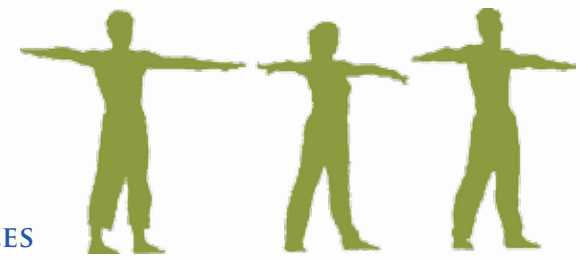
ISSN 1830-9607

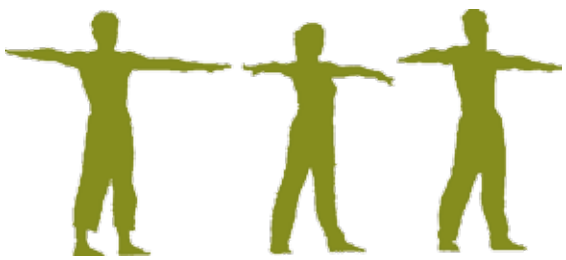
Rapport annuel 2013

Le Contrôleur Européen
de la protection des données



Rapport annuel

2013



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

Un numéro unique gratuit (*):

00 800 6 7 8 9 10 11

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

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

Luxembourg: Office des publications de l'Union européenne, 2014

ISBN 978-92-95076-85-3
doi: 10.2804/58291

Table des matières

Guide de l'utilisateur 7
Déclaration de mission, valeurs et principes 9
Avant-propos 11

1. FAITS MARQUANTS DE 2013 12

1.1 Aperçu général de 2013 12
1.2. Stratégie 2013-2014 17

2. SUPERVISION ET MISE EN APPLICATION 20

2.1. Introduction 20
2.2. Délégués à la protection des données 21
2.3. Contrôles préalables 22
2.3.1. Base juridique 22
2.3.2. Procédure 22
2.3.3. Principales questions liées aux contrôles préalables 25
2.3.4. Notifications retirées ou non soumises au contrôle préalable 28
2.3.5. Suivi des avis de contrôle préalable 29
2.3.6. Conclusions 29
2.4. Réclamations 29
2.4.1. Les fonctions du CEPD 29
2.4.2. Procédure de traitement des réclamations 30
2.4.3. Confidentialité garantie aux plaignants 32
2.4.4. Réclamations traitées en 2013 33
2.5. Contrôle du respect du règlement 34
2.5.1. Exercice général de contrôle et de compte rendu 34
2.5.2. Visites 35
2.5.3. Inspections 36
2.6. Consultations relatives aux mesures administratives 39
2.6.1. Consultations au titre de l'article 28, paragraphe 1, et de l'article 46, point d) 39
2.7. Orientations en matière de protection des données 41
2.7.1. Lignes directrices thématiques 41
2.7.2. Formations et ateliers 42
2.7.3. Coin des DPD et autres outils 43

3. CONSULTATION 44

3.1. Introduction: vue d'ensemble de l'année et tendances principales 44
3.2. Cadre d'action et priorités 45
3.2.1. Mise en œuvre de la politique de consultation 45
3.2.2. Résultats en 2013 46
3.3. Révision du cadre européen en matière de protection des données 46
3.4. Espace de liberté, de sécurité et de justice et coopération internationale 47
3.4.1. Renforcer la coopération dans le domaine de la répression au sein de l'UE: le modèle européen en matière d'échange d'informations 47
3.4.2. Europol 48
3.4.3. Stratégie de cybersécurité de l'Union européenne 49
3.4.4. Frontières intelligentes 49
3.4.5. Accord UE-Canada relatif aux données des dossiers passagers (PNR) 49
3.5. Marché intérieur, comprenant les données financières 50
3.5.1. Droit européen des sociétés et gouvernance d'entreprise 50
3.5.2. Règlement concernant la surveillance du marché des produits 50
3.5.3. Frais liés aux comptes de paiement 50
3.5.4. Lutte contre le blanchiment de capitaux 51
3.5.5. Vente de contrefaçons sur l'internet 52
3.5.6. Protection des marques 52
3.5.7. Facturation électronique dans le cadre des marchés publics 52
3.5.8. Paiements dans le marché intérieur 53
3.6. Stratégie numérique et technologie 53
3.6.1. Équipement radio 53
3.6.2. La stratégie numérique pour l'Europe - faire du numérique un moteur de la croissance européenne 54

3.6.3. Se préparer à un monde audiovisuel totalement convergent: croissance, création et valeurs 54
3.6.4. Marché unique européen des communications électroniques 55
3.7. Santé publique et consommateurs 55
3.7.1. Précurseurs de drogues et pays tiers 55
3.7.2. Dispositifs médicaux 56
3.7.3. Plan d'action pour la santé en ligne 56
3.7.4. Précurseurs de drogues et Russie 56
3.7.5. Prix des médicaments à usage humain 57
3.8. Publication d'informations personnelles 57
3.8.1. Règlement relatif aux procédures d'insolvabilité 57
3.9. Transports 58
3.9.1. Comptes rendus d'évènements dans l'aviation civile 58
3.9.2. Transport intelligent 58
3.9.3. eCall 59
3.10. Autres questions 59
3.10.1. Échanges automatiques d'informations fiscales 59
3.11. Stratégie du CEPD en matière d'accès aux documents 60
3.12. Affaires judiciaires 60
3.13. Priorités pour 2014 62

4 COOPERATION

4. COOPERATION 64

4.1. Groupe de travail «Article 29» 64
4.2. Supervision coordonnée 65
4.2.1. EURODAC 66
4.2.2. VIS 66
4.2.3. SID 67
4.2.4. Système d'information Schengen (SIS II) 68
4.3. Conférence européenne 69
4.4. Conférence internationale 69
4.5. Autres coopérations internationales 70
4.5.1. Conseil de l'Europe 70
4.5.2. OCDE 71
4.5.3. CEAP 71
4.5.4. Association francophone (AFAPDP) 71
4.5.5. Groupe de Berlin 72

5 SUIVI DE LA TECHNOLOGIE

5. SUIVI DE LA TECHNOLOGIE 73

5.1. Évolution technologique et protection des données 73
5.2. Sécurité et surveillance de l'internet 74
5.2.1. Primitives cryptographiques 74
5.2.2. Protocoles et architecture 75
5.2.3. Mise en application 75
5.2.4. Déploiement 75
5.2.5. Anonymisation 76
5.2.6. Suivi 78
5.2.7. L'internet des objets 80
5.3. Biométrie 82
5.3.1. Génomique personnelle 82
5.3.2. Reconnaissance faciale 82
5.4. Frontières 83
5.5. Drones 84

6 INFORMATION ET COMMUNICATION

6. INFORMATION ET COMMUNICATION 85

6.1. Introduction 85
6.2. Caractéristiques de la communication 86
6.2.1. Principaux publics et groupes cibles 86
6.2.2. Politique linguistique 86
6.3. Relations avec les médias 86
6.3.1. Communiqués de presse 87
6.3.2. Interviews 87
6.3.3. Conférences de presse 87
6.3.4. Demandes formulées par les médias 87
6.4. Demandes d'informations et de conseils 88
6.5. Visites d'étude 88
6.6. Outils d'information en ligne 88
6.6.1. Site internet 88
6.6.2. Newsletter 89
6.6.3. Twitter 89

6.6.4. LinkedIn 90
6.7. Publications 90
6.7.1. Rapport annuel 90
6.7.2. Publications thématiques 91
6.8. Actions de sensibilisation 91
6.8.1. Journée de la protection des données 2013 92
6.8.2. Journée portes ouvertes de l'UE 2013 92

7. ADMINISTRATION, BUDGET ET PERSONNEL 93

7.1. Introduction 93
7.2. Budget, finances et marchés publics 93
7.2.1. Budget 93
7.2.2. Finances 95
7.2.3. Marchés publics 95
7.3. Ressources humaines 96
7.3.1. Recrutement 96
7.3.2. Professionnalisation de la fonction RH 96
7.3.3. Programme de stages 97
7.3.4. Programme pour les experts nationaux détachés 97
7.3.5. Organigramme 97
7.3.6. Conditions de travail 97
7.3.7. Apprentissage et développement des compétences 97
7.3.8. Activités sociales et questions familiales 99
7.4. Fonctions de contrôle 99
7.4.1. Contrôle interne 99
7.4.2. Audit interne 100
7.4.3. Audit externe 100
7.5. Infrastructure 100
7.6. Environnement administratif 101
7.6.1. Assistance administrative et coopération interinstitutionnelle 101
7.6.2. Gestion des documents 101

8. DELEGUE A LA PROTECTION DES DONNEES DU CEPD 103

8.1. Le DPD du CEPD 103
8.2. Le registre des traitements 103
8.3. Enquête de 2013 du CEPD sur le statut des DPD 104
8.4. Information et sensibilisation 104

9. PRINCIPAUX OBJECTIFS POUR 2014 106

9.1. Supervision et mise en application 106
9.2. Politique et consultation 107
9.3. Coopération 108
9.4. Politique IT 109
9.5. Autres domaines 109

Annexe A — Cadre juridique 111
Annexe B — Extrait du règlement (CE) n° 45/2001 114
Annexe C — Liste des abréviations 116
Annexe D — Liste des délégués à la protection des données 118
Annexe E — Liste des avis de contrôle préalable et des avis sur l'absence de contrôle préalable 121
Annexe F — Liste des avis et observations formelles sur des propositions législatives 129
Annexe G — Discours du contrôleur et du contrôleur adjoint en 2013 132
Annexe H — Composition du secrétariat du CEPD 136

GUIDE DE L'UTILISATEUR

Le lecteur trouvera, immédiatement après ce guide, l'avant-propos du rapport annuel 2013, rédigé par M. Peter Hustinx, contrôleur européen de la protection des données, et M. Giovanni Buttarelli, contrôleur adjoint, précédé de l'énoncé de leur mission.

Le chapitre 1 — **«Faits marquants de 2013»**, présente les grands axes de nos activités en 2013 ainsi que nos réalisations à la lumière des principaux indicateurs de performance 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 2013. Il contient également des informations sur les orientations en matière de protection des données fournies par le CEPD soit dans des lignes directrices thématiques, soit dans le cadre de formations et d'ateliers.

Le chapitre 3 — **«Consultation»**, traite de l'évolution de notre rôle consultatif. Il s'intéresse principalement aux avis et observations formulés sur les propositions législatives et documents connexes, ainsi qu'à leur incidence dans un nombre croissant de domaines. 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. Ce chapitre aborde également l'implication du CEPD dans les litiges soumis à la Cour de justice de l'UE.

Le chapitre 4 — **«Coopération»**, décrit notre travail dans des forums importants comme, par exemple, le groupe de travail «Article 29» et différents groupes veillant à la supervision coordonnée (par le CEPD et par les autorités nationales chargées de la protection des données) des systèmes d'information à grande échelle ainsi que lors des conférences européenne et internationale sur la protection des données. Il couvre également notre coopération avec les organisations internationales et les pays tiers.

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

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

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

Le chapitre 8 — **«Délégué à la protection des données (DPD) du CEPD»**, inclut une mise à jour du registre des traitements du CEPD en 2013.

Le chapitre 9 **— Main objectives for 2013** outlines our main priorities for 2014.

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

Un résumé de ce rapport est également disponible, avec une vue d'ensemble synthétique des principaux développements intervenus en 2013 dans les activités du CEPD.

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

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

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

 @EU_EDPS

DÉCLARATION DE MISSION, VALEURS ET PRINCIPES

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

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

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

Valeurs fondamentales

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

Principes directeurs

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

[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, et en application de l'article 16 du traité sur le fonctionnement de l'Union européenne.

Le présent rapport concerne l'année 2013, dixième année d'activité du CEPD en tant qu'autorité de contrôle indépendante, dont la mission est de veiller à ce que, lors du traitement de données à caractère personnel, les libertés et droits fondamentaux des personnes physiques, en particulier leur vie privée, soient respectés par les institutions et organes de l'UE. Ce rapport couvre également la dernière année de notre mandat commun en tant que membres de cette autorité.

Notre stratégie 2013-2014, ainsi que notre règlement intérieur et notre plan de gestion annuel, nous ont fourni des conseils précieux, exprimant la vision et la méthodologie requises pour améliorer notre capacité à travailler de manière efficace dans un climat d'austérité. Notre institution a désormais atteint sa pleine maturité et dispose d'objectifs et d'indicateurs de performance clairs.

Tout au long de l'année 2013, nous avons accordé une attention particulière aux différents domaines d'activité mettant en œuvre le plan d'action établi dans notre stratégie. 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 croissant d'institutions et organes. De plus, nous avons réalisé un certain nombre d'enquêtes qui ont révélé que la plupart des institutions et organes de l'UE, y compris de nombreuses agences, ont fait des progrès notables dans le respect du règlement relatif à la protection des données, tandis que d'autres devraient renforcer leurs efforts.

En ce qui concerne la procédure de consultation, en matière de conseils sur les nouvelles mesures législatives, la révision du cadre juridique de l'UE pour la protection des données était toujours en tête de nos priorités. La stratégie numérique et les risques que font peser les nouvelles technologies sur le respect de la vie privée ont également considérablement caractérisé l'année 2013. Toutefois, la mise en œuvre du programme de Stockholm dans le domaine de la liberté, de la sécurité et de la justice, et les questions liées au marché intérieur comme la réforme du secteur financier ou encore les débats relatifs à la santé publique et à la protection des consommateurs ont aussi eu des répercussions sur la protection des données. Nous avons également renforcé notre coopération avec d'autres autorités de surveillance, en particulier en ce qui concerne les systèmes d'information à grande échelle.

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, ont soutenu 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 ont largement contribué à l'efficacité de notre action pendant l'ensemble de notre mandat.

Peter Hustinx
Contrôleur européen de la protection des données

Giovanni Buttarelli
Contrôleur adjoint

1 FAITS MARQUANTS DE 2013

1.1. Aperçu général de 2013

Dix ans après sa création, le CEPD a atteint sa maturité en tant qu'organisation et est en mesure de faire face aux nombreux défis qu'une autorité chargée de la protection des données doit relever dans un environnement très dynamique. Le principal défi opérationnel auquel nous avons été confrontés en 2013 a été de faire progresser le volume et la portée de nos activités malgré les contraintes budgétaires et les mesures liées aux ressources en raison de la crise financière.

Notre stratégie 2013-2014, ainsi que notre règlement intérieur et notre plan de gestion annuel, nous ont fourni des conseils précieux, exprimant la vision et la méthodologie requises pour améliorer notre capacité à travailler de manière efficace dans un climat d'austérité.

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

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

Ces fonctions sont analysées dans les chapitres 2, 3 et 4, qui présentent notre vision, nos principales activités et les progrès réalisés en 2013. Certains éléments-clés sont toutefois résumés dans ce chapitre.

En 2013, nous avons amélioré nos capacités technologiques. Le chapitre 5 expose en détail certaines évolutions technologiques spécifiques qui présentent une pertinence particulière pour le respect de la vie privée et la protection des données.

L'importance de l'information et de la communication pour nos activités principales continue également de croître, et le chapitre 6 présente nos travaux en matière de communication en 2013.

Toutes nos activités reposent sur une gestion efficace des ressources financières, humaines et autres, qui font l'objet du chapitre 7.

Supervision et mise en application

Nous avons observé une augmentation du nombre de notifications de contrôle préalable reçues dans le cadre de nos activités de supervision et de mise en application. Cette augmentation s'explique

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

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

principalement par le délai, fixé à juin 2013, pour la soumission des notifications de contrôle préalable ex post concernant les opérations de traitement déjà en cours. Bien qu'en ce qui concerne les affaires ex post, le CEPD ne soit pas tenu d'adopter un avis dans un délai de deux mois, nous nous sommes néanmoins efforcés de rendre notre avis dans un délai plus court. La hausse du nombre d'avis émis durant l'année résulte également du nombre élevé de notifications reçues. Nous avons continué à assurer le suivi des recommandations formulées dans les avis antérieurs du CEPD relatifs aux contrôles préalables et avons pu clôturer un nombre considérable de cas.

Le nombre de réclamations reçues a diminué, ce qui est en partie dû à une meilleure information sur les compétences du CEPD et à une sensibilisation accrue à cet égard, mais également à l'efficacité de notre formulaire de réclamation en ligne.

Une des caractéristiques du plan d'action établi dans notre stratégie 2013-2014 consiste à promouvoir une «culture de protection des données» au sein des institutions et organes de l'UE de sorte qu'ils soient au fait de leurs obligations et assument la responsabilité du respect des exigences relatives à la protection des données.

À la lumière de ce qui précède, nous avons continué à fournir des orientations et des formations aux responsables du traitement, aux délégués à la protection des données (DPD) et aux coordinateurs de la protection des données (CPD), principalement sous la forme de lignes directrices en matière de marchés publics, de subventions et d'experts externes; de l'organisation d'une formation de base, destinée aux nouveaux DPD, sur la procédure de contrôle préalable ainsi que d'une formation spéciale destinée aux DPD de cinq entreprises communes de l'Union. Nos initiatives de sensibilisation dans les institutions et organes de l'Union européenne ont notamment consisté à organiser des ateliers pour les responsables du traitement à la Fondation européenne pour la formation (ETF) et à l'Agence européenne de défense (EDA) ainsi que des ateliers généraux relatifs à la communication électronique, à l'utilisation de dispositifs mobiles sur le lieu de travail et aux sites Internet gérés par les institutions et les organes de l'Union européenne.

Un volet important de notre travail a également consisté à sensibiliser à la protection des données à tous les niveaux de direction, en particulier en rendant visite aux institutions ou organes caractérisés par des cas de non-respect des règles de protection des données ou de manque de communication. Une visite se compose généralement d'une visite sur place par le contrôleur ou le contrôleur adjoint et produit habituellement de bons résultats en ce qui concerne la participation de la direction et la sensibilisation à la protection des données.

Un autre élément fondamental a été notre dialogue continu avec les responsables du traitement, les DPD et les CPD en vue de soutenir le travail des DPD. Ces réunions nous aident à mieux comprendre les contraintes rencontrées par les institutions en vue de leur donner des conseils concrets. De nombreuses réunions ont eu lieu avec des responsables du traitement, soit dans le cadre de contrôles préalables soit dans le cadre du suivi des avis et décisions. Les réunions du réseau des DPD, les réunions bilatérales et la ligne d'assistance pour les DPD ont constitué des instruments de communication utiles pour notre travail avec les DPD et les CPD.

Les résultats de notre quatrième état des lieux général («enquête 2013»), lancé le 17 juin 2013 dans le cadre de nos activités de contrôle de la conformité, seront publiés début 2014. En janvier 2013, nous avons également publié un rapport présentant les résultats de l'enquête relative au statut des coordinateurs de la protection des données à la Commission européenne.

En 2013, nous avons adopté notre politique d'inspections: elle définit les principaux éléments de la procédure d'inspection du CEPD, fournit des orientations à l'ensemble des acteurs concernés et garantit la transparence vis-à-vis des parties prenantes. Sur la base des expériences antérieures, nous avons élaboré et adopté un manuel d'inspection interne complet à l'intention des membres du personnel du CEPD chargés d'effectuer les inspections.

Consultation

Ces dernières années, le nombre d'avis émis par le CEPD concernant des propositions de textes législatifs de l'Union et de documents y afférents a connu une hausse constante. En 2013, ce nombre a diminué: nous avons émis 20 avis législatifs et 13 séries d'observations formelles, et nous avons adressé 33 conseils informels à la Commission ou à d'autres institutions. Deux éléments principaux expliquent cette diminution: le fait que nos efforts visant à privilégier les priorités stratégiques ont porté leurs fruits, et le fait que de nombreuses ressources ont été consacrées à la réforme du cadre relatif à la protection des données.

Tout au long de l'année 2013, nous sommes restés étroitement associés au travail en cours concernant la réforme du cadre européen relatif à la protection des données. Le 15 mars 2013, nous avons adressé au Parlement européen, à la Commission et au Conseil des observations supplémentaires au sujet de la réforme. Nous avons également continué de participer aux débats qui ont suivi, tant au Parlement qu'au Conseil.

En outre, la Commission a publié un grand nombre de propositions législatives ayant des incidences sur le droit fondamental à la protection des données à caractère personnel.

Nous avons abordé le sujet de la stratégie numérique et de l'internet à plusieurs reprises, notamment dans notre avis sur la communication de la Commission intitulée «Une stratégie numérique pour l'Europe – faire du numérique un moteur pour la croissance européenne», dans notre avis relatif au «Marché unique européen des communications électroniques» et dans notre avis sur le livre vert intitulé «Se préparer à un monde audiovisuel totalement convergent: croissance, création et valeurs.

En ce qui concerne l'espace de liberté, de sécurité et de justice (ELSJ), nous avons émis des avis sur Europol, la stratégie de l'Union en matière de cybersécurité, les frontières intelligentes, les données des dossiers passagers (données PNR) UE-Canada ainsi que sur le modèle européen en matière d'échange d'informations.

Nos avis particulièrement importants concernant le marché intérieur ont été les suivants: avis sur la lutte contre le blanchiment de capitaux et le financement du terrorisme, les paiements au sein du marché intérieur, le droit européen des sociétés et la gouvernance d'entreprise et la facturation électronique dans le cadre des marchés publics.

Dans le domaine des services de santé en ligne, nous souhaitons attirer l'attention sur nos avis sur les dispositifs médicaux, sur les précurseurs de drogues et sur le plan d'action pour la santé en ligne.

Affaires judiciaires

En 2013, le CEPD est intervenu dans plusieurs affaires portées devant la Cour de justice de l'Union européenne et le Tribunal de la fonction publique.

Le CEPD a présenté une plaidoirie lors d'une audience devant la grande chambre de la Cour de justice dans le cadre d'une procédure de renvoi préjudiciel. Cette audience concernait les affaires jointes: Digital Rights Ireland (C-293/12) et Seitlinger et autres (C-293/12). Ces deux affaires portent sur la validité de la directive 2006/24/CE sur la conservation des données.

C'est la première fois que la Cour invitait le CEPD à comparaître à une audience dans le cadre d'une procédure de renvoi préjudiciel. Pour le CEPD, il s'agissait d'une étape importante susceptible d'aboutir à une décision historique sur une question que nous suivons attentivement depuis plusieurs années.

Le CEPD a plaidé dans l'affaire Commission c. Hongrie (C-288/12). Cette affaire est la troisième procédure d'infraction relative à l'indépendance des autorités chargées de la protection des données, les deux autres étant les affaires Commission c.

Autriche (C-614/10) et Commission c. Allemagne (C-518/07) dans lesquelles des arrêts ont respectivement été rendus en 2012 et en 2010.

D'autres affaires dans lesquelles le CEPD est intervenu sont toujours en instance, notamment Pachtitis c. Commission et EPSO (T-374/07), Pachtitis c. Commission (F-35/08), ZZ c. BEI (affaire F-103/11) ainsi que Dennekamp c. Parlement européen (T-115/13).

En octobre 2013, le CEPD a demandé le droit d'intervenir dans deux autres affaires: Elmaghraby et El Gazaerly c. Conseil de l'Union européenne (affaire T-319/13) et CN c. Parlement (affaire T-343/13).

