> | Luisa PALLA <i>Assistante supervision et mise en application</i> |
| Dario ROSSI <i>Assistant supervision et mise en application Correspondant Comptabilité Gestionnaire de l'entrepôt externe de données (EDWM)</i> | Galina SAMARAS <i>Assistante supervision et mise en application</i> |
| Tereza STRUNCOVA <i>Conseiller juridique</i> | Michaël VANFLETEREN <i>Conseiller juridique</i> |

• Politique législative et consultation

| | |
|---|--|
| Hielke HIJMANS <i>Chef d'unité</i> | Bénédicte HAVELANGE (*) <i>Coordinatrice grands systèmes TI et politique des frontières</i> |
| Herke KRANENBORG <i>Coordinateur procédures judiciaires</i> | Anne-Christine LACOSTE <i>Coordinatrice coopération avec les APD</i> |
| Rosa BARCELO (*) <i>Conseiller juridique</i> | Zsuzsanna BELENYESSY <i>Conseiller juridique</i> |
| Gabriel Cristian BLAJ <i>Conseiller juridique</i> | Alba BOSCH MOLINE <i>Conseiller juridique</i> |
| Isabelle CHATELIER <i>Conseiller juridique</i> | Katarzyna CUADRAT-GRZYBOWSKA <i>Conseiller juridique</i> |
| Priscilla DE LOCHT <i>Conseiller juridique / Agent contractuel</i> | Per JOHANSSON <i>Conseiller juridique</i> |
| Owe LANGFELDT <i>Conseiller juridique / Intérimaire</i> | Roberto LATTANZI (*) <i>Expert national détaché</i> |
| Parminder MUDHAR <i>Assistante politique législative et consultation</i> | Alfonso SCIROCCO (*) <i>Délégué à la protection des données Gestion de la qualité</i> |
| Vera POZZATO <i>Conseiller juridique</i> | Luis VELASCO <i>Conseiller technologies</i> |

• Registre et assistance opérationnelle

| | |
|---|---|
| Andrea BEACH <i>Chef de secteur</i> | Marta CORDOBA-HERNANDEZ <i>Assistante administrative</i> |
| Christine HUC (*) <i>Assistante administrative</i> | Kim DAUPHIN <i>Assistante administrative</i> |
| Milan KUTRA <i>Assistant administratif</i> | Kim Thien LÊ <i>Assistante administrative</i> |
| Ewa THOMSON <i>Assistante administrative</i> | |

• Information et communication

| | |
|--|--|
| Nathalie VANDELLE (*) <i>Chef de secteur</i> | Olivier ROSSIGNOL <i>Chef de secteur a.i.</i> |
| Agnieszka NYKA <i>Assistante information et communication</i> | Benoît PIRONET <i>Développeur Web / Contractant</i> |

• Ressources humaines, budget et administration

| | |
|---|--|
| Leonardo CERVERA NAVAS <i>Chef d'unité</i> | Isabelle DELATTRE <i>Assistante finances et comptabilité</i> |
| Anne LEVÊCQUE <i>Assistante Ressources humaines GECO</i> | Vittorio MASTROJENI <i>Conseiller ressources humaines</i> |
| Julia MALDONADO MOLERO <i>Agent contractuel</i> | Daniela OTTAVI <i>Assistante finances et comptabilité</i> |
| Aida PASCU <i>Assistante administrative Assistante LSO</i> | Sylvie PICARD <i>Délégué à la protection des données COFO - ICO</i> |
| Anne-Françoise REYNDERS <i>Assistante administrative</i> | Maria SANCHEZ LOPEZ <i>Conseiller finances et comptabilité</i> |

(*) Membres du personnel ayant quitté le CEPD au cours de l'année 2011

Le Contrôleur Européen de la Protection des Données

Rapport annuel 2011

Luxembourg: Office des publications de l'Union européenne

2012 — 126 p. — 21 × 29,7 cm

ISBN 978-92-95073-29-6

doi:10.2804/36295

COMMENT VOUS PROCURER LES PUBLICATIONS DE L'UNION EUROPÉENNE?

Publications gratuites:

- sur le site EU Bookshop (<http://bookshop.europa.eu>);
- auprès des représentations ou des délégations de l'Union européenne.
Vous pouvez obtenir leurs coordonnées en consultant le site <http://ec.europa.eu>
ou par télécopieur au numéro +352 2929-42758.

Publications payantes:

- sur le site EU Bookshop (<http://bookshop.europa.eu>).

Abonnements facturés (par exemple séries annuelles du *Journal officiel de l'Union européenne*, recueils de la jurisprudence de la Cour de justice de l'Union européenne):

- auprès des bureaux de vente de l'Office des publications de l'Union européenne (http://publications.europa.eu/others/agents/index_fr.htm).



LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

*Le gardien européen
de la protection des données personnelles*

www.edps.europa.eu



Office des publications

ISBN 978-92-95073-29-6



9 789295 073296