Coopération

En ce qui concerne la coopération, nous avons continué de contribuer activement aux activités du groupe de travail «Article 29. En particulier, nous avons fortement contribué en tant que rapporteur ou co-rapporteur sur les avis relatifs à la limitation de la finalité et à l'intérêt légitime (sous-groupe «Dispositions-clés»), l'avis sur le modèle d'analyse d'impact relative à la protection des données (sous-groupe «Technologie»), et l'avis relatif aux données ouvertes (sous-groupe «Administration en ligne»).

La coopération directe avec les autorités nationales est de plus en plus importante dans le cadre du développement de bases de données internationales à grande échelle comme EURODAC, le système d'information sur les visas (VIS), le système d'information Schengen II (SIS II) et le système d'information douanier (SID), qui nécessitent une approche coordonnée de la supervision. En 2013, nous avons fourni des services de secrétariat au nouveau groupe de coordination de la supervision de SIS II (SCG) et nous avons continué de présider les groupes de coordination d'EURODAC, VIS et du SID.

En 2013, les modifications relatives à la supervision coordonée ont soulevé des difficultés. Le nouveau règlement EURODAC a introduit des modifications importantes telles que la possibilité, pour les autorités responsables de l'application de la loi, d'accéder aux données d'EURODAC. En outre, SIS II est devenu opérationnel. Afin de réduire les contraintes financières, administratives et en matière de déplacements, nous avons organisé des réunions consécutives des groupes de coordination de supervision et nous nous sommes efforcés d'établir des politiques de contrôle horizontales et cohérentes concernant les systèmes d'information à grande échelle, le cas échéant.

Le modèle des groupes de coordination de supervision sera élargi en 2014 par la création d'un groupe de coordination de supervision pour le système d'information du marché intérieur (IMI). En 2013, nous avons consulté les autorités nationales chargées de la protection des données (APD) et la Commission pour faire le point sur la situation et sur les évolutions du règlement IMI, afin d'organiser la première réunion du groupe en 2014.

Le modèle de supervision coordonnée est devenu une norme pour le législateur de l'Union et, dans plusieurs propositions telles que celles sur Europol, sur les frontières intelligentes, sur Eurojust et sur le parquet européen, la Commission a suggéré que ce modèle soit utilisé.

La coopération au sein de forums internationaux a continué d'attirer l'attention, en particulier dans le cadre de la conférence européenne et de la

conférence internationale des commissaires à la protection des données et à la vie privée. En 2013, la conférence européenne organisée à Lisbonne était axée sur les développements récents dans la modernisation des cadres de protection des données de l'Union, du Conseil de l'Europe et de l'Organisation de coopération et de développement économiques (OCDE). Les discussions ont plus spécifiquement porté sur les notions de données à caractère personnel, de droits des personnes sur l'internet et de sécurité des informations.

La conférence internationale qui s'est tenue à Varsovie était axée sur les réformes en matière de protection des données mises en place partout dans le monde, sur l'interaction avec les technologies, ainsi que sur les rôles et perspectives de différents acteurs, y compris les personnes concernées, les responsables du traitement des données et les autorités de contrôle.

Dans le cadre du Conseil de l'Europe, nous avons participé à trois réunions du comité consultatif de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Il était particulièrement important pour nous de participer à ces réunions afin de pouvoir suivre et influencer la modernisation en cours de la Convention.

Nous avons également participé aux travaux du groupe d'experts chargé de mettre à jour les lignes directrices de l'OCDE sur la protection de la vie privée.

Nous avons par ailleurs apporté une contribution significative aux questions liées à la protection des données dans plusieurs autres forums importants tels que la Coopération économique Asie-Pacifique (CEAP), l'Association francophone des autorités de protection des données personnelles (AFAPDP) et le groupe de travail international sur la protection des données dans les télécommunications (Groupe de Berlin).

Politique IT

Eu égard à notre politique en matière de technologies de l'information, nous avons contribué à plusieurs avis sur des propositions de la Commission, qui revêtent une dimension stratégique pour l'avenir de la société numérique en Europe, comme l'avis du groupe de travail «Article 29» sur les réseaux intelligents dans le cadre duquel le CEPD était rapporteur. Notre expertise IT nous a également conduits à effectuer une visite auprès de l'agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle dans le contexte de la migration du SIS II. Cette expertise s'est avérée très utile dans nos activités de supervision, y compris dans le cadre des réclamations, des contrôles préalables et des inspections.

Chiffres clés du CEPD en 2013

- → **91 avis de contrôle préalable adoptés, 21 avis sur l'absence de contrôle préalable**
- → **78 réclamations reçues, dont 30 recevables**
- → **37 consultations reçues concernant des mesures administratives**
- → **8 inspections sur place (y compris 2 visites d'information) et 3 visites effectuées**
- → **1 ligne directrice publiée concernant le traitement des informations à caractère personnel dans le domaine des marchés publics**
- → **20 avis législatifs publiés**
- → **13 séries d'observations formelles publiées**
- → **33 séries d'observations informelles publiées**

Cette expertise IT a favorisé nos échanges avec le personnel compétent de l'administration de l'Union dans le cadre de l'élaboration de nos lignes directrices relatives à la protection des données et à la technologie; ces échanges ont amorcé des discussions au sein des institutions de l'Union concernant l'approche générale qu'elles adoptent à l'égard de l'évaluation des risques et des mesures de sécurité, compte tenu des faiblesses avérées de certains outils cryptographiques et de sécurité couramment utilisés.

Information et communication

Dans le domaine de la communication, nous avons renforcé la visibilité du CEPD au niveau institutionnel dans l'exercice de nos trois fonctions principales: la supervision, la consultation et la coopération. Nous utilisons plusieurs indicateurs, tels que

le nombre de demandes d'informations soumises par les citoyens, le nombre de demandes de renseignement provenant des médias et le nombre de demandes d'entretien (relations avec la presse), le nombre d'abonnés à notre newsletter, le nombre de personnes suivant le CEPD sur Twitter, ainsi que le nombre d'invitations à venir s'exprimer à des conférences et le trafic sur le site internet. Tous ces indicateurs tendent à montrer que nous sommes de plus en plus perçus comme un point de référence pour les questions liées à la protection des données au niveau de l'Union européenne. Le nombre de visites sur le site web du CEPD a connu une hausse constante au cours de l'année (63 % par rapport à 2012) et le nombre de visites d'étude a augmenté (17 groupes, contre deux en 2012), tout comme le nombre de demandes d'informations et de conseils soumises par des particuliers (176 demandes écrites, soit une augmentation de 51 % par rapport à 2012). En décembre, nous avons créé une page spécifiquement consacrée à notre organisation sur LinkedIn, ce qui constitue un autre moyen de promouvoir le CEPD en tant qu'institution, de renforcer notre présence en ligne et d'améliorer notre visibilité.

Organisation interne

À la suite du départ du chef du secteur «Opérations, planning et assistance» après la mise en service de notre système de gestion des dossiers en octobre 2013, nous avons restructuré notre organigramme de sorte que l'équipe de gestion des dossiers rend désormais compte au directeur.

Conformément aux recommandations du service d'audit interne (SAI) et afin de renforcer l'efficacité, la fonction de coordinateur du contrôle interne a été séparée de l'équipe chargée des ressources humaines, du budget et de l'administration, et elle rend désormais également compte au directeur.

Gestion des ressources

En 2013, nous sommes parvenus à accroître notre taux d'exécution du budget. Néanmoins, le résultat final n'a pas répondu à nos attentes, en raison de la décision de la Cour de justice relative à l'ajustement des salaires du personnel de l'Union européenne. Cette décision inattendue a été adoptée tard dans l'année, ce qui n'a laissé qu'une très faible marge de manœuvre pour organiser un redéploiement. En outre, le fait que le Conseil refuse d'envisager tout transfert opéré à partir du budget des salaires vers d'autres lignes budgétaires a réduit encore davantage la marge de manœuvre. Si le Conseil et le Parlement étaient parvenus à un accord avant la fin de l'année, comme le souhaitait la Commission, le taux d'exécution final (84,7 %) aurait été plus élevé (87,2 %).

1.2. Stratégie 2013-2014

Dans notre stratégie 2013-2014, nous avons défini plusieurs objectifs stratégiques afin d'accroître les incidences de nos activités principales sur la protection des données au niveau européen. Pour évaluer les progrès accomplis dans cette direction, nous avons déterminé les activités essentielles pour la réalisation de ces objectifs. Les indicateurs clés de performance (ICP) correspondants nous permettront de contrôler et d'ajuster, si nécessaire, les incidences de nos activités et l'efficacité avec laquelle nous utilisons les ressources.

Nous présentons dans ce chapitre les réalisations de nos activités en 2013, conformément aux objectifs stratégiques et au plan d'action définis dans la stratégie 2013-2014. Les activités de mise en œuvre du plan d'action sont résumées dans l'aperçu général de 2013 (section 1.1).

De manière générale, les résultats témoignent d'une tendance positive dans l'exercice de nos activités. Globalement, la mise en œuvre de la stratégie est en bonne voie et aucune mesure corrective n'est nécessaire au stade actuel.

Le tableau de bord des ICP

Le tableau de bord des ICP comprend une description succincte des ICP et des méthodes de calcul.

Dans la plupart des cas, les indicateurs sont mesurés par rapport aux objectifs initiaux. Pour trois de ces indicateurs, les résultats de 2013 serviront de valeurs de référence pour les années suivantes.

De gauche à droite les membres du conseil d'administration du CEPD: Christopher Docksey, Directeur; Peter Hustinx, Contrôleur; Giovanni Buttarelli, Contrôleur adjoint

ICP	Description	Résultats 2013	Objectif pour 2013
ICP 1	Nombre d'inspections ou de visites effectuées. Mesure : par rapport à l'objectif.	3 visites 8 inspections	8 (au minimum)
ICP 2	Nombre d'initiatives de sensibilisation et de formation au sein des institutions et organes de l'Union que nous avons organisées ou co-organisées (ateliers, réunions, conférences, formations et séminaires). Mesure : par rapport à l'objectif.	4 formations 4 ateliers (dont 3 en coopération avec le secteur ITP)	8 ateliers + formations
ICP 3	Niveau de satisfaction des DPD/CPD par rapport aux formations et aux orientations. Mesure : enquête de satisfaction auprès des DPD/CPD réalisée à chaque fois qu'une formation est organisée ou que des orientations sont publiées.	Formation de base pour les DPD: 70 % de réactions positives Formation du personnel de l'AED: 92 % de réactions positives	60 % de réactions positives
ICP 4	Nombre d'avis formels et informels formulés à l'endroit du législateur. Mesure : par rapport à l'année précédente.	Avis: 20 Observations formelles: 13 Observations informelles: 33	2013 sert de valeur de référence.
ICP 5	Taux d'exécution des dossiers dans notre inventaire de politiques devant faire l'objet d'une action. Mesure : pourcentage d'initiatives «dans le rouge» (pour lesquelles le délai de soumission d'observations est arrivé à échéance) mises en œuvre comme prévu dans l'inventaire 2013.	90 % (18/20)	90 %
ICP 6	Nombre d'affaires traitées par le groupe de travail «Article 29» pour lesquelles le CEPD a apporté une contribution écrite importante. Mesure : par rapport à l'année précédente.	13	2013 sert de valeur de référence
ICP 7	Nombre d'affaires pour lesquelles des orientations sur les développements technologiques sont fournies. Mesure : par rapport à l'année précédente.	21	20
ICP 8	Nombre de visites sur le site Internet du CEPD. Mesure : par rapport à l'année précédente.	293 029 (+ 63 % par rapport à 2012)	2013 sert de valeur de référence
ICP 9	Taux d'exécution du budget. Mesure : montant des paiements traités au cours de l'année, divisé par le budget annuel.	84,7 %	85 %
ICP 10	Taux de mise en œuvre des formations destinées au personnel du CEPD. Mesure : nombre de jours de formation effectifs divisé par le nombre estimé de jours de formation.	85 %	80 %

Les ICP mesurent la mise en œuvre des objectifs stratégiques comme suit:

1. **Promouvoir une *culture de protection des données* au sein des institutions et organes de l'Union européenne de manière à ce qu'ils soient au fait de leurs obligations et assument la responsabilité du respect des exigences relatives à la protection des données.**

   ICP n° 1, 2 et 3. Tous les objectifs ont été atteints.

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

   ICP n° 4 et 5. L'objectif correspondant à l'ICP n° 5 a été atteint. Les résultats de 2013 détermineront l'objectif pour l'ICP n° 4.

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

   Les résultats de 2013 détermineront l'objectif pour l'ICP n° 6.

   L'ICP n° 7 correspond aux objectifs stratégiques 1, 2 et 3. L'objectif a été atteint.

4. **Développer une stratégie de communication efficace et créative.**

   Les résultats de 2013 détermineront l'objectif pour l'ICP n° 8.

5. **Améliorer l'utilisation des ressources humaines, financières, techniques et organisationnelles du CEPD (au moyen de processus, compétences et connaissances appropriés).**

   ICP n° 9 et 10. L'objectif correspondant à l'ICP n° 10 a été atteint.

   Nous n'avons pas atteint l'objectif prévu pour l'ICP n° 9. À cet égard, même si nous avons accru notre taux d'exécution du budget, le résultat final n'a pas suffi pour remplir l'objectif, en raison de la décision de la Cour de justice relative à l'ajustement des salaires du personnel de l'Union européenne. Si la Cour avait approuvé l'approche proposée par la Commission, notre taux d'exécution final (84,7 %) aurait été plus élevé (87,2 %) et nous aurions atteint notre objectif.

2 SUPERVISION ET MISE EN APPLICATION

Notre objectif stratégique

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

Nos principes directeurs

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

2.1. Introduction

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

En 2013, dans le cadre de nos activités régulières de supervision, nous avons accordé une attention particulière au plan d'action défini dans notre stratégie 2013-2014. Une des caractéristiques du plan d'action consiste à promouvoir une «culture de protection des données» au sein des institutions et organes de l'Union européenne de sorte qu'ils soient au fait de leurs obligations et assument la responsabilité du respect des exigences relatives à la protection des données.

À la lumière de ce qui précède, nous avons continué à fournir des orientations et des formations aux responsables du traitement, aux délégués à la protection des données (DPD) et aux coordinateurs de la protection des données (CPD), sous la forme de lignes directrices en matière de marchés publics, de subventions et d'experts externes; de l'organisation d'une formation de base, destinée aux nouveaux DPD, sur la procédure de contrôle préalable; ainsi que d'une formation spéciale destinée aux DPD de cinq entreprises communes de l'Union. Nous avons également organisé des initiatives de sensibilisation au sein des institutions et organes de l'UE en organisant des ateliers pour les responsables du traitement à l'ETF et à l'EDA ainsi que des ateliers généraux relatifs à la communication électronique, à l'utilisation de dispositifs mobiles sur le lieu de travail et aux sites Internet gérés par les institutions et les organes de l'Union européenne.

Un volet important de notre travail a également consisté à sensibiliser à la protection des données à tous les niveaux de direction, en particulier en rendant visite aux organes de l'Union caractérisés par des cas de non-respect des règles de protection des données ou de manque de communication. Ces visites incluent généralement une réunion sur place avec le contrôleur ou le contrôleur adjoint, dont le résultat est positif: engagement de la direction et sensibilisation à la protection des données.

La promotion du dialogue avec les responsables du traitement, les DPD et les CPD est un élément essentiel de notre soutien aux activités du DPD et nous permet de mieux comprendre les contraintes des institutions de sorte que nous puissions donner des conseils pragmatiques. À cette fin, de nombreuses réunions ont eu lieu avec des responsables du traitement, soit dans le cadre de nos contrôles préalables soit dans le cadre du suivi des avis et décisions. Les réunions du réseau des DPD, les réunions bilatérales et la ligne d'assistance pour les DPD ont été des instruments de communication utiles pour notre travail avec les DPD et les CPD.

Dans le cadre de nos activités de contrôle de la conformité, nous avons lancé le 17 juin 2013 notre quatrième état des lieux général (Enquête 2013) dont les résultats devraient être publiés début 2014. En janvier 2013, nous avons également publié un rapport présentant les résultats de l'enquête relative au statut des coordinateurs de la protection des données (CPD) à la Commission européenne.

Cette année a également été marquée par l'adoption de notre politique d'inspection qui définit les éléments principaux de la procédure d'inspection du CEPD en vue de fournir des orientations à l'ensemble des acteurs concernés et de garantir la transparence vis-à-vis des parties prenantes. Sur la base des expériences tirées de nos inspections antérieures, nous avons élaboré un manuel d'inspection interne complet afin de fournir des orientations aux membres du personnel du CEPD chargés d'effectuer les inspections.

Tout au long de l'année, nos principales activités de supervision dans le domaine des contrôles préalables, des réclamations et des consultations sur les mesures administratives sont restées des priorités. Le contrôle préalable des traitements présentant des risques spécifiques est resté un aspect important des activités de supervision du CEPD en 2013. Nous avons enregistré une augmentation considérable du nombre de notifications reçues, ainsi qu'une augmentation du nombre d'avis adoptés (91 avis et 21 avis sur l'absence de contrôle préalable dont 8 avis conjoints couvrant 36 notifications).

Le nombre de réclamations reçues a diminué, ce qui est en partie dû à une meilleure information sur les compétences du CEPD et à une sensibilisation accrue à cet égard, mais également à l'efficacité de notre formulaire de réclamation en ligne. En 2013, le CEPD a reçu 37 consultations sur des mesures administratives.

2.2. Délégués à la protection des données

En vertu de l'article 24, paragraphe 1, du règlement, les institutions et les organes de l'Union européenne doivent désigner au moins un 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 (OLAF) afin que l'OLAF puisse exercer ses fonctions de manière indépendante. Plusieurs institutions ont également nommé des coordinateurs ou contacts de la protection des données (CPD) chargés de coordonner tous les aspects de la protection des données au sein d'une direction ou d'une unité particulière.

En 2013, cinq nouveaux DPD ont été nommés au sein d'institutions et d'organes existants et au sein des nouvelles agences ou entreprises communes, portant le nombre total des DPD à 62 (le DPD de la Banque centrale européenne fait également office de DPD du Comité européen du risque systémique; le CEDEFOP compte deux DPD).

Depuis plusieurs années, les DPD se rencontrent régulièrement afin de partager leurs expériences et d'examiner les questions horizontales. Ce réseau informel, qui a prouvé son efficacité et encourage la collaboration, s'est aussi réuni en 2013.

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 coordonné le réseau des DPD. Le CEPD a continué de collaborer étroitement avec ce quatuor.

Le CEPD a participé à la réunion des DPD qui s'est tenue en mars à l'Observatoire européen des drogues et des toxicomanies, à Lisbonne, et a organisé une autre réunion à Bruxelles en novembre. Nous avons profité de ces réunions pour fournir aux DPD des informations sur nos récents travaux et leur donner un aperçu de l'évolution récente de la protection des données dans l'Union. Cette année, nous avons en particulier privilégié la réforme de la protection des données, les évolutions au niveau européen et au niveau international, les développements dans le domaine judiciaire et les évolutions pertinentes des activités du CEPD comme le rapport relatif au statut des DPD et des CPD, les lignes directrices et les ateliers du CEPD et la fin des notifications de contrôle préalable ex post. Ces réunions ont également été l'occasion de discussions ouvertes entre les DPD et le CEPD concernant des questions et problèmes communs tels que le traitement des informations personnelles liées à l'utilisation de l'Internet et des réseaux de communication et les conflits d'intérêts.

En 2013, nous avons organisé plusieurs formations et ateliers pour les DPD et CPD (voir la section 2.7 «Orientations en matière de protection des données»). Des réunions individuelles ont également été organisées entre les membres du personnel et certains DPD en fonction de leurs besoins spécifiques d'orientation. Notre participation au programme de formation et de certification de l'IEAP pour les DPD a également contribué à soutenir les activités et le rôle des DPD.

Les membres de notre équipe «Supervision et mise en application» traitent également les questions posées par téléphone par les DPD et, dans la mesure du possible, leur apportent une aide et des conseils immédiats concernant des questions spécifiques (les questions plus complexes sont traitées dans le cadre de consultations par écrit). En réponse à l'augmentation du nombre de questions posées par téléphone, nous avons créé une ligne d'assistance téléphonique à l'attention des DPD qui est joignable à un horaire fixe pendant la semaine, lorsqu'un membre du personnel du CEPD répond aux questions par téléphone. Cette initiative porte ses fruits: elle nous permet de répondre rapidement et de manière informelle aux questions simples et de fournir des orientations spécifiques aux DPD. Cette ligne d'assistance directe renforce également la coopération et la communication entre nous et les DPD des institutions et organes de l'Union européenne.

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 sont 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 spécifiques. En 2013, le CEPD a continué d'appliquer les critères élaborés au cours des années précédentes[4] lors de l'interprétation de cette disposition, tant pour décider si une notification par un DPD doit faire l'objet d'un contrôle préalable ou non que pour émettre un avis dans le cadre d'une consultation sur la nécessité de procéder à un tel contrôle.

2.3.2. Procédure

2.3.2.1. Notification

Lorsque nous recevons une notification par courriel de la part d'un DPD, au moyen du formulaire standard du CEPD (article 19 du règlement intérieur), nous sommes tenus d'effectuer un contrôle préalable. Le DPD doit fournir des informations supplémentaires concernant l'opération de traitement notifiée dans une annexe au formulaire de notification.

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

Afin de résorber cet arriéré de dossiers de contrôles préalables ex post, le 5 juillet 2012, les institutions et

4 Voir le rapport annuel 2005, section 2.3.1.

les organes de l'Union européenne ont été invités à garantir que toutes les opérations de traitement soumises au contrôle préalable ont été notifiées au CEPD avant fin juin 2013 (à l'exception de certaines activités effectuées par les organes nouvellement créés dans l'impossibilité de notifier au préalable, comme le recrutement). Par conséquent, le CEPD a reçu 138 notifications entre début juin 2013 et fin juillet 2013 (pour un total de 272 notifications en 2013).

Consultations sur la nécessité de contrôles préalables: en cas de doute, les DPD peuvent consulter le CEPD quant à la nécessité d'un contrôle préalable en vertu de l'article 27, paragraphe 3, du règlement. En 2013, nous avons reçu 31 consultations de ce type de la part de DPD.

CJUE

Le DPD de la Cour de justice de l'Union européenne (CJUE) a consulté le CEPD sur la nécessité de présenter une notification de contrôle préalable pour trois traitements: infrastructure générale IT, conservation des journaux du serveur (log files) pour les applications IT et procédures de contrôle de l'internet. En ce qui concerne les deux premiers traitements, nous avons considéré qu'ils n'étaient pas soumis en tant que tels aux contrôles préalables dans la mesure où ils concernent plusieurs traitements différents à analyser séparément. Par exemple, l'infrastructure IT pourrait être utilisée pour un certain nombre d'applications différentes et à des fins différentes, comme en ce qui concerne le système de contrôle électronique, le système de gestion des dossiers, l'internet, etc. Parallèlement, les journaux du serveur peuvent être conservés et traités dans différentes applications et dans des circonstances multiples.

Nous avons toutefois considéré que le contrôle de l'utilisation de l'internet par les membres de la CJUE était soumis à un contrôle préalable dans la mesure où la finalité du traitement était d'évaluer des aspects de la personnalité pouvant être liés à des soupçons d'infraction. Nous avons recommandé que l'examen des courriels individuels identifiant l'utilisateur ne soit effectué que s'il existe des soupçons raisonnables de méfaits, corroborés par des éléments de preuve initiaux concrets et dans le cadre d'une enquête administrative.

2.3.2.2. Délai, suspension et prolongation

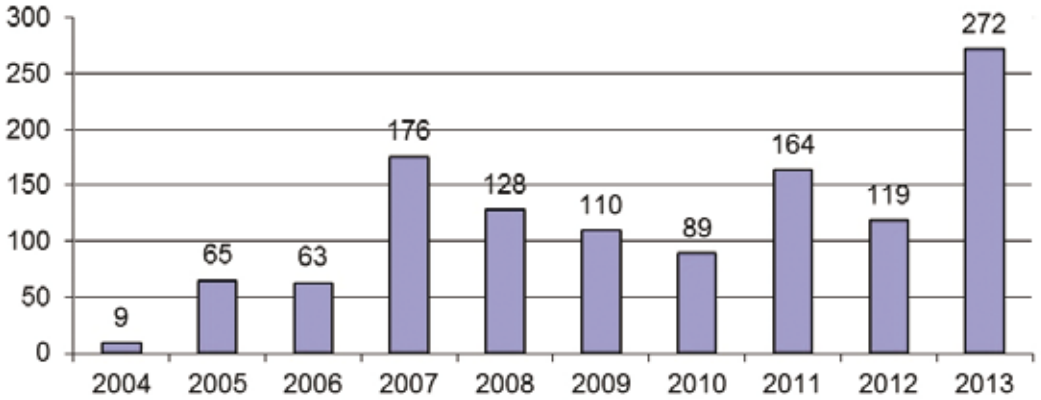
En vertu de l'article 27, paragraphe 4, du règlement et de l'article 21 du règlement intérieur, le CEPD doit rendre un avis dans un délai de deux mois après réception d'une notification[5]. Ce délai de deux mois peut être suspendu jusqu'à la réception d'informations supplémentaires éventuellement demandées par le CEPD. Lorsque la complexité du dossier le rend nécessaire, ce délai peut également être prolongé pour une nouvelle période de deux mois. Si, au terme du délai de deux mois, éventuellement prolongé, l'avis n'est pas rendu, il est considéré favorable. Jusqu'à présent, ce cas de figure dans lequel l'avis aurait été rendu de manière tacite ne s'est jamais produit. Le délai de deux mois commence à courir le lendemain de la réception du formulaire de notification. Si l'échéance tombe un jour férié ou un autre jour de fermeture des bureaux du CEPD, le jour ouvrable suivant est considéré comme la date ultime à laquelle l'avis doit être rendu.

Avant l'adoption d'un avis, nous envoyons un projet d'avis à l'institution concernée pour lui permettre de faire des commentaires sur les aspects pratiques et les inexactitudes factuelles éventuelles. Ces commentaires doivent nous parvenir dans un délai de 10 jours. Ce délai peut être prolongé moyennant une demande motivée par le responsable du traitement. Si aucun commentaire n'est reçu dans les délais, le CEPD adopte l'avis (article 22 du règlement intérieur).

2.3.2.3. Registre

En 2013, nous avons reçu 272 notifications de contrôle préalable (dont 2 ont été retirées). Même si

Notifications au CEPD



5 *Les notifications ex post sont maintenant traitées dans les meilleurs délais possibles, dans la mesure où le délai de deux mois pour l'adoption d'un avis ne s'applique pas.*

nous sommes venus à bout de l'arriéré des contrôles préalables ex post pour la plupart des institutions de l'UE, le délai fixé pour traiter toutes les notifications ex post, les autres 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 2013, ont entraîné une hausse considérable du nombre de notifications.

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

2.3.2.4. Avis

Conformément à l'article 27, paragraphe 4, du règlement, notre position finale concernant une opération de traitement revêt la forme d'un avis qui est notifié au responsable de cette opération et au DPD de l'institution ou de l'organe. En 2013, nous avons rendu 91 avis de contrôle préalable et 21 avis sur l'absence de contrôle préalable (voir la section 2.3.4). Ces chiffres prennent en considération le fait que nous avons traité un nombre important de dossier en rendant des avis conjoints: en 2013, nous avons rendu 8 avis conjoints (dont 3 concernaient des dossiers non soumis à un contrôle préalable) en réponse à un total de 36 notifications.

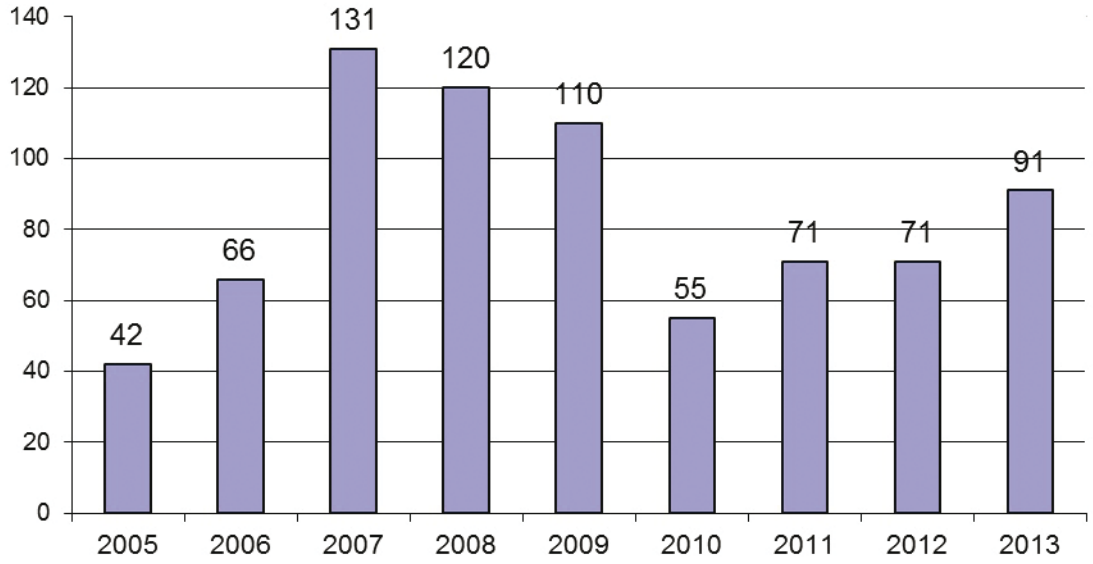
En 2013, nous avons continué d'adresser la majorité de nos avis aux agences et organes de l'Union. Les agences de l'UE ont continué de notifier leurs activités principales et leurs procédures administratives standardisées conformément aux procédures pertinentes du CEPD (voir la section 2.3.2.1).

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, nous incluons des recommandations à l'intention du responsable du traitement en vue de garantir le respect du règlement. Dans ses remarques de conclusion, le CEPD indique généralement que le traitement ne semble pas enfreindre les dispositions du règlement à condition que ces recommandations soient prises en compte, mais il peut bien sûr également exercer d'autres pouvoirs qui lui sont conférés en vertu de l'article 47 du règlement.

Une fois que nous avons rendu notre avis, celui-ci est publié. Tous nos avis sont disponibles sur notre site internet en trois versions linguistiques (en fonction des délais de traduction) avec, dans la plupart des cas, un résumé du dossier.

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

Avis de contrôle préalable du CEPD par an



2.3.3. Principales questions liées aux contrôles préalables

2.3.3.1. Limitation de la finalité / utilisation compatible

Plusieurs dossiers analysés en 2013 ont trait à la définition de l'utilisation compatible et font preuve d'une éventuelle tendance liée à l'utilisation ultérieure d'informations collectées à l'origine pour d'autres finalités. Le concept de la limitation de la finalité est une première étape essentielle dans l'application de la législation relative à la protection des données. La limitation de la finalité signifie que les informations personnelles ne peuvent être collectées qu'à des fins spécifiées, explicites et légitimes. Ce concept contribue à la transparence, à la sécurité juridique et à la prévisibilité et vise à protéger les individus en fixant des limites quant à la manière dont leurs informations sont utilisées.

Une notification de l'Autorité européenne de sécurité des aliments (EFSA) nous a permis de clarifier l'utilisation compatible des informations provenant du système de contrôle de l'accès. L'EFSA avait l'intention d'utiliser les informations contenues dans les badges d'accès pour contrôler la présence des membres du personnel au bureau. Alors que, dans notre réponse du 9 avril 2013, nous avons conclu que ce traitement particulier n'était pas soumis au contrôle préalable, nous avons souligné l'importance du principe de limitation de la finalité. Cela signifie que, dans chaque situation où l'utilisation ultérieure d'informations personnelles est envisagée, il convient d'opérer une distinction entre les utilisations supplémentaires qui sont «compatibles» et les autres utilisations qui sont considérées comme étant «incompatibles». Par exemple, la possibilité de relier une base de données de contrôle d'accès à une base de données de gestion du temps n'est pas compatible parce que cela nécessiterait une modification structurelle de la finalité. Dans le cas de l'EFSA, l'utilisation pourrait être considérée comme étant compatible en vue d'aider les employés en facilitant l'enregistrement de l'horaire flexible. Nous avons cependant exprimé des doutes quant à la nécessité de mettre en place un tel système dans la mesure où d'autres moyens existent et ne requièrent pas l'utilisation d'enregistrements provenant du système de contrôle de l'accès.

La Banque européenne d'investissement (BEI) nous a consultés sur la légalité d'analyser des informations provenant d'un système de sécurité de l'accès ou d'un système de gestion du temps pour d'autres finalités, à savoir des enquêtes afin d'instruire des procédures disciplinaires. Dans notre avis du 17 avril 2013, nous avons insisté sur le principe de limitation de la finalité, mais nous avons également fait remarquer qu'il offrait un certain degré de flexibilité à la BEI. À la suite d'une analyse des règles régissant les procédures disciplinaires et les enquêtes en matière de fraude au sein de la BEI, nous avons conclu que les limitations suivantes s'appliquent lorsque la BEI utilise ces informations dans le cadre d'enquêtes disciplinaires:

- cette utilisation doit être limitée aux finalités des procédures disciplinaires et des enquêtes en matière de fraude au sein de la BEI et la proportionnalité et la nécessité du traitement des informations doivent être respectées;

- la réutilisation de ces informations à d'autres finalités n'est permise que dans le cadre d'une procédure disciplinaire ouverte dans un dossier précis et ne doit pas servir d'opportunité pour obtenir des informations (tentative de découvrir les faits sur quelque chose en collectant un grand nombre d'informations, souvent sur des questions non liées, mineures ou en secret).

2.3.3.2. Communication électronique et contrôle électronique

Dans un certain nombre de dossiers, le CEPD a reçu des notifications ou a été consulté en matière de traitements relatifs à la communication électronique et au contrôle électronique.

Dans le cadre d'une consultation sur la supervision d'appels de données provenant du système de communication unifié (UniComm) au sein de l'Agence des droits fondamentaux de l'Union européenne (FRA), nous avons précisé le type de dossiers relatifs à des communications électroniques devant nous être notifié en vue du contrôle préalable. Dans sa réponse du 1er février 2013, le CEPD a établi le principe selon lequel les communications électroniques (et en particulier le traitement des enregistrements téléphoniques) sont soumises au contrôle préalable si l'une des trois conditions suivantes est remplie:

1. en cas de violation structurelle de la confidentialité de la communication, ou
2. si le traitement a trait à des soupçons d'infraction ou à des mesures de sûreté, ou
3. s'il vise à évaluer des aspects liés à la personnalité des individus.

Dans le dossier relatif à la FRA, il est apparu que les informations personnelles en question ne sont traitées que pour veiller au bon fonctionnement, à l'identification et au traitement des menaces pour la sécurité contre le système Unicomm. Parallèlement, le traitement ne semble pas violer la confidentialité des communications, dans la mesure où certaines informations relatives au trafic ne sont traitées que pour permettre aux individus d'identifier leurs appels privés, sans aucune interférence avec le contenu de leurs communications. Nous avons dès lors conclu que le traitement n'était pas soumis à un contrôle préalable.

Nous avons également analysé en détail un courriel contrôlant la politique mise en place au sein de l'Agence ferroviaire européenne (ERA), courriel qui a été rédigé pour contribuer à éviter les perturbations et les abus par les membres du personnel. Nous avons recommandé des modifications dans un certain nombre de domaines. Dans notre réponse à la notification en vue d'un contrôle préalable, nous avons souligné les principes essentiels suivants:

- tout contrôle des courriels doit être nécessaire et proportionné;
- il doit d'abord être effectué de manière automatisée et sur une base anonyme;
- les courriels individuels identifiant l'utilisateur ne doivent être examinés que s'il existe des soupçons raisonnables de méfaits, corroborés par des données initiales concrètes et dans le cadre d'une enquête administrative.

Nous avons entre autres invité l'ERA à exclure l'applicabilité de la politique relative aux courriels aux comptes de messagerie électronique personnels et à supprimer, ou à limiter considérablement, le pouvoir de l'ERA d'interférer avec les communications personnelles.

Un deuxième dossier concernant l'Agence ferroviaire européenne (ERA) avait trait au contrôle électronique en vue de vérifier si l'utilisation de l'internet est conforme à la politique interne consignée. Dans notre avis de contrôle préalable, nous avons appliqué l'orientation figurant dans nos avis antérieurs, et souligné les points suivants:

- le contrôle général de l'utilisation individuelle de l'internet en l'absence de soupçons est excessif;
- une stratégie devrait autoriser une augmentation graduelle du contrôle selon les circonstances et les besoins concrets;
- le contrôle de l'utilisation de l'internet par des individus identifiés ne devrait avoir lieu que s'il existe des soupçons raisonnables, corroborés par des preuves et dans le cadre d'une enquête administrative;
- avant de passer au contrôle individuel, d'autres mesures moins intrusives (comme des rappels ou des avertissements généraux) devraient être envisagées le cas échéant.

2.3.3.3. Transferts des données

La question du transfert des données à des destinataires internes et externes, par exemple, dans le cadre d'enquêtes en matière de sécurité et de fraudes et d'irrégularités financières dans la gestion

des fonds européens, était un sujet récurrent dans les dossiers traités en 2013.

Le 1er février 2013, nous avons publié notre premier avis de contrôle préalable concernant un traitement du service européen pour l'action extérieure (SEAE). Ce contrôle préalable concernait des enquêtes en matière de sécurité effectuées par la division «Sécurité et politique de sécurité» du SEAE. La notification originale du SEAE couvrait différentes mesures de sécurité, qui ont été précisées et dont la portée a été limitée au cours de l'examen.

Dans nos conclusions, nous avons recommandé de modifier la politique de sécurité proposée. Une autre recommandation formulée concernait les transferts des données – le SEAE étant un service extérieur, ces transferts peuvent inclure les transferts vers des pays tiers et des organisations internationales - et nous avons fait référence à notre document à venir sur les transferts des données.

Au sein du Centre commun de recherche (JRC) à Petten, une décision du comité de la sécurité définit les tâches générales du service chargé de la sécurité. À la lumière de sa révision et du futur protocole d'accord entre la direction générale «Ressources humaines et Sécurité» de la Commission européenne et le JRC en vue de mener certains types d'enquête en matière de sécurité, le JRC a notifié au CEPD des traitements effectués dans des enquêtes en matière de sécurité. La finalité de ce traitement est d'obtenir des informations sur des accidents liés à la sécurité comme des accidents de la circulation, des violations en matière de stationnement et des actes de vandalisme qui ont eu lieu sur le site du JRC de Petten, et qui ont donné lieu à un rapport décrivant les faits.

Les principales préoccupations que nous avons mises en avant dans notre avis du 19 mars 2013 concernaient le transfert de données à des destinataires comme les institutions et les organes de l'Union ou les autorités nationales (policières et judiciaires, par exemple) et l'utilisation que ces dernières pourraient en faire. Nous avons proposé qu'un avis sur la limitation de la finalité soit fourni à ces destinataires et que la nécessité d'un transfert potentiel d'informations soit dûment évalué et documenté avant tout transfert effectif.

La plate-forme de consultation des données d'enquête (plate-forme IDCP) est un projet de base de données visant à faciliter la coopération et l'échange d'informations sur les enquêtes anti-fraude entre l'OLAF et ses autorités partenaires au niveau international. Cette plate-forme contient un sous-ensemble de données provenant des dossiers d'enquête de l'OLAF et de ses partenaires internationaux sélectionnés (partenaires IDCP). La finalité de cet outil est de permettre aux utilisateurs de la plate-forme IDCP d'identifier et d'échanger des informations pertinentes relatives aux enquêtes. L'OLAF souhaite que cette plate-forme fonctionne avant tout comme un localisateur des informations de base liées aux enquêtes. En consultant le sous-ensemble de données conservées dans la plate-forme IDCP, le partenaire sera en mesure de déterminer si une autre autorité possède éventuellement des informations pertinentes pour son enquête et de soumettre une demande spécifique de coopération en vertu de l'accord de coopération administrative applicable.

L'OLAF a notifié la plate-forme IDCP au CEPD en mars 2012 en vue d'un contrôle préalable bien avant de finaliser sa mise en œuvre. L'analyse du traitement en vertu de l'article 27 ainsi que son développement ont eu lieu plus ou moins en parallèle.

Après une évaluation approfondie, nous avons conclu que le traitement proposé doit être soumis à un certain nombre de conditions et de limitations afin de respecter pleinement le règlement (CE) n° 45/2001 relatif à la protection des données. Nous avons notamment formulé les recommandations suivantes:

- préciser clairement les responsabilités de l'OLAF et des autres partenaires de la plate-forme IDCP en vue de respecter les exigences du règlement;
- limiter considérablement les conditions et les modalités de consultation de la base de données afin de respecter les principes de la nécessité et de la proportionnalité;
- assurer des révisions suffisamment fréquentes (au minimum annuelles) de l'exactitude, de l'exhaustivité et de la mise à jour des données à caractère personnel contenues dans la plate-forme IDCP;
- réaliser une analyse complète des risques et définir en détail les contrôles spécifiques en matière de sécurité devant être mis en œuvre afin de réduire les risques à un niveau acceptable pour la direction de l'OLAF.

En outre, nous avons exigé de l'OLAF qu'il demande une autorisation séparée aux fins de l'article 9, paragraphe 7, du règlement. Cette autorisation vise à véri-

fier que des garanties suffisantes en matière de respect de la vie privée et de protection des données sont en place.

2.3.3.4. Divers

L'objectif de la mise en œuvre par la Banque européenne d'investissement des contrôles visant la lutte contre le blanchiment des capitaux et le financement du terrorisme (LBC/FT) est d'appliquer les bonnes pratiques bancaires dans ces domaines et de réduire au maximum les risques pour l'intégrité et la réputation.

Dans notre avis de contrôle préalable, nous avons demandé instamment à la BEI de renforcer la base juridique existante. Nous avons également insisté sur la nécessité d'introduire un certain nombre de garanties en vue d'accroître la qualité des données à caractère personnel traitées. Les informations personnelles qui ne sont pas pertinentes à la vue de l'objectif ne devraient pas être traitées. Les rumeurs, les communiqués de presse et autres allégations non vérifiés devraient être traités prudemment. Enfin, la BEI devrait mettre en place des procédures pour veiller à ce que les informations utilisées soient précises et à jour.

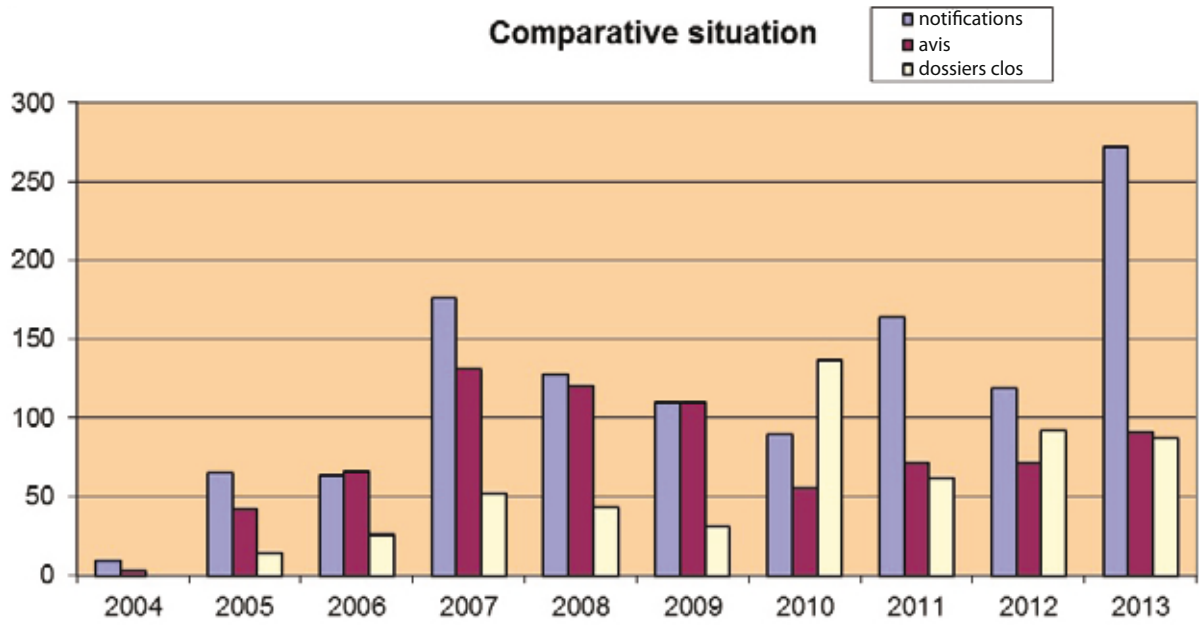
Le 8 mars 2013, l'entreprise commune Fusion for Energy (F4E) nous a notifié ses traitements concernant les déclarations d'intérêts des membres de son comité exécutif. Ces déclarations protègent l'indépendance de ses membres et évitent tout conflit d'intérêt qui pourrait interférer avec leurs activités. Ces déclarations d'intérêts peuvent être publiées sur demande. Dans notre avis du 30 mai 2013, nous avons indiqué que cette publication peut être justifiée pour permettre le contrôle par les pairs et par le grand public selon les tâches des membres du comité exécutif. Les institutions et les organes devraient évaluer le caractère potentiellement public des informations personnelles lorsqu'ils les collectent et devraient dûment informer les personnes concernées quant à leur éventuelle divulgation.

Nous avons également fait remarquer que la divulgation des déclarations d'intérêts est en effet un transfert de données. Comme indiqué dans le document du CEPD intitulé *Accès du public aux documents contenant des données à caractère personnel après l'arrêt rendu dans l'affaire Bavarian Lager*, une institution doit tenir compte des intérêts et points de vue légitimes des personnes concernées afin d'équilibrer les intérêts de toutes les personnes concernées et de rendre une décision bien documentée. Nous estimons que le consentement n'est pas nécessaire dans la mesure où l'équilibre des intérêts dans ce cas serait sinon dénué de substance. Néanmoins, les personnes ont le droit de s'opposer à la publication pour des raisons impérieuses et légitimes.

2.3.4. Notifications retirées ou non soumises au contrôle préalable

Il a été conclu que 41 dossiers ne devaient pas faire l'objet d'un contrôle préalable en 2013. Dans ces situations («traitements non soumis à un contrôle préalable»), le CEPD peut malgré tout faire des recommandations. Par ailleurs, deux notifications ont été retirées et une notification a été remplacée. L'augmentation significative du nombre de dossiers présentés de manière inappropriée (contre 8 en 2012) est une conséquence du délai fixé par le CEPD pour résorber l'arriéré de dossiers de contrôles préalables ex post (voir le paragraphe 2.3.2.1). La plupart des dossiers non soumis au contrôle préalable ont été introduits juste avant la date limite.

Il arrive parfois que nous devions demander au responsable du traitement de retirer une notification lorsque les informations soumises sont incomplètes, inexactes ou trompeuses. En 2013, deux notifications ont été retirées et remplacées à notre demande. La première notification n'était pas alignée sur les notifications de contrôle préalable relatives à des traitements similaires, la finalité du traitement n'était pas clairement décrite et aucune base juridique précise n'était mentionnée. En ce qui concerne la seconde notification, nous avons demandé au responsable du traitement de retirer la notification initiale de contrôle préalable parce que lors de la phase de développement, le projet notifié a été soumis à des modifications considérables par rapport à la description contenue dans la notification.



2.3.5. Suivi des avis de contrôle préalable

Le CEPD conclut généralement ses avis de contrôle préalable en indiquant que le traitement ne semble pas enfreindre les dispositions du règlement, à condition que certaines ***recommandations*** *soient prises en considération. Des recommandations sont également formulées lorsque le CEPD examine un dossier afin de vérifier la nécessité d'un contrôle préalable et lorsque certains aspects essentiels semblent nécessiter des rectifications. Une fois l'avis rendu, le CEPD accorde aux institutions concernées un délai de trois mois pour rendre compte de la mise en œuvre des recommandations contenues dans cet avis. Si le responsable du traitement ne respecte pas ces recommandations, le CEPD peut exercer les pouvoirs qui lui sont conférés en vertu de l'article 47 du règlement.*

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

Comme souligné dans le règlement intérieur (article 25, paragraphe 2), nous considérons ce suivi comme un élément fondamental du respect intégral du règlement. Conformément à notre document stratégique de 2010 intitulé *«Contrôler et garantir le respect du règlement (CE) n° 45/2001»*, nous attendons des institutions et des organes qu'ils se montrent responsables des recommandations éventuellement formulées. Cela signifie qu'ils sont chargés de les mettre en œuvre, et qu'ils doivent pouvoir nous en apporter la preuve. Toute institution ou tout organe qui ne donne pas suite à ces recommandations s'expose donc à une mesure formelle de mise en application.

2.3.6. Conclusions

Les 91 avis de contrôle préalable formulés ont jeté une lumière précieuse sur les traitements de l'administration européenne et nous ont permis de formuler des recommandations qui protègeront de manière uniforme le droit fondamental des personnes à la protection de leurs données à caractère personnel. L'importance de cette activité réside dans le fait qu'elle nous permet de vérifier la conformité avec les règles de protection des données avant la mise en place de l'activité de traitement.

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

Concernant le suivi de nos avis de contrôle préalable, 87 dossiers ont été clos en 2013. Nous continuerons de contrôler et de suivre de près nos recommandations afin de faire en sorte que les institutions et agences les intègrent en temps utile et de façon satisfaisante.

2.4. Réclamations

2.4.1. Le mandat du CEPD

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

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

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

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

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

Un ressortissant tchèque a déposé une réclamation relative aux procédures d'un tribunal national concernant la restitution de ses biens. Étant donné qu'aucun traitement de données à caractère personnel n'a été effectué par les institutions européennes, cette réclamation n'a pas été traitée.

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

Un ressortissant grec a déposé une réclamation auprès du CEPD expliquant qu'il s'était adressé à l'autorité grecque chargée de la protection des données (qui ne lui a pas répondu) afin de vérifier la conformité avec la législation grecque en matière de protection des données d'une décision prise par un organe du service public grec. Le plaignant a demandé au CEPD d'intervenir dans son dossier. Nous avons expliqué que le CEPD n'est pas compétent pour prendre des mesures contre les autorités nationales chargées de la protection des données, dans la mesure où ses compétences se limitent au traitement des données à caractère personnel par les institutions ou les organes de l'Union.

2.4.2. Procédure de traitement des réclamations

Le CEPD examine les réclamations en vertu du cadre juridique en vigueur, du règlement intérieur du CEPD, des principes généraux du droit de l'Union européenne et des bonnes pratiques administratives communes aux institutions et organes de l'UE.

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

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

En février 2011, nous avons actualisé la manière dont les réclamations peuvent nous être soumises et nous avons créé un **formulaire de réclamation en ligne** disponible en anglais, en français et en allemand sur notre site internet. Ce formulaire aide les plaignants à évaluer la recevabilité de leur réclamation, et donc à ne soumettre au CEPD que des cas

pertinents. Il nous permet également d'analyser des informations plus complètes afin d'accélérer le traitement des réclamations et de réduire le nombre des réclamations manifestement irrecevables.

En février 2011, nous avons actualisé la manière dont les réclamations peuvent nous être soumises et nous avons créé un formulaire de réclamation en ligne disponible en anglais, en français et en allemand sur notre site internet. Ce formulaire aide les plaignants à évaluer la recevabilité de leur réclamation, et donc à ne soumettre au CEPD que des cas pertinents. Il nous permet également d'analyser des informations plus complètes afin d'accélérer le traitement des réclamations et de réduire le nombre des réclamations manifestement irrecevables.

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

Notre **manuel interne** a été conçu pour mettre des orientations en matière de traitement des réclamations à la disposition de notre personnel. Nous avons également mis en place un outil **statistique** conçu pour examiner les activités liées aux réclamations, et en particulier pour suivre l'évolution de certains dossiers.

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

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

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

Dans le cadre d'une réclamation concernant une enquête administrative contre un membre du personnel, le plaignant a lancé une procédure en vertu de l'article 91 du statut des fonctionnaires après avoir déposé une réclamation auprès du CEPD.

Le CEPD a par conséquent décidé de suspendre cette réclamation.

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

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

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

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

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

Aucune décision du CEPD n'a fait l'objet d'une contestation devant la Cour en 2013.

2.4.3. Confidentialité garantie aux plaignants

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

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

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

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

Au cours et au terme d'une enquête, nous ne divulguons à des tiers aucun **document relatif à la réclamation**, en ce compris la décision finale, sauf si une obligation légale nous l'impose.

2.4.4. Réclamations traitées en 2013

2.4.4.1. Nombre des réclamations

Le CEPD a reçu 78 réclamations en 2013, soit une diminution d'environ 9 % par rapport à 2012, ce qui confirme l'efficacité du formulaire de dépôt de réclamation en ligne pour réduire le nombre des réclamations irrecevables. Sur ce total, 48 réclamations ont été jugées irrecevables, la majorité portant sur un traitement au niveau national, et non au niveau d'une institution ou d'un organe de l'Union européenne.

Les 30 réclamations restantes ont nécessité une enquête approfondie, ce qui a représenté une diminution de 25 % par rapport à 2012. De plus, 20 réclamations recevables déposées les années précédentes (deux en 2009, une en 2010, quatre en 2011 et 13 en 2012) en étaient toujours à la phase de l'enquête, de l'examen ou du suivi au 31 décembre 2013.

2.4.4.2. Nature des plaignants

Sur les 78 réclamations reçues, 23 (29 %) 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 55 autres réclamations, le plaignant ne semblait pas avoir de lien professionnel avec l'administration de l'UE.

2.4.4.3. Institutions et nombre de réclamations

Sur les 30 réclamations recevables déposées en 2013, la plupart étaient dirigées contre la Commission européenne, l'OLAF et le Parlement européen. Cette situation est prévisible dans la mesure où la Commission et le Parlement traitent plus d'informations personnelles que les autres institutions et organes de l'UE. Le nombre relativement élevé de réclamations contre l'OLAF peut s'expliquer par la nature des activités exercées par cet organe. Cependant, un nombre considérable de réclamations était aussi dirigé contre l'Agence des droits fondamentaux.

2.4.4 .4. Langue des réclamations

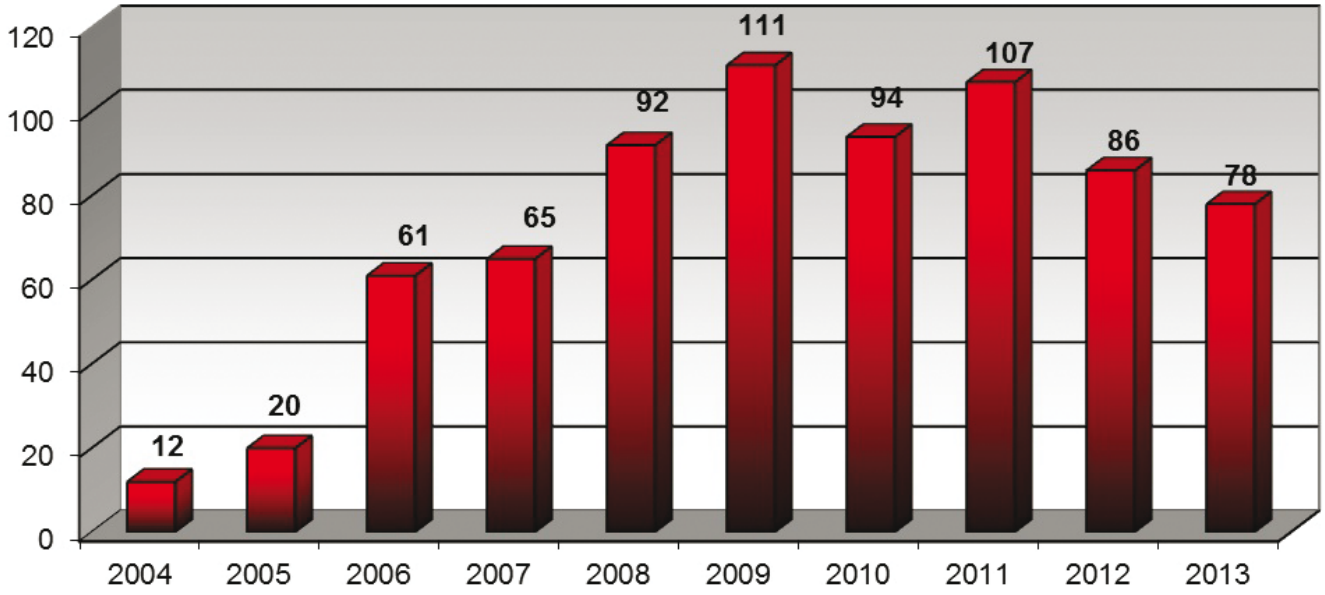
La majorité des réclamations ont été déposées en anglais (50 %), en allemand (17 %), en français (15 %) et en italien (8 %). Les réclamations dans d'autres langues sont relativement rares (10 %).

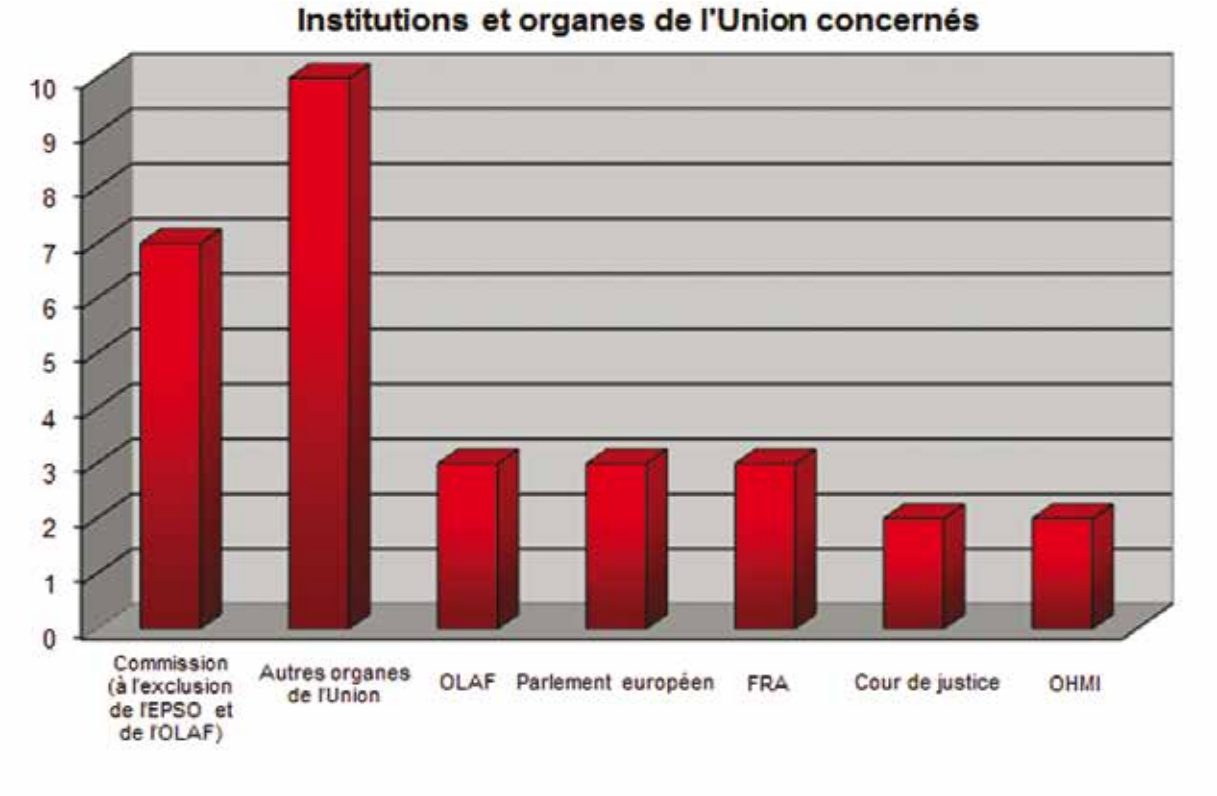
2.4.4.5. Types de violations invoqués

Les violations des règles en matière de protection des données alléguées par les plaignants en 2013 concernaient principalement:

- la divulgation des données (47 %), une atteinte aux droits des personnes concernées, comme une collecte excessive d'informations personnelles (13 %), des transferts de données (10 %), la qualité des données et l'information des personnes concernées (10 %);

Nombre de réclamations reçues





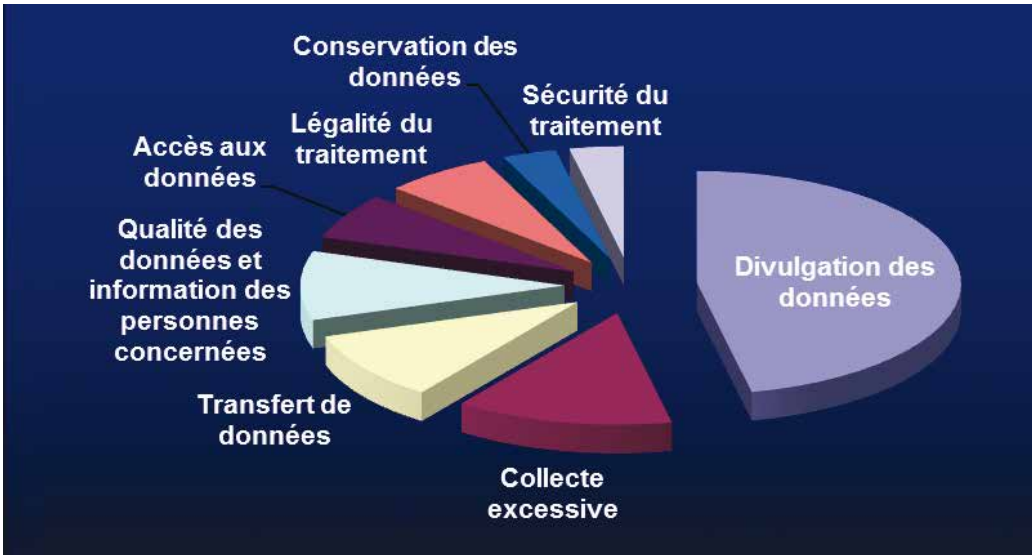
- l'accès aux données (7 %), la légalité du traitement (3 %) et la conservation des données (3 %).

2.4.4.6. Résultats des enquêtes du CEPD

Dans quatre affaires résolues en 2013, 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.

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

Le CEPD a reçu une réclamation quant à l'accès aux données à caractère personnel d'une personne qui avait depuis quitté l'institution et quant à la conservation de ces données dans une base de données pendant une période plus longue que nécessaire par rapport aux finalités pour lesquelles elles ont été collectées. Le CEPD a considéré que l'institution n'avait pas respecté le règlement car elle n'avait pas adopté de mesures techniques et organisationnelles adéquates pour faire en sorte qu'il soit impossible d'accéder illégalement aux informations personnelles du plaignant et car elle n'avait pas supprimé les données après une certaine période.



Dans deux affaires, les allégations communiquées au CEPD dans le contexte d'une réclamation ont entraîné une décision par celui-ci de lancer une mission d'information plus étendue dans les locaux de l'institution européenne concernée.

2.5. Contrôle du respect du règlement

Le CEPD est chargé d'assurer le suivi et de veiller à l'application du règlement (CE) n° 45/2001. Le contrôle prend la forme d'enquêtes générales périodiques. En plus de cet état des lieux général, nous avons également effectué des contrôles ciblés dans les cas où, à la suite de nos activités de supervision, nous avions des raisons de nous inquiéter du degré de conformité aux normes de certaines institutions ou certains organes. En 2013, ces contrôles ont pris la forme d'une visite d'une journée de l'organe concerné aux fins de remédier aux défauts de conformité. En outre, des inspections ont été ménées dans certaines institutions et certains organes pour vérifier leur respect du règlement concernant des questions spécifiques.

2.5.1. Exercice général de contrôle et de compte rendu Enquête 2013: enquête sur le rôle de coordinateur de la protection des données à la Commission européenne et compte rendu général

Au cours de ces dernières années, certaines des institutions les plus grandes ont mis en place des réseaux de coordinateurs de la protection des données (CPD) pour qu'ils agissent en tant que relais pour le délégué à la protection des données au niveau local. La Commission européenne a lancé son réseau en 2002 et toutes les DG y participent en principe désormais.

En juin 2012, nous avons lancé une enquête sur la fonction de CPD à la Commission européenne. Les résultats ont été publiés dans un rapport en janvier 2013.

Les résultats révèlent des disparités importantes au niveau des ressources allouées à la fonction par les directions générales: les CPD consacrent entre 5 % et 100 % de leur temps à leur fonction de CPD. Cependant, tous les CPD doivent réaliser une série de tâches de base communes indépendamment du temps disponible pour ce faire. Dès lors, l'une des principales conclusions à laquelle aboutit notre rapport est que, pour préserver l'utilité de cette fonction, il est nécessaire d'établir des critères minimaux devant être remplis par les directions générales.

Nos conclusions mentionnent aussi entre autres:

- que la décision de nomination devrait mentionner la durée minimale du mandat;
- qu'une référence spécifique au rôle du CPD devrait être insérée dans la description de la fonction;
- que les ressources nécessaires devraient être garanties, comme du temps pour participer aux réunions du réseau des CPD, et
- que les responsabilités du CPD devraient être insérées dans l'évaluation individuelle.

Le rapport souligne en outre les bonnes pratiques appliquées par certaines DG, telles que la création d'une messagerie fonctionnelle qui peut être utilisée pour consulter le CPD, la conception d'une page intranet consacrée à la protection des données, la visibilité dans l'organigramme du rôle du CPD, la structuration de l'accès par le CPD à ses supérieurs et l'accès effectif à l'information dont il a besoin.

Le rapport nous a permis de manifester notre soutien à la fonction de CPD, dans la mesure où elle participe à la bonne gouvernance. Les CPD, dont la fonction est reconnue en interne, contribuent à responsabiliser davantage les DG en matière de protection des données; il s'agit d'un concept essentiel dans le cadre de la réforme en cours de la protection des données.

Le 17 juin 2013, nous avons lancé notre quatrième état des lieux général («Enquête 2013»), afin de déterminer les progrès accomplis dans la mise en œuvre du règlement dans l'ensemble des 62 institutions et organes. Outre les questions examinées dans le cadre des enquêtes précédentes (nombre de notifications au DPD, nombre de contrôles préalables, etc.), nous avons demandé des renseignements sur:

- les formations proposées au personnel en matière de protection des données;
- les clauses contractuelles applicables aux sous-traitants;
- la participation du DPD à la conception de nouvelles opérations de traitement; et
- les transferts de données à des destinataires non soumis aux dispositions nationales d'exécution de la directive 95/46/CE.

Des enquêtes générales nous permettent de déterminer les organes dont les performances sont insuffisantes et de prendre des mesures spécifiques pour résoudre les problèmes. Les résultats de l'enquête seront publiés début 2014.

2.5.2. Visites

Le CEPD promeut le concept de responsabilisation, mais prend également des mesures si nécessaire. Les visites sont un moyen typique pour nous de prendre des mesures ciblées. Les visites sont un outil de conformité, dont l'objectif est d'obtenir l'engagement de la haute hiérarchie d'une institution ou agence de respecter le règlement.

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

Ces visites ont pour résultat:

- de sensibiliser à la protection des données;
- de renforcer le respect du règlement par un engagement de la hiérarchie;
- d'accroître notre connaissance des agences; et
- de façon générale, de favoriser une meilleure coopération avec les agences visitées.

En 2013, nous avons rendu visite à deux agences de l'Union européenne, l'AEMF et l'EIGE. Une réunion de travail a eu lieu avec eu-LISA.

AEMF

L'Autorité européenne des marchés financiers (AEMF) est devenue opérationnelle à Paris, le 1er janvier 2011. Bien que nous ayons été consultés sur les dispositions d'application relatives à la fonction du DPD, un DPD n'a été désigné qu'au printemps 2013 et aucune notification de contrôle préalable ne nous a été soumise avant cette désignation. Afin d'améliorer la protection des données au sein de l'AEMF, une réunion a eu lieu à Bruxelles en avril 2013 entre le contrôleur adjoint et le directeur exécutif de l'AEMF ainsi que le DPD nouvellement désigné. À la suite de cette réunion, l'AEMF a considérablement accru ses efforts en matière de respect du règlement et ses performances sont maintenant d'un niveau similaire à celui des performances des autres agences nouvellement créées.

EIGE

L'Institut européen pour l'égalité entre les hommes et les femmes (EIGE), situé à Vilnius, est devenu officiellement opérationnel à l'été 2010. L'EIGE a répondu tardivement à notre enquête générale de 2011 et, début 2013, il n'avait présenté aucune notification de contrôle préalable. C'est la raison pour laquelle le contrôleur adjoint a rendu visite à l'EIGE en mai 2013. Au cours de cette visite d'une demi-journée, des réunions ont eu lieu avec la direction, avec le personnel responsable des traitements ainsi qu'avec le DPD et le DPD adjoint. Après cette visite, l'EIGE et le CEPD se sont mis d'accord sur une feuille de route en vue d'atteindre un niveau de respect total. À ce jour, l'EIGE respecte les étapes de la feuille de route et ses performances sont maintenant meilleures que celles de beaucoup d'autres agences nouvellement créées.

eu-LISA

L'agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle (eu-LISA) est actuellement responsable de la gestion opérationnelle d'EURODAC, du VIS et du SIS II et est devenue opérationnelle en décembre 2012. Alors que son siège se trouve à Tallinn, le personnel technique et le centre de données principal sont basés à Strasbourg. En mai 2013, les membres du personnel du CEPD se sont rendus dans les locaux de l'agence à Strasbourg pour une visite de travail afin d'avoir un aperçu des activités, de collecter des informations sur les mesures de sûreté et de recevoir les informations les plus récentes sur l'évolution de la situation en ce qui concerne la migration vers la nouvelle version du système d'information Schengen. Il ne s'agissait pas d'une visite de niveau 'direction' axée sur des questions de conformité, mais d'une réunion de travail visant à favoriser la bonne coopération et des idées techniques au sein de cette nouvelle agence de l'Union.

Nous avons continué le suivi en ce qui concerne les visites précédentes et la mise en œuvre des feuilles de route. L'ETF, en particulier, a fait preuve d'une collaboration active en adoptant des mesures concrètes pour mettre en œuvre nos recommandations figurant dans la feuille de route.

2.5.3. Inspections

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

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

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

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

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

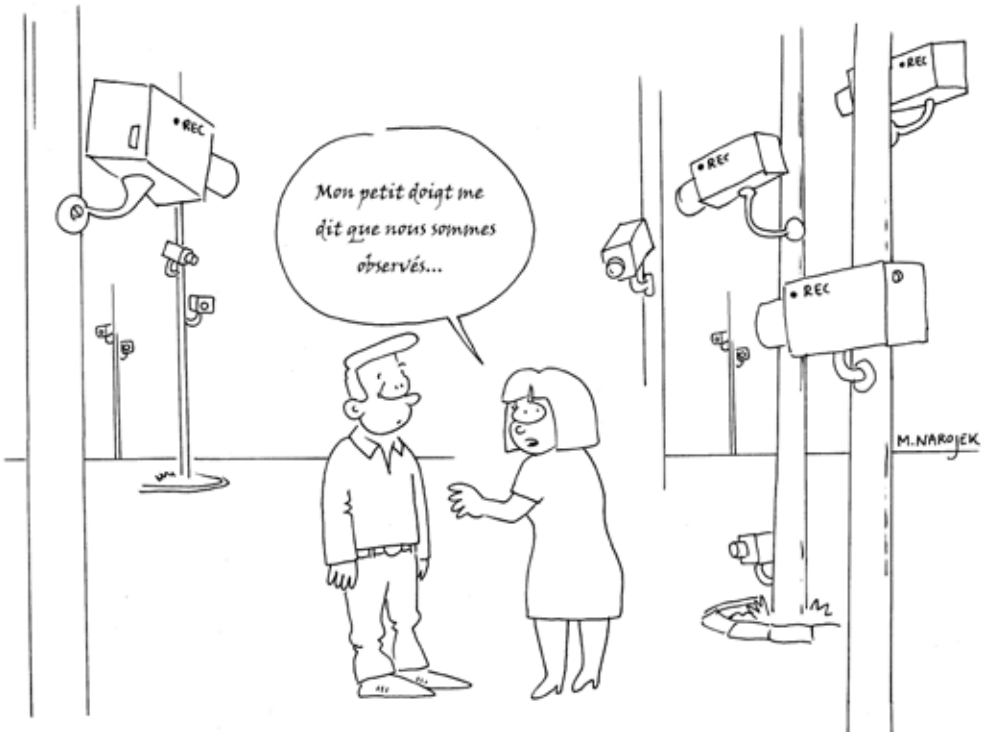
En novembre 2013, le CEPD a adopté un manuel d'inspection complet afin de fournir des orientations aux membres du personnel du CEPD chargés d'effectuer les inspections. Ce document contient une description de la procédure administrative, les fonctions des inspecteurs et la politique de sécurité en matière d'inspection, ainsi que des formulaires types pour la production de documents d'inspection. Ce manuel est complété par une politique d'inspection et par des lignes directrices en la matière. La politique d'inspection définit les éléments principaux de la procédure d'inspection du CEPD en vue de fournir des orientations à l'ensemble des acteurs concernés et de garantir la transparence vis-à-vis des parties prenantes. Les lignes directrices en matière d'inspection, qui sont transmises à l'institution concernée avant toute inspection, constituent un lien entre la politique et le manuel et elles exposent brièvement tant des questions opérationnelles que des questions juridiques.

En 2013, nous avons procédé au suivi des inspections antérieures. Nous avons inspecté l'EMA en juin 2013 et effectué des inspections ciblées sur place en juillet auprès de quatre institutions et organes basés à Luxembourg. Ces inspections ont porté sur la façon dont ces institutions et organes informent le grand public de la vidéosurveillance dans leurs locaux. Nous avons également effectué une inspection portant sur l'OLAF-SID-MAB-FIDE ainsi que deux visites d'information.

Inspection de l'EMA

En juin 2013, nous avons effectué une inspection auprès de l'Agence européenne des médicaments (EMA) située à Londres. Cette inspection était axée sur deux traitements: EudraVigilance, l'un des systèmes de l'activité principale de l'EMA et la vidéosurveillance sur le site de l'EMA. EudraVigilance a été sélectionné pour deux raisons: premièrement, parce que cette base de données est susceptible de contenir de grandes quantités de données médicales sensibles, et, deuxièmement, en vue d'accélérer le suivi d'un contrôle préalable émis.

EudraVigilance stocke des informations sur les réactions négatives aux médicaments, tant ceux autorisés au sein de l'Union que ceux utilisés dans le cadre d'essais cliniques. Cette base de données vise à découvrir de nouveaux effets secondaires et d'autres risques pour la sécurité liés aux médicaments. Elle contient actuellement plus de quatre millions de dossiers. L'inspection a permis de vérifier des faits et des pratiques liés à EudraVigilance.



En ce qui concerne la vidéosurveillance, l'inspection visait à vérifier le respect des lignes directrices du CEPD en la matière. Elle était similaire à l'inspection ciblée de la vidéosurveillance menée à Bruxelles en 2012, et a également pris en considération la forte dépendance dans l'État membre d'accueil vis-à-vis de la vidéosurveillance.

L'EMA a collaboré pleinement et de manière constructive avec notre équipe d'inspection. À l'heure de rédiger le présent rapport annuel, le rapport d'inspection était en cours de finalisation.

Inspection ciblée de la vidéosurveillance

En février 2012, à la suite de nos lignes directrices de 2010 en matière de vidéosurveillance, nous avons publié un rapport de suivi qui soulignait le niveau de respect par les institutions et organes de l'Union des recommandations du CEPD. Ce rapport annonçait plusieurs mesures de suivi sur le sujet, y compris des projets en vue de réaliser un certain nombre d'inspections thématiques.

Après avoir effectué des inspections auprès de 13 institutions et organes de l'Union basés à Bruxelles en juin et juillet 2012, le CEPD a réalisé un exercice similaire auprès de quatre institutions et organes de l'Union basés à Luxembourg les 9 et 10 juillet 2013.

Comme pour l'exercice précédent en 2012, nos inspections étaient axées sur la manière dont les institutions et organes de l'Union basés à Luxembourg informent le public de la vidéosurveillance, y compris en ce qui concerne:

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

Les résultats des inspections auprès des institutions et organes de l'Union sont actuellement en cours d'examen.

Inspection OLAF-SID-MAB-FIDE

En décembre 2013, nous avons effectué une inspection auprès de l'Office européen de lutte antifraude (OLAF) à Bruxelles, et ciblé plusieurs parties du système d'information antifraude (AFIS), à savoir le système d'information douanier (SID), le courtier d'assistance mutuelle (MAB) et le fichier d'identification des données d'enquête (FIDE). Nous avons également analysé le cadre de sécurité de l'AFIS.

Ces systèmes encouragent la coopération entre les autorités douanières des États membres et entre ces dernières et l'OLAF. Le MAB et le SID contiennent des informations sur les saisies de biens de contre-

bande et sur les soupçons en matière de contrebande et d'autres violations de la législation douanière et agricole. Le FIDE est un index des personnes et des entités faisant l'objet d'une enquête et de celles qui ont été reconnues coupables d'infractions en matière douanière.

Le procès-verbal et le rapport de l'inspection sont en cours de préparation.

Visites d'information

En janvier et en mai 2013, nous avons également mené deux visites d'information auprès de l'OLAF dans le cadre de deux dossiers de réclamation différents.

2.6. Consultations relatives aux mesures administratives

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

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

L'article 28, paragraphe 1, du règlement prévoit que les institutions et organes de l'Union européenne doivent informer le CEPD des mesures administratives relatives au traitement des données à caractère personnel. En outre, l'article 46, point d), du règlement impose au CEPD de conseiller l'ensemble des institutions et organes communautaires, soit de sa propre initiative, soit en réponse à une consultation pour toutes les questions concernant le traitement d'informations personnelles.

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

Comme indiqué dans le document stratégique, nous encourageons les responsables du traitement à nous consulter dans les cas particuliers et limités où ce traitement: a) présente un caractère nouveau ou une certaine complexité (en cas de doute véritable dans le chef du DPD ou de l'institution) ou b) a une incidence manifeste sur les droits des personnes concernées (que ce soit en raison des risques entraînés par les activités de traitement, du fait de la portée d'une mesure, etc.).

En principe, le CEPD examinera uniquement les consultations qui ont été soumises préalablement au DPD de l'institution concernée (article 24, paragraphe 3, du règlement intérieur). En 2013, nous avons reçu 37 consultations sur des mesures administratives. Dans le cadre des consultations menées sur des mesures administratives envisagées par une institution ou un organe, plusieurs questions ont été examinées en 2013. Les sous-points suivants rendent compte de certains de ces dossiers.

2.6.1.1. Transfert de données des membres du personnel aux Représentations Permanentes des États membres

Le DPD d'une agence de l'Union a consulté le CEPD sur le transfert de données à caractère personnel des membres du personnel aux Représentations permanentes des États membres. La responsabilité principale des Représentations permanentes est de

préparer collectivement les travaux du Conseil de l'Union européenne dans le cadre du COREPER.

Dans notre réponse du 9 avril 2013, nous avons indiqué que ces demandes doivent toujours préciser une finalité et reposer sur une base juridique claire, comme par exemple l'article 15, deuxième alinéa, du protocole n° 7 du traité sur le fonctionnement de l'Union européenne (TFEU) sur les privilèges et immunités de l'Union européenne, qui prévoit que les noms, qualités et adresses des fonctionnaires et autres agents compris dans certaines catégories sont «communiqués périodiquement aux gouvernements des États membres».

2.6.1.2. Changement de finalité de l'utilisation de données collectées à une fin spécifique

Le 17 avril 2013, nous avons répondu à une consultation émanant d'un organe de l'Union qui s'interrogeait sur le caractère légal de l'utilisation d'informations personnelles collectées à partir d'un système de sécurité de l'accès ou d'un système de gestion du temps à d'autres fins, plus précisément afin d'instruire une procédure disciplinaire dans le cadre d'une enquête.

Dans notre réponse, nous avons effectué une analyse sur la base du principe de limitation de la finalité (article 4) et du changement de finalité (article 6).

Nous avons conclu que les règles régissant les procédures disciplinaires et les enquêtes en matière de fraude permettent l'utilisation de tout type pertinent de données dans le cadre d'enquêtes disciplinaires. En outre, nous avons considéré que le traitement de données provenant d'un système de sécurité de l'accès ou d'un système de gestion du temps peut être considéré compatible dans le cadre de procédures disciplinaires.

L'autorisation doit toutefois être strictement interprétée afin que la proportionnalité et la nécessité du traitement soient respectées et que la réutilisation à d'autres finalités ne soit permise que dans le contexte spécifique d'une procédure disciplinaire ouverte dans un dossier précis. Des questions similaires ont été traitées dans le contexte des contrôles préalables (voir section 2.3.3.1).

2.6.1.3. Demande d'accès du public présentée à la BCE - équilibrer les intérêts des membres du personnel et du public

EUROPEAN CENTRAL BANK

Le 20 septembre 2013, nous avons répondu à une consultation de la Banque centrale européenne (BCE) quant à l'accès du public à un registre établi dans le cadre des règles de la BCE en matière d'éthique et relatives aux dons reçus par les membres du personnel de la BCE.

En tenant compte de la décision de la BCE sur l'accès du public et les faits de l'espèce, notre analyse s'est fondée sur l'arrêt «Bavarian Lager» de la CJUE et le document du CEPD intitulé *«Accès du*

public aux documents contenant des données à caractère personnel après l'arrêt rendu dans l'affaire Bavarian Lager». Nous avons considéré que cette demande d'accès public était un transfert devant respecter le règlement (CE) n° 45/2001. La BCE doit équilibrer les intérêts du destinataire pour établir la nécessité du transfert d'informations ainsi que les intérêts de l'institution pour établir s'il existe des raisons de penser que le fait d'autoriser l'accès aux informations personnelles d'un individu pourrait porter préjudice aux intérêts légitimes de ce dernier.

La mise en équilibre des intérêts doit aussi tenir compte des catégories des membres du personnel concernés dans la mesure où des exigences en matière de transparence pourraient justifier la publication de données à caractère personnel de membres du bureau exécutif ou de cadres supérieurs.

Nous avons conclu que la BCE doit évaluer l'éventuelle nature publique du don enregistré et indiquer précisément aux personnes mentionnées dans le registre dans quelle mesure le traitement pourrait être divulgué publiquement. Par conséquent, une personne doit être informée avant que ses données à caractère personnel ne soient divulguées pour la première fois et elle doit avoir le droit de s'opposer à la divulgation pour des raisons impérieuses et légitimes en vertu du règlement sur la protection des données.

2.7. Orientations en matière de protection des données

L'expérience acquise grâce à l'application du règlement relatif à la protection des données a permis à notre personnel de traduire son expertise en une orientation spécifique pour les institutions et organes. En 2013, ce travail d'orientation a pris la forme d'orientations dans le domaine des marchés publics, des subventions et des experts externes ainsi que d'un suivi d'orientations antérieures en matière de congé et d'horaire flexible, de formations pour les DPD, d'un atelier pour les responsables du traitement et les DPD, d'un espace réservé aux DPD sur le site internet du CEPD et d'une ligne d'assistance pour les DPD.

2.7.1. Lignes directrices thématiques

Dans l'esprit du plan d'action établi dans la révision stratégique 2013-2014, et à la suite de demandes émanant de parties prenantes en faveur de plus d'orientations en matière de protection des données, nous avons continué à concevoir des lignes directrices thématiques. Ces lignes directrices ne couvrent pas uniquement des domaines soumis au contrôle préalable du CEPD, mais aussi des thèmes horizontaux.

Là où nos lignes directrices couvrent des domaines soumis au contrôle préalable du CEPD, elles ont contribué à réduire ce travail et nous ont permis d'axer nos avis sur les traitements qui divergent des lignes directrices.

- Lignes directrices concernant les marchés publics, les subventions et les experts externes

En juin 2013, nous avons publié des lignes directrices sur le traitement des informations à caractère personnel dans le contexte des marchés publics, des subventions, ainsi que de la sélection et l'utilisation d'experts externes. Toutes ces procédures sont fondées sur le règlement financier de l'Union et englobent l'évaluation des candidats respectifs sur la base du même ensemble de critères. Le point principal abordé dans les lignes directrices était la conservation des données à caractère personnel dans ce contexte. Nous avons souligné les dispositions respectives des règles d'application du règlement financier de l'Union, autorisant la conservation des données à des fins de contrôle et d'audit pendant sept ans maximum après la signature du contrat ou de l'accord concerné.

- Enquête sur la conservation des données dans un contexte d'évaluation

Afin d'assurer le suivi des lignes directrices de 2011 relatives à l'évaluation du personnel, nous avons réalisé en juin 2013 une enquête sur la conservation des informations à caractère personnel dans le cadre d'une évaluation. Un questionnaire a été transmis aux participants à notre atelier de 2012 sur la conservation des données pour recueillir, auprès d'experts en ressources humaines et de responsables de la gestion documentaire, des informations sur les raisons justifiant les délais en vigueur et sur le stockage sur fichiers électroniques.

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

Fin 2012, nous avons fourni des orientations aux institutions et agences de l'Union européenne avec l'adoption des lignes directrices concernant le traitement de données à caractère personnel en matière de congé et d'horaire flexible. Ces lignes directrices ont pour objectif de proposer des conseils pratiques et une assistance à tous les

DPD et responsables du traitement dans leur mission de notification au CEPD des traitements de données existants et/ou futurs dans ce domaine.

En 2013, le CEPD a reçu de nombreuses notifications de contrôle préalable soumises par des institutions et organes de l'Union européenne au sujet de ces lignes directrices. Ces notifications nous ont permis d'analyser avec plus de précision la mise en œuvre des lignes directrices. Plutôt que d'adopter un avis général couvrant l'ensemble des notifications reçues, nous avons adopté des avis spécifiques pour chaque agence, portant sur les opérations de traitement en matière de congé et d'horaire flexible en général, et nous avons concentré notre analyse sur les divergences observées entre les opérations de traitement et les lignes directrices.

2.7.2. Formations et ateliers

Le 31 janvier 2013, une formation spéciale a été organisée pour les DPD de cinq entreprises communes de l'Union: ARTEMIS, Clean-Sky, ENIAC, IMI & SESAR. Ces exposés étaient axés sur le rôle et les missions du DPD, les lignes directrices disponibles sur le site internet du CEPD (en particulier, le coin de DPD), les outils du CEPD en matière de contrôle du respect et les pouvoirs d'exécution du CEPD.

Le 25 février 2013, à la suite d'une demande spécifique émanant de la Fondation européenne pour la formation (ETF), le CEPD a organisé une session de formation thématique pour les membres du personnel de cette Agence chargés des ressources

humaines, des technologies de l'information et des marchés publics. La plupart des participants ont confirmé qu'ils avaient acquis de nouvelles connaissances quant à la mise en œuvre concrète des lignes directrices du CEPD dans ces domaines et que cette formation avait permis un échange de vues utile avec le personnel du CEPD. Il est intéressant de noter que certains participants ont cité l'importance du processus de notification préalable, que le contrôle préalable est une opportunité et qu'ils devraient chercher des lignes directrices et des avis

sur le site internet du CEPD lorsqu'ils rédigent des politiques et procédures.

Le 10 avril 2013, nous avons organisé une session de formation à la demande du DPD de l'Agence européenne de défense (AED) pour plusieurs responsables du traitement de cette agence. Le personnel du CEPD a axé son exposé sur l'importance de soumettre des notifications au DPD, sur la manière dont les responsables du traitement doivent remplir les notifications et il a fourni des exemples concrets relatifs aux droits des personnes concernées. Cette formation s'est avérée utile car elle a sensibilité les responsables du traitement et les a motivé à soumettre leurs notifications au DPD de l'Agence, qui les envoie ensuite au CEPD en vue d'un contrôle préalable.

Le 17 avril 2013, nous avons organisé une formation générale pour les DPD des institutions et organes de l'Union. Cette formation était axée sur la procédure de contrôle préalable. Les exposés ont porté sur les responsabilités du DPD dans ce domaine, les étapes de la procédure de contrôle préalable, les délais applicables ainsi que les orientations disponibles sur le site du CEPD. Cette formation contenait un exercice de groupe visant à remplir un véritable formulaire de notification en vue du contrôle préalable.

Nous avons également lancé une série d'ateliers qui nous permettront de publier des orientations sur des sujets liés à la technologie. Les discussions lors de ces ateliers confirment la nécessité d'une approche commune pour protéger les informations personnelles et soulignent les avantages de l'échange entre les institutions et organes de l'Union des expériences relatives aux bonnes pratiques en matière de protection des données, en particulier dans ces domaines technologiques qui sont complexes et évoluent rapidement.

Le premier atelier de cette série a eu lieu le 12 juin 2013; il portait sur les communications électroniques sur le lieu de travail. 75 participants, y compris des DPD, des CPD et du personnel des domaines des technologies de l'information et des ressources humaines, représentaient la majorité des institutions et organes de l'Union. Ils ont apporté des contributions précieuses se fondant sur leur travail quotidien dans le domaine de l'utilisation des téléphones, de l'internet et du courrier électronique. D'autres réunions et contacts par courriels avec les réseaux des DPD/CPD, le personnel de l'administration européenne responsable des technologies de l'information, des ressources humaines et d'autres domaines contribueront à rassembler d'autres informations pertinentes afin de rédiger des orientations en la matière.

Le 19 septembre 2013, nous avons organisé deux ateliers sur l'utilisation des dispositifs mobiles sur le lieu de travail et sur les sites internet gérés par les institutions et organes de l'Union. Plus de 60 participants ont participé à chaque atelier. Avant cette réunion, nous avons demandé aux personnes s'étant inscrites à l'atelier de participer à notre enquête portant sur leurs propres pratiques. Cette enquête nous a éclairés de manière unique et précieuse sur l'expérience et les points de vue qui ont ensuite été abordés lors du débat, y compris l'utilisation des cookies sur les sites internet et des dispositifs mobiles privés sur le lieu de travail.

Atelier relatif aux transferts

Un atelier sur les flux de données transfrontaliers a été organisé pour les DPD le 22 novembre 2013. L'objectif de cet atelier était double: d'une part, aborder les principaux éléments du régime juridique tel qu'établi à l'article 9 du règlement (CE) n° 45/2001 et, d'autre part, faire fonction de forum au sein duquel discuter de l'expérience des DPD en la matière: dossiers, besoins et problèmes rencontrés. Cet événement a commencé par une présentation qui a abordé la notion de transferts, la portée de l'article 9, le principe de la protection adéquate, les dérogations, les mesures de protection adéquates, la législation et les accords bilatéraux et la supervision et la mise en application dans le domaine des transferts. Un grand nombre de personnes a participé à cet atelier et un échange productif d'idées a eu lieu.

2.7.3. Coin des DPD et autres outils

Le «Coin des DPD» du site internet du CEPD est une rubrique restreinte réservée aux DPD des institutions et organes de l'Union européenne. Le «Coin des DPD» contient des informations utiles et des outils pratiques pour aider les DPD dans leur travail ainsi que des documents sur le rôle et la mission des DPD, des modèles et présentations pour aider les DPD dans leurs activités de sensibilisation, des résumés des évolutions récentes dans le domaine de la protection des données, et une liste d'événements (formations ou réunions). Ces informations sont mises à jour régulièrement.

Nous avons également créé une ligne d'assistance téléphonique pour répondre aux questions de base des DPD ou pour les réorienter vers un responsable de dossier qui pourra répondre à leurs questions concernant un thème ou un dossier particulier (voir le point 2.2 concernant les délégués à la protection des données)[6].

6 Nous recevons habituellement plus ou moins dix questions de ce type par mois.

3 CONSULTATION

Notre objectif stratégique

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

Nos principes directeurs

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

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

L'année 2013 a elle aussi été marquée par des évolutions majeures dans le domaine de la protection des données, dont deux ont eu des incidences significatives sur nos activités.

Le débat suscité par les révélations d'Edward Snowden a mis en évidence les méthodes de surveillance de masse dans l'Union et aux États-Unis. Ces révélations ont grandement contribué à sensibiliser l'opinion publique aux questions liées à la vie privée et à la protection des données et elles nous ont permis de conseiller le législateur de l'Union et d'autres parties intéressées. Dans son discours, prononcé lors de l'audition publique organisée en octobre 2013 par la commission des libertés civiles (LIBE) du Parlement européen et qui portait sur la surveillance électronique de masse des citoyens européens, le CEPD a insisté sur le fait qu'il est temps de reprendre le contrôle de notre vie privée au sein de l'Union. En novembre 2013, la Commission a consulté le CEPD sur sa communication «Restaurer la confiance dans les flux de données entre l'Union européenne et les États-Unis». Nous avons déjà fourni des observations informelles, mais nous présenterons un avis officiel sur le sujet au début de l'année 2014.

La réforme des règles en vigueur en matière de protection des données dans l'Union a été l'autre thème dominant de l'année. Ce projet a constitué l'une de nos priorités en 2013 et il le restera à mesure que la procédure législative se poursuit. Les débats en cours au Parlement européen et au Conseil ont suscité un intérêt considérable de la part du secteur public et du secteur privé, à l'intérieur comme à l'extérieur de l'UE. Ce processus a également démontré une compréhension fondamentale des principes sous-jacents de la réforme par les institutions de l'Union européenne. Le 15 mars 2013, nous avons transmis nos observations supplémentaires relatives à cette réforme au Parlement européen, à la Commission et au Conseil.

Nous avons également continué à participer aux discussions au sein du Parlement et du Conseil.

Outre ces sujets et dans le prolongement de la tendance observée les années précédentes, les domaines couverts par nos avis ont continué de se diversifier. En 2013, la Commission a publié un grand nombre de propositions législatives ayant des incidences sur le droit fondamental à la protection des données à caractère personnel. Hormis les priorités traditionnelles, telles que la poursuite du développement de l'espace de liberté, de sécurité et de justice (ELSJ) ou les transferts internationaux de données, de nouveaux domaines apparaissent, comme la stratégie numérique, l'internet, les questions financières et les services de santé en ligne.

Nous avons abordé la question de la stratégie numérique et de l'internet dans notre avis sur la communication de la Commission intitulée «Une stratégie numérique pour l'Europe – faire du numérique un moteur pour la croissance européenne», dans notre avis sur le «Marché unique européen des communications électroniques» et dans notre avis sur le livre vert intitulé «Se préparer à un monde audiovisuel totalement convergent: croissance, création et valeurs».

En ce qui concerne l'espace de liberté, de sécurité et de justice (ELSJ), nous avons émis des avis sur Europol, la stratégie de l'Union en matière de cybersécurité, les frontières intelligentes ainsi que l'accord UE-Canada relatif aux dossiers passagers (PNR) et le modèle européen d'échange d'informations.

En ce qui concerne le marché intérieur, nous avons publié des avis sur la lutte contre le blanchiment de capitaux et le financement du terrorisme, sur les paiements dans le marché intérieur, sur le droit européen des sociétés et la gouvernance d'entreprise, ainsi que sur la facturation électronique dans le cadre des marchés publics.

Dans le domaine des services de santé en ligne, l'accent a été mis sur les dispositifs médicaux, les précurseurs de drogues et sur le plan d'action pour la santé en ligne.

3.2. Cadre d'action et priorités

3.2.1. Mise en œuvre de la politique de consultation

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

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

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

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

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 d'autres instruments dans son rôle consultatif. Si cette approche nécessite des contacts étroits avec les institutions, il est essentiel de conserver notre indépendance.

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

À ces instruments ont été récemment ajoutés des lignes directrices tournées vers l'avenir et des avis préliminaires. Nous les utilisons pour expliquer l'importance et les avantages de la mise en œuvre correcte des principes en matière de protection des données. Ils seront élaborés de notre propre initia-

tive et non liés à une proposition législative spécifique. Ils sont destinés à fournir aux décideurs politiques et aux organismes de contrôle des points de référence pour l'application des principes fondamentaux dans les politiques futures.

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.

Les consultations formelles sont assez souvent précédées d'une demande d'observations informelles. Lorsque la Commission élabore une nouvelle mesure législative ayant des répercussions sur la protection des données, le projet nous est généralement envoyé au cours de la consultation interservices, c'est-à-dire avant que la proposition ne soit finalisée et adoptée. Ces observations informelles, au nombre de 33 en 2013, permettent de traiter les questions de protection des données à un stade précoce où il est encore possible de modifier le texte d'une proposition relativement aisément. La présentation d'observations informelles à la Commission est un moyen précieux de garantir que les principes de protection des données sont dûment pris en considération au moment de la rédaction d'une proposition législative, et il est très souvent possible de résoudre des problèmes cruciaux à cette étape. En règle générale, ces observations informelles ne sont pas rendues publiques. Si elles sont suivies par un avis ou des observations formelles, nous faisons généralement référence aux observations informelles présentées antérieurement.

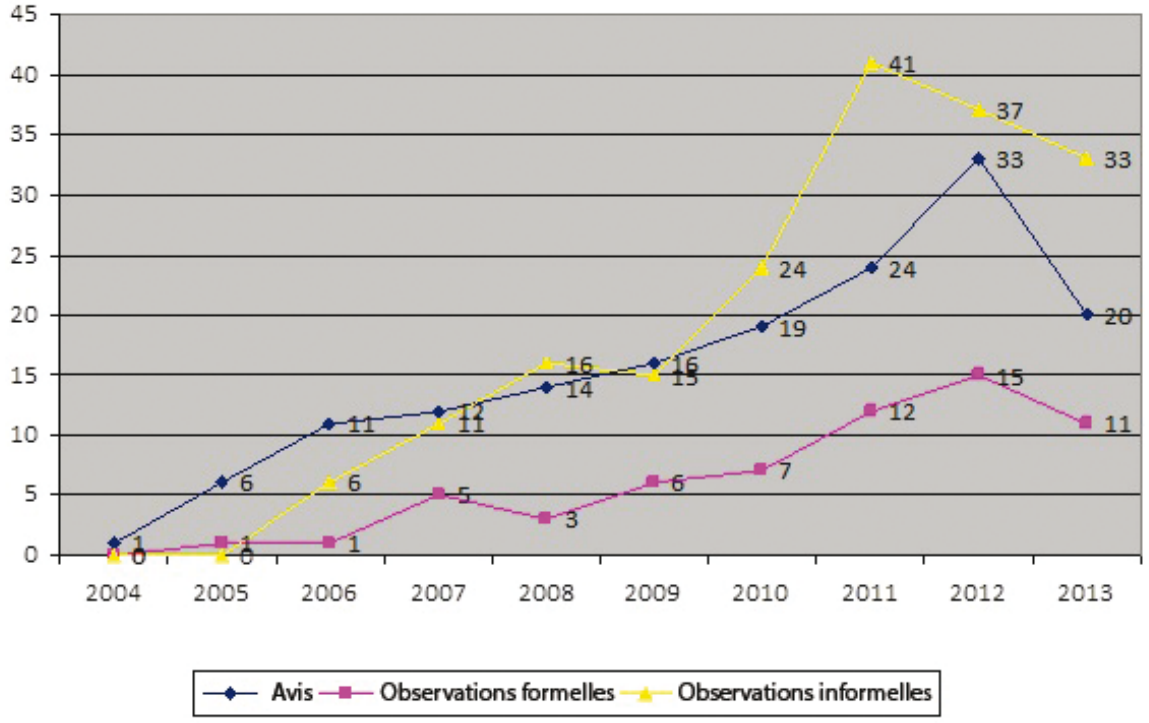
Des contacts réguliers avec les services de l'institution concernée auront lieu après la publication d'observations ou d'avis du CEPD. Dans certains cas, nous sommes largement impliqués dans les discussions et négociations qui se déroulent au Parlement et au Conseil. Dans d'autres cas, la Commission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

3.2.2. Résultats en 2013

En 2013, le nombre d'avis que nous avons émis a connu une légère diminution par rapport à la hausse constante enregistrée les années précédentes. Cette diminution s'explique en grande partie par le fait que nous nous sommes concentrés efficacement sur nos priorités stratégiques, notamment sur la révision du cadre en matière de protection des données. Le CEPD a émis 20 avis, 13 observations formelles et 33 observations informelles sur toute une série de thèmes. Grâce à ces avis et aux autres instruments utilisés dans nos interventions, nous avons mis en œuvre les priorités du CEPD pour 2013, telles que définies dans notre inventaire.

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

À la suite des nombreuses activités entreprises dans le cadre de la réforme en 2012 et de notre avis de mars 2012, nous avons adressé des observations supplémentaires au Parlement européen,



à la Commission européenne et au Conseil le 15 mars 2013. Ces observations portaient sur des points particuliers nécessitant des éclaircissements et répondaient également aux amendements proposés par les commissions compétentes du Parlement européen.

Dans nos observations, nous avons réitéré que les données pseudonymisées restent des données à caractère personnel (ou des informations personnelles) et doivent être protégées en tant que telles. Toute définition des données anonymes ou des données pseudonymisées doit, dès lors, être pleinement cohérente avec la définition des données à caractère personnel et ne doit pas engendrer la suppression excessive de certaines catégories de données à caractère personnel de la portée du cadre en matière de protection des données. Nous avons également déconseillé d'exclure des secteurs spécifiques de la portée de l'application du cadre européen en matière de protection des données; nous avons par ailleurs déconseillé de limiter la portée territoriale du règlement général proposé en matière de protection des données.

Nous avons soutenu l'élimination d'un éventuel traitement ultérieur des données en vue de finalités incompatibles et nous avons souligné que la définition du consentement explicite doit être conservée. Nous avons également apporté notre soutien à la définition relative aux responsables du traitement et aux sous-traitants et à leurs responsabilités telle que proposée par la Commission, ainsi qu'au principe de responsabilité qui doit s'appliquer à l'ensemble de la proposition. Certains éléments de l'approche dite fondée sur le risque étaient les bienvenus, mais nous avons indiqué que la protection complète telle que prévue dans le règlement doit s'appliquer à tous les traitements. En ce qui concerne les transferts internationaux, nous avons recommandé de clarifier les règles et nous avons accueilli favorablement les amendements introduisant un nouvel article sur les transferts non autorisés en vertu de la législation européenne.

Pour ce qui est de la proposition de directive sur la protection des données en matière d'application de la législation pénale, nous avons apporté notre soutien à l'alignement le plus étroit de la proposition de directive sur la proposition de règlement et ce afin de veiller à la cohérence. Nous avons également accueilli favorablement les amendements introduisant des conditions et protections spécifiques en ce qui concerne l'accès par les autorités répressives aux données initialement traitées à d'autres fins et nous avons mis en évidence le fait que tout transfert vers des parties privées ou vers des autorités autres que des autorités répressives doit être strictement limité.

À la suite de négociations épineuses et de nombreux compromis politiques, la commission LIBE du Parlement européen a voté en faveur de son rapport le 21 octobre 2013. Des progrès fondamentaux ont été accomplis, mais le processus politique au sein du Parlement européen n'est pas encore achevé, étant donné que la prochaine et dernière étape de la première lecture du Parlement est un vote en plénière.

Au Conseil, les progrès sont restés plus limités. Les négociations entre les États membres se poursuivent sur des volets importants du cadre législatif, tels que le mécanisme de guichet unique et l'idée d'adopter un paquet législatif composé d'un règlement et d'une directive, parmi d'autres questions sensibles d'un point de vue politique et complexes sur le plan juridique.

Au cours de l'année 2013, nous avons continué de conseiller le Parlement européen et le Conseil et nous avons participé aux discussions. Nous avons également contribué au lancement du processus de révision du règlement (CE) n° 45/2001, qui régit le traitement des données par les institutions européennes, en adressant à la Commission une lettre exprimant nos positions initiales.

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

3.4.1. Renforcer la coopération dans le domaine de la répression au sein de l'UE: le modèle européen en matière d'échange d'informations

Le 29 avril 2013, nous avons adopté un avis sur la communication de la Commission intitulée «Renforcer la coopération dans le domaine de la répression au sein de l'UE: le modèle européen en matière d'échange d'informations». Nous avons apprécié l'attention générale accordée à la protection des données dans cette communication et nous nous sommes réjouis du fait que cette dernière conclut que ni une nouvelle base

de données paneuropéenne concernant l'application de la législation ni de nouveaux instruments relatifs à l'échange d'informations au sein de l'Union ne sont nécessaires.

Nous avons cependant insisté sur la nécessité de procéder à une évaluation complète des initiatives et instruments existants dans le domaine de la justice et des affaires intérieures, ce qui devrait aboutir à une stratégie européenne globale, intégrée et bien structurée en matière de gestion des informations et des échanges.

3.4.2. Europol

Le 31 mai 2013, nous avons adopté un avis sur la proposition de la Commission relative à un nouveau cadre juridique pour l'Agence de l'Union européenne pour la coopération et la formation des services répressifs (Europol). Dans notre avis, nous avons souligné que cette proposition a des répercussions importantes pour la protection des données étant donné que le traitement d'informations englobant des données à caractère personnel est la raison principale de l'existence d'Europol. Nous avons également souligné qu'un cadre solide de protection des données est non seulement important pour les personnes concernées, mais qu'il contribue également à une coopération policière et judiciaire fructueuse.

Nous avons compris la nécessité d'approches innovantes et flexibles pour prévenir et lutter contre les crimes graves, mais nous avons insisté sur des mesures de protection fortes et sur la nécessité de définir clairement les finalités du traitement des données effectué par Europol ainsi que les critères pour les transferts de données vers des pays tiers et des organisations internationales. Nous avons également formulé des recommandations pour continuer à améliorer le régime de la protection des données d'Europol et nous nous sommes en partie réjouis de l'architecture solide de la supervision du traitement des données, qui englobe la surveillance par le CEPD et, le cas échéant, avec la participation active des autorités nationales chargées de la protection des données (APD).

Dans des courriers adressés au Conseil et au Parlement en novembre 2013, nous avons expliqué plus en détail la nécessité d'une supervision forte d'Europol.

3.4.3. Stratégie de cybersécurité de l'Union européenne

Le 17 juin 2013, nous avons publié un avis sur la stratégie de cybersécurité de l'Union européenne. Nous avons souligné que si la cybersécurité vise à favoriser la protection des données à caractère personnel dans l'environnement en ligne, elle ne saurait cependant servir d'excuse à l'analyse et au contrôle illimités des informations personnelles des particuliers. Bien qu'elle reconnaisse à juste titre l'importance des principes de protection des données, dans le cadre de la gestion de la sécurité du cyberespace, la stratégie n'est pas claire sur la façon dont ces principes seront appliqués dans la pratique.

Nous avons observé un manque de clarté quant à l'intégration des mesures proposées dans la législation existante et à venir en matière de protection des données et de sécurité. Nous avons fait remarquer que le rôle des autorités chargées de la protection des données dans la mise en œuvre et la mise en application des obligations en matière de sécurité et dans le renforcement de la cybersécurité n'était pas envisagé correctement. En outre, l'échange d'informations relatives à la sécurité entre les autorités nationales compétentes en matière de sécurité tel qu'établi par la proposition ne fournit cependant pas de garanties suffisantes en ce qui concerne les niveaux de sécurité et la protection des données à caractère personnel.

3.4.4. Frontières intelligentes

Le 18 juillet 2013, nous avons rendu notre avis sur les frontières intelligentes, axé en particulier sur le système d'entrée/sortie. Dans cet avis, nous avons indiqué qu'il n'existe pas de preuves claires du fait que les propositions de la Commission concernant la création d'un système de frontières intelligentes pour les frontières extérieures de l'Union rempliront les objectifs qu'elles ont fixés. Nous avons considéré que l'un des objectifs annoncés des propositions était le remplacement du système en vigueur, qualifié de «lent et peu fiable», mais les évaluations de la Commission n'indiquent nullement que la solution de remplacement sera suffisamment efficace pour justifier les dépenses et les intrusions dans la vie privée.

Nous reconnaissons que l'amélioration de la gestion des contrôles aux frontières est un exercice légitime. Nous avons cependant fait remarquer qu'il serait plus efficace de le faire lorsqu'une politique européenne claire de gestion des 'over stayers' (individus qui dépassent la durée du droit de séjour) aura été établie. En l'absence d'une telle politique, la création d'une nouvelle base de données IT à grande échelle pour stocker des quantités énormes d'informations personnelles est une réponse disproportionnée à un problème que d'autres systèmes créés récemment pourraient être à même de résoudre. Il serait prudent, d'un point de vue à la fois économique et pratique, d'évaluer les systèmes existants afin, au minimum, de garantir cohérence et bonnes pratiques.

3.4.5. Accord UE-Canada relatif aux données des dossiers passagers (PNR)

Le 30 septembre 2013, nous avons émis un avis sur les propositions de la Commission relatives à la conclusion et à la signature de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers (PNR).

De même que dans nos avis précédents sur les accords européens PNR, , nous nous sommes interrogés sur la nécessité et la proportionnalité des régimes PNR et sur les transferts importants de données PNR vers des pays tiers. Nous avons également contesté le choix de la base juridique qui, d'après nous, devrait être essentiellement l'article 16 du TFUE concernant la protection des données à caractère personnel, plutôt que l'article 82, paragraphe 1, point d), et l'article 87, paragraphe 2, point a), sur la coopération judiciaire en matière pénale et sur la coopération policière.

Nous nous sommes également inquiétés de l'accès limité à un recours administratif indépendant et à un recours judiciaire à part entière pour les citoyens de l'UE qui ne se trouvent pas au Canada, et nous nous sommes interrogés sur la pertinence d'un accord exécutif pour y parvenir. Nous avons également recommandé qu'il soit clairement indiqué qu'aucune autre autorité canadienne ne peut avoir directement accès aux données PNR ou les demander directement aux transporteurs.

3.5. Marché intérieur, comprenant les données financières

3.5.1. Droit européen des sociétés et gouvernance d'entreprise

Dans son *Plan d'action relatif au droit européen des sociétés et à la gouvernance d'entreprise: trouver l'équilibre entre le respect de la vie privée des investisseurs et la nécessité de surveillance réglementaire et de transparence*, la Commission a exposé les grandes lignes de ses initiatives en vue de moderniser le droit des sociétés et la gouvernance d'entreprises en Europe.

Dans notre courrier du 27 mars 2013, nous avons rappelé à la Commission que toute proposition législative visant à améliorer la visibilité des participations doit tenir dûment compte des droits des actionnaires à la protection de leurs informations personnelles. Les responsables politiques doivent évaluer soigneusement et définir clairement les objectifs de politique publique qui augmentent cette visibilité et mettre ces objectifs en balance avec les risques pour les droits des actionnaires à la protection de leur vie privée.

Une meilleure surveillance de la politique de rémunération par les actionnaires est un autre domaine de la proposition dans lequel la nécessité de transparence devrait être mise en balance avec les droits des personnes au respect de leur vie privée et à la protection de leurs données. Nous encourageons l'exploration de diverses méthodes, modalités et granularités de mise à la disposition du public de données à caractère personnel pour garantir que les mesures adoptées soient proportionnées à tout scénario qui autorise l'accès du public aux informations sur la rémunération des membres de la direction et/ou des organes de supervision.

3.5.2. Règlement concernant la surveillance du marché des produits

Dans notre avis du 30 mai 2013, nous avons analysé la proposition de règlement de la Commission sur la surveillance du marché des produits qui vise à garantir que les produits ne portent pas atteinte à la santé et à la sécurité ou à tout autre aspect de l'intérêt public et qu'ils sont conformes aux exigences définies dans la législation d'harmonisation de l'Union. Dans notre avis, nous avons souligné qu'une proposition doit toujours examiner si les règles européennes en matière de protection des données sont applicables, en particulier lorsque le partage d'informations est autorisé, que ce soit par l'intermédiaire de plates-formes informatiques spécifiques ou non.

En règle générale, lorsqu'une proposition législative concerne le traitement d'informations personnelles, même s'il ne s'agit pas de la finalité principale, les règles nationales de mise en œuvre de la directive 95/46/CE sur la protection des données ou les dispositions du règlement (CE) n° 45/2001 sont applicables. Certaines conditions s'appliquent dès lors lorsque des informations personnelles doivent être collectées, analysées ou traitées. Par exemple, seules les informations personnelles strictement nécessaires pour la finalité déclarée doivent être collectées et des délais spécifiques relatifs à la conservation des informations collectées doivent être fixés.

Nous avons également souligné que, lorsque les informations personnelles d'un opérateur économique (par exemple, le fabricant, son représentant autorisé, l'importateur et/ou le distributeur d'un produit disponible sur le marché de l'Union) doivent être rendues publiques, le type de données à caractère personnel qui doit être publié et les raisons de cette publication doivent être explicités dans une déclaration de confidentialité préalable à l'attention des personnes concernées.

3.5.3. Frais liés aux comptes de paiement

Le 27 juin 2013, nous avons publié des observations formelles sur la proposition de directive de la Commission sur la comparabilité des frais liés aux comptes de paiement, le changement de compte de paiement et l'accès à un compte de paiement assorti de prestations de base. La proposition souligne les mesures relatives à la comparabilité des frais liés aux comptes de paiement et présente aux consommateurs un aperçu des offres sur le marché ainsi que les

modalités de changement qui leur permettront de changer facilement de compte si une meilleure offre est disponible. Tous ces éléments visent à renforcer la concurrence sur le marché des services financiers, au profit des consommateurs. Cependant, afin de garantir qu'autant de consommateurs que possible puissent réellement bénéficier des avantages de ces améliorations, il est essentiel de veiller à ce que tous les citoyens européens disposent du droit d'accès aux services de base des comptes de paiement.

Nous avons accueilli favorablement le fait que tout échange de données à caractère personnel des consommateurs par les prestataires de services de paiement lors de la «phase de changement» est soumis au consentement préalable, écrit et explicite du consommateur. Nous nous sommes également réjouis du fait que la proposition de directive rappelle spécifiquement le principe de nécessité en ce qui concerne le partage d'informations entre les prestataires de services de paiement. Nous avons cependant souligné que la proposition doit mentionner que la législation européenne pertinente en matière de protection des données continue de s'appliquer pleinement pour ce qui est des obligations introduites par la directive.

3.5.4. Lutte contre le blanchiment de capitaux

Le 4 juillet 2013, nous avons émis un avis sur la proposition de directive de la Commission relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme et sur sa proposition de règlement relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds. Nous avons reconnu la légitimité de la transparence des sources de paiement, des dépôts de fonds et des transferts de fonds afin de lutter contre le terrorisme et le blanchiment de capitaux, mais nous avons insisté sur le fait que les exigences de la protection des données doivent être incluses dans la législation transposant les normes internationales au niveau de l'Union. Nous avons regretté que ni la proposition de directive ni la proposition de règlement n'abordent pleinement les préoccupations en matière de protection des données et ne précisent pas l'application des règles européennes relatives à la protection des données aux activités de traitement spécifiques concernées. Les textes proposés ne contenaient aucune disposition importante sur les questions relatives à la protection des données.

Plus précisément, nous avons exprimé nos préoccupations quant aux grandes quantités d'informations personnelles collectées au nom de la lutte contre le blanchiment de capitaux et contre le terrorisme, en particulier par les professionnels en raison de l'obligation de diligence à l'égard de la clientèle. Nous avons recommandé que le principe de limitation de la finalité soit strictement respecté et que des orientations supplémentaires soient communiquées aux professionnels sur les données qu'ils doivent ou non collecter. Nous avons également souligné que les textes doivent davantage développer le rôle des droits des individus, et en particulier sensibiliser les professionnels et les clients. Nous avons également indiqué que limiter le droit des individus n'est justifié que si cela s'avère nécessaire.

Considérant les transferts répétés, structurels et de masse de données à caractère personnel qui auront lieu dans le cadre de la proposition de directive et de la proposition de règlement, nous avons souligné les risques liés à ces transferts vers des pays tiers et avons recommandé d'y inclure des dispositions spécifiques de fond relatives aux transferts de données à caractère personnel, comme un test de proportionnalité, afin d'assurer correctement la protection des individus lorsque des informations les concernant sont transférées.

Nous avons en outre indiqué que le choix des périodes de conservation des données doit être justifié. Nous avons également insisté sur le fait que la publication des sanctions imposées aux professionnels ne respectant pas leurs obligations en vertu de ces textes doit respecter le principe de proportionnalité.

3.5.5. Vente de contrefaçons sur l'internet

Le 11 juillet 2013, nous avons publié nos observations sur le rapport de la Commission sur le fonctionnement du protocole d'accord sur la vente de contrefaçons sur l'internet. Nous avons accueilli favorablement la publication de ce rapport, qui fournit des informations sur la manière dont les plates-formes internet étant partie au

protocole d'accord ont mis en œuvre des procédures de notification et de retrait ('notice and take down') et sur les mécanismes qu'elles ont créés pour coopérer et partager des informations - y compris les informations personnelles des contrevenants présumés - avec les détenteurs de droits.

Nous avons pris note du rôle de la Commission dans la reconnaissance de l'importance de ces questions et dans la facilitation du dialogue entre les sociétés et les associations professionnelles afin de garantir que toutes les mesures prises respectent la législation applicable ainsi que les droits des individus au respect de la vie privée et à la protection des données. Nous avons en outre exprimé notre souhait de participer au dialogue en cours.

3.5.6. Protection des marques

Le 11 juillet 2013, nous avons rendu un avis sur la proposition de directive de la Commission rapprochant les législations des États membres sur les marques et sur sa proposition de règlement modifiant le règlement sur la marque communautaire. Dans notre avis, nous avons mis l'accent sur le fait que la collecte et le traitement des données à caractère personnel par les services centraux de la propriété industrielle des États membres et par l'Office de l'harmonisation dans le marché intérieur (OHMI) doivent respecter la législation applicable en matière de protection des données.

Nous avons également recommandé que les modalités relatives aux échanges d'informations via des bases de données de marques communes ou connectées et via des portails soient clairement fixées, en particulier en définissant les destinataires autorisés des données à caractère personnel, les types de données, la finalité de ces échanges et la durée de conservation des données dans ces systèmes informatiques. Nous avons par ailleurs recommandé que si les échanges d'informations entre l'OHMI et les offices nationaux englobent des données à caractère personnel il convient de le préciser, ainsi que leurs types.

3.5.7. Facturation électronique dans le cadre des marchés publics

Le 11 novembre 2013, nous avons rendu un avis sur une proposition de directive de la Commission relative à la facturation électronique dans le cadre des marchés publics. Dans cet avis, nous avons apporté notre soutien à l'objectif poursuivi par la Commission de faciliter le passage à la facturation électro-

nique sans support papier. Dans le même temps, nous avons également attiré l'attention sur l'accroissement des risques concernant la protection de la vie privée et des données qui découlera de la disponibilité croissante de données de facturation sans support papier et dans un format lisible par machine pour des finalités ultérieures.

Si nous avons reconnu que d'autres utilisations acceptables de données sont susceptibles d'exister, par exemple, dans le cadre des paiements électroniques et de l'archivage électronique; nous avons averti que d'autres finalités, comme le profilage automatisé et l'extraction de données pour des finalités fiscales et judiciaires, ne seront probablement pas considérées comme compatibles et pourront n'être envisageables, le cas échéant, que sous réserve des exceptions et des critères stricts prévus à l'article 13 de la directive 95/46/CE.

3.5.8. Paiements dans le marché intérieur

Le 5 décembre 2013, nous avons émis un avis sur la proposition de directive relative aux services de paiement dans le marché intérieur. Dans cet avis, nous avons accueilli favorablement l'introduction d'une disposition importante qui indique que tout traitement de données à caractère personnel ayant lieu dans le cadre de cette proposition de directive doit être effectué dans le plein respect des législations nationales mettant en œuvre la directive 95/46/CE et la directive 2002/58/CE et dans le plein respect du règlement (CE) n° 45/2001.

Nous avons recommandé de préciser les références à la législation applicable en matière de protection des données par l'intermédiaire de mesures concrètes qui s'appliqueront à toute situation dans laquelle le traitement de données à caractère personnel est envisagé. Il convient en outre de préciser expressément que le traitement d'informations personnelles peut être effectué dans la mesure où il est nécessaire pour la réalisation des services de paiement. Nous avons en outre mis en évidence d'autres questions relatives à la protection des données, par exemple, en ce qui concerne les échanges d'informations, l'accès par des tiers aux informations sur le compte et les rapports en matière de sécurité.

3.6. Stratégie numérique et technologie

3.6.1. Équipement radio

La proposition de directive de la Commission relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements radioélectriques remplacera la directive 1999/5/CE concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité (la directive dite «R&TTE».

À quelques exceptions près, tout équipement faisant usage des ondes radio ou des fréquences de télécommunication serait concerné par ces règles, par exemple, les voitures équipées de cartes SIM (comme en ce qui concerne le service intégré eCall abordé ci-dessous), qui utilisent un équipement hertzien. Étant donné que l'utilisation de cette technologie autorise le suivi de la localisation d'un véhicule (et dès lors d'une personne), son utilisation a des incidences pour la vie privée des individus. Dans nos observations formelles du 27 février 2013, nous avons fait remarquer que la directive dite «R&TTE» a incité les fabricants de ces équipements à appliquer la protection de la vie privée dès la conception.

Nous étions dès lors satisfaits que la proposition se fonde sur l'approche de la directive R&TTE en matière de vie privée et de protection des données dans la mesure où ces domaines restent des exigences essentielles en ce qui concerne la conception des équipements hertziens. Nous avons également accueilli favorablement le fait que la proposition impose clairement aux fabricants la responsabilité de garantir que les équipements hertziens commercialisés sont conçus et fabriqués de telle façon qu'ils sont munis, entre autres, de dispositifs visant à garantir la protection des données à caractère personnel et de la vie privée des consommateurs. Nous regrettons cependant que les équipements terminaux fixes aient été exclus du champ d'application de la directive, ce qui réduit les incitations à intégrer le principe du respect de la vie privée dès la conception dans ces équipements. Cela est particulièrement regrettable dans la mesure où les équipements terminaux jouent un rôle de plus en plus important pour la protection de la vie privée et qu'il n'existe pas de règle équivalente relative à la protection des données à caractère personnel et de la vie privée dans d'autres instruments législatifs qui s'appliquent aux équipements terminaux n'utilisant pas la radio.

Nous avons dès lors recommandé que la proposition contienne un engagement de la Commission à contrôler la conformité des équipements terminaux aux exigences en matière de protection des données et de respect de la vie privée et à mettre en œuvre les mesures nécessaires le cas échéant.

3.6.2. La stratégie numérique pour l'Europe - faire du numérique un moteur de la croissance européenne

Dans sa communication intitulée «*La stratégie numérique pour l'Europe - faire du numérique un moteur de la croissance européenne*», la Commission a défini plusieurs domaines politiques sur lesquels elle concentrera ses efforts pour permettre et stimuler le développement de l'économie numérique, comme le marché unique numérique, la fourniture et la demande de l'internet très rapide, l'informatique en nuage ainsi que la confiance et la sécurité.

Dans notre avis du 10 avril 2013, nous avons souligné que toute conception et tout déploiement de nouvelles applications et solutions TIC pour le monde du numérique doit respecter les principes de la protection des données, en particulier étant donné que le *respect de la vie privée dès la conception* deviendra une obligation juridique en vertu de la proposition de règlement sur la protection des données. Nous avons en outre rappelé à la Commission que le recours à l'interopérabilité comme instrument pour favoriser le partage des données entre les bases de données doit s'appuyer sur une base juridique adéquate et être soumis à des garanties sur la protection des données appropriées.

Dans le domaine de l'informatique en nuage, nous avons mentionné les nombreuses orientations qui ont été fournies par les autorités chargées de la protection des données et par le CEPD au sujet de l'application de la législation sur la protection des données actuellement en vigueur, d'une part, de l'impact de la proposition de règlement sur la protection des données, d'autre part. Nous avons dès lors demandé instamment à la Commission de s'inspirer de ces orientations pour renforcer la confiance des individus et des clients dans ces nouvelles technologies, ce qui garantira alors le succès de leur déploiement.

3.6.3. Se préparer à un monde audiovisuel totalement convergent: croissance, création et valeurs

Le 24 avril 2013, la Commission a publié un livre vert intitulé «*Se préparer à un monde audiovisuel totalement convergent: croissance, création et valeurs*». Ce livre vert a lancé une consultation publique sur les conséquences de la transformation du paysage audiovisuel en cours: les médias audiovisuels ne sont plus uniquement fournis par les moyens traditionnels et par les services de radiodiffusion traditionnels, mais ils sont également fournis par des fournisseurs à la demander par l'internet et ils atteignent les consommateurs par l'intermédiaire de télévisions, ordinateurs de bureau ou portables ou tablettes et terminaux mobiles connectés, et souvent qualifiés d'«intelligents», comme les téléphones intelligents.

Dans nos observations du 30 août 2013, nous avons souligné que ces nouveaux modes de distribution et de consommation des œuvres audiovisuelles génèrent de nouvelles formes de collecte et de traitement des données à caractère personnel des utilisateurs. Cependant, les utilisateurs risquent de ne pas toujours savoir que lorsqu'ils visionnent des œuvres audiovisuelles ou interagissent avec des services associés, des données à caractère personnel sont générées à différents niveaux de la fourniture de services (par exemple, par leur terminal, leur fournisseur de services internet ou leur radiodiffuseur) ou ils risquent de ne pas être au courant de l'ampleur de ce traitement. Les utilisateurs ne contrôlent par conséquent pas leurs données.

Nous estimons que tout choix politique dans ce domaine doit pleinement respecter le cadre juridique européen en matière de protection des données. Nous avons entre autres souligné qu'il convient d'assurer aux utilisateurs une transparence intégrale à l'égard des types de données à caractère personnel les concernant qui sont collectées, et à l'égard des personnes qui les collectent, qu'il convient d'obtenir le consentement de l'utilisateur au traitement de ses données le cas échéant, et qu'une attention particulière doit être accordée à la protection de la vie privée et des données à caractère personnel des enfants, en particulier dans le domaine de la publicité. Des outils techniques doivent contribuer à protéger la vie privée et les données à caractère personnel des enfants.

3.6.4. Marché unique européen des communications électroniques

Le 14 novembre 2013, nous avons publié un avis sur la proposition de règlement de la Commission harmonisant les services de communications électroniques au sein de l'Union.

Dans notre avis, nous avons signalé que les mesures proposées étaient de nature à restreindre indûment la liberté de l'internet. Nous avons salué l'inclusion du principe de neutralité de l'internet dans le texte, c'est-à-dire la transmission impartiale d'informations sur l'internet, mais nous avons également indiqué qu'il était dénué de substance compte tenu du droit quasi illimité dont dispose les fournisseurs en matière de gestion du trafic sur l'internet. Nous avons également mis en garde contre l'application de mesures hautement intrusives pour la vie privée sous le couvert de la répression pénale ou aux fins de filtrer des contenus illégaux en vertu du droit national ou européen, des mesures qui sont incompatibles avec le principe de l'internet ouvert.

La confiance en notre environnement numérique au cours des années à venir dépend de notre capacité à fournir des infrastructures juridiques et techniques qui puissent générer et préserver la confiance en la société numérique. Cette confiance a déjà été sérieusement ébranlée récemment par les différents scandales en matière de surveillance. Pour renforcer la confiance des consommateurs dans le marché des communications électroniques au sein de l'Union, il convient de garantir aux utilisateurs le respect de leurs droits à la vie privée, à la confidentialité de leurs communications et à la protection de leurs informations à caractère personnel. Nous avons instamment demandé à la Commission d'indiquer des raisons plus précises pour lesquelles des mesures de gestion du trafic peuvent être appliquées. Toute interférence avec leurs droits doit être clairement communiquée aux utilisateurs, pour leur permettre de passer aux fournisseurs appliquant à leurs services des techniques de gestion du trafic moins intrusives pour la vie privée.

Enfin, nous avons fait remarquer que la supervision de toute demande de mesures de gestion du trafic par des fournisseurs devrait inclure un rôle accru pour les autorités nationales chargées de la protection des données afin de garantir le plein respect des droits des utilisateurs en matière de vie privée et de protection des données.

3.7. Santé publique et consommateurs

3.7.1. Précurseurs de drogues et pays tiers

Le 18 janvier 2013, nous avons publié un avis sur les propositions de la Commission visant à modifier les règlements sur le commerce intra-UE et sur le commerce avec les pays tiers de précurseurs de drogues (substances légales utilisées dans la fabrication de substances narcotiques et psychotropes). Nous avons accueilli favorablement la référence dans les proposi-

tions à l'applicabilité de la législation européenne en matière de protection des données. Nous sommes également satisfaits du fait que de nombreuses catégories d'informations à traiter étaient précisées et que le principe de limitation de la finalité était mentionné dans la proposition relative au commerce extérieur.

Nous avons cependant recommandé que les principaux textes législatifs soulignent tous les éléments essentiels des traitements, comme l'exclusion du traitement des données sensibles. En outre, toutes les catégories d'informations à traiter devraient être précisées, au minimum, dans les actes délégués, mais de préférence également dans les propositions.

Parmi nos autres recommandations, figuraient les éléments suivants: la proposition relative au commerce intra-UE devrait préciser que les informations personnelles relatives à des transactions suspectes ne peuvent être utilisées que pour empêcher le détournement de substances classifiées, que des périodes de conservation maximales devraient être fixées pour tous les traitements et que des garanties appropriées devraient être fournies pour les transferts internationaux d'informations personnelles.

Nous avons en outre recommandé de clarifier qui a accès à la nouvelle base de données européenne sur les précurseurs de drogues et de veiller à la supervision coordonnée de cette base de données européenne par le CEPD et les autorités nationales chargées de la protection des données, de la même manière que pour le système d'information du marché intérieur. Nous avons par ailleurs recommandé d'interdire l'interconnexion de cette base de données européenne avec d'autres bases de données créées à des finalités différentes.

3.7.2. Dispositifs médicaux

Les propositions de règlement de la Commission concernant les dispositifs médicaux et les dispositifs médicaux in vitro engendreront le traitement et le stockage de grands volumes d'informations personnelles, et peut-être l'enregistrement de données sensibles, comme des informations sur la santé de patients, dans une base de données centrale européenne (Eudamed).

Dans notre avis du 8 février 2013, nous avons reconnu et accueilli favorablement l'attention spécifique accordée à la protection des données dans les propositions de règlement. Nous estimons cependant que des améliorations et précisions supplémentaires sont nécessaires, par exemple, sur les types de catégories d'informations personnelles à traiter, en particulier lorsque des données sensibles relatives à la santé sont susceptibles d'être traitées et stockées. Nous avons recommandé que ces propositions de règlement précisent les circonstances dans lesquelles des données à caractère personnel relatives à la santé peuvent être incluses dans la base de données Eudamed et que des garanties soient mentionnées en ce qui concerne le traitement et le stockage.

3.7.3. Plan d'action pour la santé en ligne

Dans notre avis du 27 mars 2013, sur la communication de la Commission intitulée «*Plan d'action pour la santé en ligne 2012 - 2020 - des soins de santé innovants pour le XXIe siècle*», nous nous sommes félicités de l'attention accordée à la protection des données dans la communication. Cependant, les données à caractère personnel traitées dans le cadre des TIC de santé en ligne et de bien-être portent souvent sur des données sanitaires, d'où la nécessité d'assurer un niveau de protection des données plus élevé.

Nous avons instamment demandé aux professionnels du secteur, aux États membres et à la Commission de dûment tenir compte des incidences en matière de protection des données, lors de la mise en œuvre d'initiatives dans le domaine de la santé en ligne. Nous avons en outre recommandé à la Commission de consulter le CEPD avant de prendre de nouvelles mesures législatives et non législatives comme celles décrites dans la communication.

3.7.4. Précurseurs de drogues et Russie

Le 23 avril 2013, nous avons adopté un avis sur la proposition de la Commission relative à la conclusion d'un accord entre l'Union européenne et la Fédération de Russie concernant les précurseurs de drogues. Cet accord vise à accroître la coopération pour empêcher que des substances légales ne soient utilisées pour fabriquer illégalement des stupéfiants et des substances psychotropes (qualifiés de «précurseurs de drogues»). Cet accord autori-

sera par exemple le transfert d'informations personnelles relatives à des transactions suspectes de précurseurs de drogues.

Nous nous sommes félicités de la présence, dans le texte de l'accord, de dispositions relatives à la protection des données à caractère personnel et de l'inclusion de principes contraignants relatifs à la protection des données dans l'annexe. Nous nous sommes préoccupés du caractère exécutoire réel de ces principes. Nous avons dès lors conseillé que les autorités chargées de la protection des données de l'Union européenne et la Russie examinent ensemble la mise en œuvre de l'accord. Nous avons également recommandé que le texte prévoie explicitement la possibilité de suspension ou de résiliation de l'accord si les principes de la protection des données sont violés.

En outre, nous avons conseillé de mieux préciser les garanties en matière de protection des données, par exemple, la finalité des transferts d'informations personnelles, les délais de conservation, les catégories des données à échanger et la protection des données relatives à des transactions suspectes. Aux fins de l'exhaustivité des principes contraignants relatifs à la protection des données, nous avons recommandé d'ajouter des dispositions relatives aux données sensibles, à la sécurité des données et à la restriction des transferts ultérieurs d'informations personnelles.

3.7.5. Prix des médicaments à usage humain

Le 30 mai 2013, nous avons adopté un avis sur la proposition modifiée de directive de la Commission relative à la *transparence des mesures régissant la fixation des prix des médicaments à usage humain et leur inclusion dans le champ d'application des systèmes publics d'assurance-maladie*. Cette proposition vise à garantir que les mesures nationales réglementant la fixation des prix et le remboursement des médicaments ne sont pas contraires au principe de libre circulation des biens.

Nous avons souligné que les informations personnelles traitées dans le cadre des procédures de fixation des prix et de remboursement des autorités sanitaires nationales sont susceptibles d'être liées à des données relatives à la santé des patients. Par conséquent, un niveau supérieur de protection des données est exigé. Nous avons recommandé que toutes les données relatives à la santé des patients incluses par une société pharmaceutique dans sa demande d'autorisation de mise sur le marché d'un médicament soient rendues complètement anonymes - en d'autres termes, que l'identité de la personne ne puisse être déterminée - avant que ces données ne soient transférées aux autorités sanitaires nationales pour faire l'objet d'un nouveau traitement. Nous nous sommes également interrogés sur la nécessité et la proportionnalité de l'obligation de publication des noms et des déclarations d'intérêt des experts, des membres des organes de décision, et des membres des organes responsables des procédures de recours.

3.8. Publication d'informations personnelles

3.8.1. Règlement relatif aux procédures d'insolvabilité

Le 27 mars 2013, nous avons adopté un avis sur la proposition de règlement de la Commission relatif aux procédures d'insolvabilité. Nous nous sommes réjouis des références que la proposition fait à l'applicabilité de la législation européenne en matière de protection des données. Nous avons cependant recommandé que les dispositions de fond soient plus claires en ce qui concerne la manière dont les principes de protection des données s'appliquent concrètement aux procédures d'insolvabilité, en particulier aux informations échangées entre parties prenantes et qui sont parfois aussi publiées.

Nous avons fait part de nos préoccupations en ce qui concerne la publication d'informations relatives à l'ouverture et à la clôture de procédures d'insolvabilité dans les registres d'insolvabilité qui sont accessibles au public, sur internet, gratuitement. Nous avons reconnu que l'objectif d'encourager la transparence et la communication entre les parties prenantes est légitime, mais avons toutefois considéré que cette méthode particulière de publication pose des risques spécifiques et porte atteinte à la vie privée.

Nous avons indiqué que la proportionnalité de cette mesure n'était pas prouvée étant donné que, contrairement à l'approche fixée dans l'arrêt Schecke, aucune option alternative, à savoir une méthode de publication différente qui serait moins attentatoire au droit de ces bénéficiaires au respect de leur vie privée, n'a été examinée. Nous avons entre autres conseillé que les responsables du traitement soient désignés, que des mises à jour des données échangées ou publiées soient effectuées, que la période de conservation des données trai-

tées soit précisée et que des procédures soient mises en place pour informer les personnes concernées du traitement de leurs informations personnelles.

3.9. Transports

3.9.1. Comptes rendus d'évènements dans l'aviation civile

Un événement est tout ce qui pourrait affecter la sécurité aérienne, y compris les accidents, les anomalies, les défauts et les autres problèmes liés au fonctionnement des avions. Afin que les comptes rendus soient plus exhaustifs et de meilleure qualité, la proposition présente, entre autres, un système de compte rendu volontaire pour compléter le système obligatoire et elle encourage les organisations - et pas uniquement les États membres - à notifier des événements. La proposition propose aussi une protection harmonisée en ce qui concerne les sanctions imposées par la hiérarchie ou les poursuites judiciaires visant les auteurs des comptes rendus et elle vise à garantir un accès adéquat aux informations contenues dans le répertoire central européen.

Dans notre avis du 10 avril 2013 sur la proposition de règlement de la Commission concernant les comptes rendus d'événements dans l'aviation civile, nous nous sommes réjouis de l'attention portée à la protection des données à caractère personnel, notamment par le biais de l'engagement «*d'anonymiser*» une majeure partie des données traitées. Nous avons cependant signalé que les dispositions prévues correspondent au mieux à une anonymisation partielle. Les données traitées gardent dès lors leur caractère personnel et restent soumises à l'applicabilité de la législation européenne sur la protection des données.

Nous avons recommandé de préciser plusieurs points du texte pour mieux protéger les données et les anonymiser complètement le cas échéant. Nous avons également conseillé que le responsable du traitement de chaque base de données soit clairement identifié, que la durée de conservation des données dans les bases de données soit précisée et que les droits des personnes concernées et les mesures de sécurité à mettre en œuvre soient mentionnés. Nous avons en outre recommandé d'adopter des garanties supplémentaires pour le transfert de données vers des pays tiers et le traitement de données sensibles.

3.9.2. Transport intelligent

Le 13 juin 2013, nous avons publié des observations formelles sur deux projets de règlement de la Commission dans le domaine des systèmes de transport intelligents qui étaient en cours d'examen par le Parlement européen et le Conseil. Ces projets d'instrument concernent la collecte et la mise à disposition de services d'information en matière de sécurité routière, un pour les informations générales sur la circulation, l'autre sur les possibilités de stationnement pour les camions.

Nous sommes heureux d'avoir été consultés lors du processus de rédaction et du fait que les éléments liés à la protection des données ont été pris en considération dans les projets de la Commission. À l'avenir, les systèmes d'information sur la circulation routière sont susceptibles de dépendre plus fortement d'informations collectées via la multitude de dispositifs mobiles qui seront installés dans les voitures ou transportés par leurs conducteurs, comme des téléphones portables dotés d'une fonction de localisation, des systèmes de navigation par GPS connectés et d'autres systèmes de transport intelligents, comme des caméras capables de reconnaître les numéros de plaques d'immatriculation.

Nous avons souligné l'importance de la protection des données lorsque nombre de données de trafic collectées concernent des personnes qui sont identifiées ou identifiables. Nous apprécions que ces considérations soient prises en compte dans les règlements, mais nous avons expliqué que des mesures comme l'anonymisation des données se compliquent alors que des données plus précises sont collectées (une *étude* sur les données de localisation a montré qu'il est possible d'identifier la localisation de personnes à partir d'un nombre très limité de périphériques d'information, sans autres informations). La combinaison de données dans les systèmes d'information sur la circulation,

y compris la réutilisation d'informations du secteur public (données ouvertes), doit dès lors toujours être mise en œuvre avec des mesures adéquates en matière de protection des données.

3.9.3. eCall

Le 29 octobre 2013, nous avons rendu un avis sur la proposition de règlement de la Commission concernant les exigences en matière de réception par type pour le déploiement du système eCall embarqué et modifiant la directive 2007/46/CE. Nous avons souligné la nature potentiellement intrusive du système eCall basé sur le numéro 112 et même si nous avons remarqué que de nombreuses garanties essentielles en matière de protection des données avaient été précisées dans la proposition, nous avons néanmoins insisté pour que des garanties complémentaires soient également incluses.

En outre, l'installation obligatoire de dispositifs eCall dans tous les nouveaux véhicules à compter du 1er octobre 2015 ne permettra pas uniquement le déploiement plus large et le fonctionnement du système eCall basé sur le numéro 112, mais fournira aussi une plate-forme de géolocalisation intégrée qui sera utilisée pour les services eCall privés et les services à valeur ajoutée. Nous avons souligné que tout traitement de données à caractère personnel par l'intermédiaire du système eCall embarqué devrait respecter la directive 95/46/CE. Nous avons dès lors regretté que les incidences en matière de protection des données des services eCall privés et des services à valeur ajoutée ne soient pas abordées dans la proposition. Nous avons demandé l'application de garanties équivalentes en matière de protection des données à ces services et avons précisé ces demandes dans notre avis.

3.10. Autres questions

3.10.1. Échanges automatiques d'informations fiscales

Le 5 novembre 2013, nous avons adopté des commentaires sur la proposition de la Commission en vue de modifier la directive relative à l'échange automatique et obligatoire d'informations dans le domaine fiscal. Dans notre courrier, nous avons donc instamment invité le législateur à préciser les types de données à caractère personnel qui peuvent être échangées au titre de la directive et à mieux définir les finalités et le contexte pour lesquels des données à caractère personnel peuvent être échangées. Nous avons également souligné que les principes de nécessité et de proportionnalité doivent être respectés dans la directive.

Nous avons par ailleurs observé que ni la directive actuelle ni la nouvelle proposition ne contiennent de dispositions expliquant comment le principe de transparence devrait être mis en œuvre dans la pratique, par exemple si (et comment) l'échange d'informations est communiqué au grand public ou comment les personnes concernées sont informées du traitement. Nous avons donc instamment invité le législateur à adopter une disposition traitant de la transparence des échanges d'informations proposés.

3.11. Stratégie du CEPD en matière d'accès aux documents

En tant qu'institution européenne et en vertu de son règlement intérieur, le CEPD est soumis au règlement (CE) n° 1049/2001 relatif à l'accès du public aux documents. Le nombre de demandes d'accès public à des documents détenus par le CEPD augmente progressivement chaque année. Plus précisément, ce nombre a récemment doublé, passant de 14 demandes en 2012 à 28 en 2013.

En 2013, nous avons traité quatre demandes confirmatives ou demandes d'examen interne de la décision initiale d'une institution de ne pas divulguer un document ou de ne le divulguer que partiellement. Il vaut la peine de mentionner que 11 de ces 28 demandes ont été reçues via le site d'Access Info: www.asktheeu.org. AsktheEU.org est un portail centralisé permettant de poser des questions aux organes publics de l'Union. Son objectif est de permettre au grand public de demander plus facilement des informations.

Nous traitons les demandes selon notre manuel relatif à l'accès aux documents que nous avons adopté en 2012. Ce manuel contient des orientations pour les membres du CEPD sur la manière de traiter les demandes d'accès public et il est révisé et mis à jour périodiquement. Conformément à ce manuel, nous avons également consacré une section de notre site internet à la politique de transparence du CEPD.

L'augmentation du nombre de demandes d'accès aux documents que nous recevons souligne la nécessité de disposer de lignes directrices plus

détaillées quant à la mise en œuvre concrète du règlement relatif à l'accès du public aux documents, en particulier concernant la divulgation de données à caractère personnel. Des réunions informelles de travail distinctes ont eu lieu entre le CEPD et la Commission européenne, le Parlement européen et le Conseil de l'UE. Lors de la réunion des DPD du 21 novembre 2013, ces institutions nous ont demandé de diriger l'organisation d'un atelier, auquel participera le Médiateur européen (qui détient une responsabilité spéciale en matière de transparence au sein de l'administration de l'Union), en vue de discuter de cette question et de concevoir des lignes directrices.

3.12. Affaires judiciaires

Aucune décision du CEPD n'a été contestée devant la Cour de justice de l'Union européenne en 2013, et nous n'avons intenté aucune action contre d'autres institutions ou organes de l'UE.

- **Digital Rights Ireland et Seitlinger et autres**

Le 9 juillet 2013, le CEPD a été invité à comparaître lors d'une audience devant la grande chambre de la Cour de justice dans le cadre d'une procédure de renvoi préjudiciel. Cette audition concernait des affaires jointes: C-293/12, Digital Rights Ireland et C-594/12, Seitlinger et autres. Ces deux affaires ont trait à la validité de la directive 2006/24/CE sur la conservation des données.

C'est la première fois que la Cour invitait le CEPD à comparaître à une audience dans le cadre d'une procédure de renvoi préjudiciel, pour répondre à des questions spécifiques, sur la base de l'article 24 de ses statuts. Dans nos conclusions, nous avons souligné la nécessité de faire la distinction entre l'article 7 (*respect de la vie privée et familiale*) et l'article 8 (*protection des données à caractère personnel*) de la Charte européenne des droits fondamentaux. Ces dispositions sont étroitement liées, mais sont très différentes de par leur nature. Pour déterminer la validité des actes juridiques en vertu de la Charte, la Cour doit dès lors appliquer un double critère, et évaluer si les exigences distinctes des articles 7 et 8 sont respectées.

Le 12 décembre 2013, l'avocat général Pedro Cruz Villalón a présenté ses conclusions dans ces affaires. Il a fait observer que la directive relative à la conservation des données poursuit une fin parfaitement légitime, à savoir garantir la disponibilité des données de trafic et de localisation aux fins de la recherche, de la détection et de la poursuite d'infractions graves. Il a cependant indiqué que la directive relative à la conservation des données constitue une

ingérence grave et injustifiée dans le droit fondamental des citoyens à la vie privée protégé par l'article 7 de la Charte européenne des droits fondamentaux. Il a fait observer en particulier que lorsqu'un acte établit une obligation qui constitue une telle ingérence, les législateurs européens auraient dû prévoir les garanties nécessaires plutôt que d'abandonner cette responsabilité aux États membres. Entre autres choses, le concept d'infractions graves aurait dû être décrit de manière plus précise et les principes de base gouvernant l'accès aux données collectées et leur utilisation auraient dû au minimum être fixés dans la directive elle-même.

Il s'agit, pour le CEPD, d'une étape importante qui pourrait engendrer une décision historique sur un sujet que nous suivons de près depuis un certain nombre d'années. Nous sommes curieux de voir si la Cour suivra le raisonnement de l'avocat général.

- **Commission c. Hongrie**

Le 15 octobre 2013, le CEPD a comparu au cours de l'audience dans l'affaire Commission c. Hongrie (affaire C-288/12). Cette affaire est la troisième procédure d'infraction relative à l'indépendance des autorités chargées de la protection des données, les deux autres étant: Commission c. Autriche (C-614/10) et Commission c. Allemagne (C-518/07), dans le cadre desquelles des décisions ont été rendues en 2012 et 2009 respectivement. Dans nos conclusions, nous avons indiqué que la Hongrie n'avait pas rempli ses obligations afin de garantir que l'autorité de contrôle nationale agit en complète indépendance. Une modification de la législation ne peut en elle-même justifier la fin du mandat de l'autorité de contrôle. Le fait que les modifications aient eu lieu au niveau constitutionnel ne devrait pas faire obstacle à la primauté du droit européen. La décision est attendue au début de l'année 2014.

Les autres affaires dans lesquelles le CEPD est intervenu sont toujours pendantes.

- **Pachtitis c. Commission et EPSO (T-374/07) et Pachtitis c. Commission (F-35/08)**

Le demandeur, Pachtitis, a demandé l'annulation de la décision dans laquelle EPSO a rejeté sa demande d'accès aux questions d'examen du concours général (EPSO/AD/77/06) auquel il avait participé. Le CEPD est intervenu en faveur du demandeur, en alléguant que les questions sont une partie intégrale de ses données à caractère personnel et que dès lors y refuser l'accès engendre une violation de l'obligation d'appliquer le règlement (CE) n° 45/2001 en vigueur.

En décembre 2011, le Tribunal a contacté les parties pour leur demander si «les intérêts légitimes» du demandeur doivent être revus dans cette affaire à la lumière de l'arrêt rendu dans l'affaire T-361/10P[7]. Nous estimons que la demande de M. Pachtitis en vue d'avoir accès aux questions reste légitime.

- **ZZ c. BEI (affaire F-103/11)**

Au cours d'une enquête interne pour harcèlement menée par la BEI, la plainte complète concernant le harcèlement allégué, y compris les documents joints (parmi lesquels des déclarations médicales) a été envoyée aux harceleurs présumés. Le demandeur a déclaré devant le Tribunal de la fonction publique que cette pratique était contraire au règlement (CE) n° 45/2001.

En juin 2012, le CEPD a présenté une intervention écrite en faveur du demandeur, dans la mesure où la demande était fondée sur une violation présumée des règles relatives à la protection des données.

- **Dennekamp c. Parlement européen**

Le CEPD a récemment soumis des arguments écrits dans l'affaire «Dennekamp II», (affaire T-115/13, Dennekamp c. Parlement européen), qui concerne la nécessité de trouver un équilibre approprié entre l'accès public et la protection des données. Le demandeur, un journaliste néerlandais, a demandé une série de documents contenant des informations sur l'adhésion des députés européens au régime de retraite volontaire (y compris une liste de noms) du Parlement européen. Dans l'affaire «Dennekamp I», le Tribunal a donné raison au Parlement, considérant que le défendeur n'avait pas fourni de justifications explicites légitimes pour prouver qu'il était nécessaire que les informations lui soient transférées.

Dans nos conclusions écrites dans l'affaire Dennekamp II, nous avons abordé la nécessité du transfert pour des raisons étroitement liées à l'intérêt général de la transparence. Le CEPD considère qu'accepter cette nécessité n'équivaut pas à accorder un droit d'accès spécial aux journalistes, mais refléterait simplement le rôle unique des journalistes en tant qu'observateurs publics. En reconnaissant l'importance du droit à la liberté d'expression dans une société démocratique, nous soutenons que, dans les situations comme celle-ci, l'équilibre entre les différents intérêts en jeu devrait être en faveur de l'ouverture.

7 Dans son arrêt du 14 décembre 2011 dans l'affaire T-361/10P, le Tribunal a indiqué que «l'intérêt légitime du demandeur doit être examiné tant à la lumière du jour de la demande que du jour de l'audience». Le Tribunal a indiqué que «l'intérêt légitime pourrait être éliminé au cours du processus en raison de motifs objectifs ou subjectifs».

En octobre 2013, le CEPD a demandé l'autorisation d'intervenir dans deux affaires:

- **Elmaghraby et El Gazaerly c. Conseil de l'Union européenne (affaire T-319/13)**

Dans cette affaire, les demandeurs ont demandé au Tribunal d'annuler une décision du Conseil concernant des mesures restrictives contre certaines personnes, entités et organes en raison de la situation en Égypte et d'effacer les allégations selon lesquelles chaque demandeur est responsable de détournement de fonds étatiques et est soumis à une enquête judiciaire en Égypte. Les demandeurs ont allégué une violation des règles relatives à la protection des données en vertu de la directive 95/46/CE relative à la protection des données et du règlement (CE) n° 45/2001.

Le CEPD considère que cette affaire est l'occasion d'évaluer les défis en matière de protection des données soulevés par les mesures restrictives adoptées par les institutions européennes.

- **CN c. Parlement (affaire T-343/13)**

Le demandeur cherche à obtenir des dédommagements pour les dommages matériels et non matériels qu'il a subis à la suite de la publication, sur le site internet du Parlement européen, d'un extrait d'une pétition qu'il a présentée et contenant des informations personnelles (y compris son état de santé et le fait que sa famille compte une personne handicapée). Le CEPD a demandé l'autorisation d'intervenir en faveur du demandeur.

3.13. Priorités pour 2014

En décembre 2013, le CEPD a publié son septième 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.

Les principales tendances suivantes ont été considérées comme étant prédominantes pour 2014.

1. Le débat qui a suivi les révélations en matière de surveillance de masse a mis davantage en lumière les pratiques des deux côtés de l'Atlantique. Dans ce contexte, le renforcement du respect de la vie privée et de la protection des données en tant que droits fondamentaux a pris une priorité encore plus importante dans l'ordre du jour politique de l'Union. La protection des données est mentionnée comme étant un sujet essentiel des débats de préparation en vue de l'établissement d'un accord de libre-échange entre l'Union européenne et les États-Unis, et l'accord sur la sphère de sécurité entre l'Union européenne et les États-Unis est en cours de révision. En particulier, le débat engendré par les révélations concernant les programmes mis en place par les services de renseignements étrangers et européen a contribué à sensibiliser le grand public au respect de la vie privée et à la protection des données, une tendance qui encourage le CEPD à fournir de nouvelles orientations et contributions au législateur européen et aux autres parties prenantes. Comme première étape, nous réagirons à la communication de la Commission du 27 novembre 2013 intitulée «Restaurer la confiance dans les flux de données entre l'Union européenne et les États-Unis», en prenant également en considération les résultats de l'enquête de la commission LIBE portant sur la surveillance électronique de masse des citoyens européens.
2. Il existe une tendance croissante à doter les autorités administratives, à la fois au niveau de l'UE et au niveau national, de puissants outils d'enquête et de collecte d'information. Cela concerne particulièrement l'espace de liberté, de sécurité et de justice et la révision du cadre législatif concernant la surveillance financière. Dans ce contexte, l'importance croissante du contrôle de l'internet par les autorités publiques et par des parties privées doit être envisagée avec soin par rapport aux irrégularités commises sur l'internet.
3. Une énorme quantité d'informations personnelles est échangée chaque jour sur l'internet. Des volumes de données à caractère personnel sont collectés par des entreprises pour préserver et renforcer les relations existantes avec leurs clients et pour nouer de nouvelles relations. Ces données à caractère personnel peuvent être vendues à d'autres parties intéressées et sont en effet devenues des actifs incorporels qui n'apparaissent pas dans les bilans de sociétés. L'utilisation ultérieure de ces masses d'informations à des fins répressives pourrait aussi avoir lieu. En raison de ces évolutions, les questions comme le lien entre la protection des données et la législation en matière de concurrence sont de plus en plus importantes. À la suite de notre avis sur l'informatique en nuage, nous envisageons de publier un avis sur le rôle de la protection des données dans la législation européenne en matière de concurrence et nous envisageons de continuer nos travaux dans les domaines

de la circulation massive de données («Big Data») et des données en tant que monnaie.

4. La législation de l'UE facilite de plus en plus d'importants échanges d'informations entre les autorités nationales, impliquant souvent des organes de l'UE et des bases de données à grande échelle (avec ou sans unité centrale) d'une taille et d'une puissance de traitement croissantes. Cette tendance se poursuivra probablement en 2014 dans le cadre du nouveau programme dans le domaine de la liberté, de la sécurité et de la justice (post-Stockholm). Cela nécessite dès lors un examen minutieux de la part des décideurs et des acteurs lors de la définition des exigences de protection des données dans le cadre de la procédure législative, en raison des conséquences importantes que ces échanges peuvent avoir sur la protection de la vie privée des citoyens, par exemple en facilitant la surveillance de leur vie.
5. Afin d'alléger la charge fiscale imposée aux citoyens européens par la crise financière, les États membres coordonnent de plus en plus leur action contre la fraude et l'évasion fiscales au niveau européen, en renforçant l'efficacité des outils en matière de coopération administrative dans le secteur fiscal - comme cela a été le cas lors du G20 et les initiatives prises contre le secret bancaire. Parallèlement, l'Union a entamé des négociations avec des pays tiers en vue de conclure des accords internationaux visant à lutter contre la fraude à la TVA, grâce à l'échange d'informations fiscales. Bien que justifiables pour des motifs impérieux d'intérêt public, ces initiatives doivent être alignées avec les règles en matière de protection des données, en particulier avec le principe de la proportionnalité. Elles figureront parmi les premières priorités du CEPD en 2014.

Le CEPD s'engage à consacrer des ressources considérables en 2014 à l'analyse des propositions d'importance stratégique. Le CEPD a également recensé plusieurs initiatives de moindre importance stratégique qui peuvent néanmoins être pertinentes pour la protection des données. Le fait que ces initiatives figurent dans l'inventaire du CEPD implique qu'elles seront régulièrement surveillées, mais pas nécessairement 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:

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

b. Rétablir la confiance dans les flux mondiaux de données à la suite de PRISM
   - Suivi de la communication de la Commission du 27 novembre 2013 intitulée «Restaurer la confiance dans les flux de données entre l'Union européenne et les États-Unis»
   - Révision de la mise en œuvre de l'accord sur les dossiers passagers
   - Analyse du fonctionnement de la sphère de sécurité

c. Initiatives visant à stimuler la croissance économique et la stratégie numérique
   - Marché unique en matière de télécommunications (par exemple, les droits de propriété intellectuelle, la sécurité des réseaux et de l'information, la protection des données)
   - Propositions en matière de marchés publics, santé en ligne, données ouvertes
   - Révision des règles en matière de concurrence
   - Cybersécurité
   - Informatique en nuage

d. Développement de l'espace de liberté, de sécurité et de justice
   - Post-programme de Stockholm
   - Réforme d'agences et d'organes (par exemple Eurojust, OLAF, Parquet européen)
   - Initiatives contre le terrorisme et l'extrémisme
   - Négociations portant sur des accords avec des pays tiers en matière de protection des données

e. Réforme du secteur financier
   - Réglementation et supervision des marchés et acteurs financiers
   - Surveillance bancaire

f. Fraude fiscale et secret bancaire
   - Passage à un système de TVA définitif
   - Négociations portant sur des accords avec des pays tiers sur l'échange d'informations relatives à la TVA
   - Secret bancaire

4 COOPÉRATION

Notre objectif stratégique

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

Nos principes directeurs

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

4.1. Groupe de travail «Article 29»

Le groupe de travail «Article 29» sur la protection des données (groupe de travail «Article 29») est un organe consultatif indépendant institué par l'article 29 de la directive 95/46/CE. Il est composé de représentants des autorités nationales chargées de la protection des données, du CEPD et de la Commission. 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.

En 2013, nous avons continué de contribuer activement aux travaux du groupe de travail «Article 29», en particulier par notre participation aux sous-groupes thématiques tels que: Frontières, déplacements et application de la loi, Administration en ligne, Questions financières, Avenir du respect de la vie privée, Transferts internationaux, Dispositions clés et Technologie.

Nous avons en particulier participé en tant que rapporteur ou co-rapporteur aux avis relatifs à la limitation de la finalité[8] et à l'intérêt légitime (sous-groupe «Dispositions clés»). Ce sous-groupe s'est vu confier par la plénière la rédaction d'avis importants sur l'interprétation des principes essentiels de la directive relative à la protection des données, en vue de fournir une interprétation cohérente des règles et recommandations existantes pour la réforme à venir du cadre européen en matière de protection des données.

Nous avons également considérablement contribué à la rédaction de deux avis sur le modèle d'analyse d'impact relative à la protection des données pour les réseaux intelligents[9] (sous-groupe «Tech-

8 Avis 03/2013 sur la limitation de la finalité - GT 203.

9 Avis 04/2013 et avis 07/2013 sur le modèle d'analyse d'impact relative à la protection des données pour les réseaux intelligents et les systèmes de relevés intelligents (modèle d'AIPD) élaboré par le groupe d'experts 2 de la task-force sur les réseaux intelligents de la Commission - GT 205 et GT 209.

nologie») et de l'avis relatif aux données ouvertes[10] (sous-groupe «Administration en ligne»).

En 2013, en plus de contribuer aux discussions en cours sur le profilage, nous avons consacré des ressources significatives au suivi des avis et des documents de travail suivants:

- discussions sur la réforme de la protection des données (actes d'exécution)[11]
- orientations sur l'obligation de consentement pour certains cookies[12]
- applications destinées aux dispositifs intelligents[13]
- applications mobiles.

Nous avons également contribué de manière significative à plusieurs analyses et courriers relatifs aux révélations de Snowden et à la surveillance mondiale, aux accords sur les données passagers, aux données relatives aux informations préalables sur les passagers, à la nouvelle capacité de distribution de l'AITA, à l'accès transfrontalier aux données dans le cadre de la cybercriminalité, aux règles d'entreprise contraignantes et aux questions relatives à la lutte contre le blanchiment de capitaux.

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

4.2. Supervision coordonnée

La coopération directe avec les autorités nationales est de plus en plus importante dans le cadre du développement de bases de données internationales à grande échelle comme EURODAC, le système d'information sur les visas (VIS), le système d'information Schengen II (SIS II) et le système d'information douanier (SID), qui nécessitent d'une approche coordonnées de la supervision.

En 2013, nous avons fourni les services de secrétariat pour le groupe de coordination du contrôle du nouveau SIS II (SCG) et nous avons présidé les groupes de coordination du contrôle d'EURODAC, du VIS et du CIS.

Les changements intervenus en 2013 ont été accompagnés de défis concernant la supervision coordonnée. Le nouveau règlement EURODAC[14] contenait des modifications significatives, comme l'éventuel accès aux données EURODAC par les autorités répressives. En outre, le système SIS II est devenu opérationnel. Afin de réduire les charges financières et administratives et de réduire les déplacements, nous avons établi des réunions groupées des groupes de coordination du contrôle visant à garantir des politiques de contrôle des systèmes d'information à grande échelle qui soient cohérentes et horizontales, le cas échéant.

Le modèle des groupes de coordination du contrôle s'élargira en 2014 grâce à un nouveau groupe de coordination du contrôle pour le système d'information du marché intérieur (IMI)[15]. Nous avons dès lors consulté les autorités nationales chargées de la protection des données et la Commission en 2013 afin de faire le point sur le statut et l'évolution du règlement IMI afin d'organiser la première réunion du groupe en 2014.

Le modèle de supervision coordonnée est devenu une norme pour le législateur de l'Union et la Commission a suggéré que ce modèle soit utilisé dans plusieurs propositions telles que celles sur Europol, sur les frontières intelligentes, sur Eurojust et sur le Parquet européen.

10 Avis 06/2013 sur la réutilisation des informations du secteur public (ISP) et des données ouvertes - GT 207.

11 Document de travail 01/2013 - Contribution au débat sur les propositions d'actes d'exécution - GT 200.

12 Document de travail 02/2013 énonçant des lignes directrices sur le recueil du consentement pour le dépôt de cookies - GT 208 (2.10.2013).

13 Avis 02/2013 sur les applications destinées aux dispositifs intelligents - GT 202.

14 Règlement (UE) n° 603/2013 du Parlement européen et du Conseil du 26 juin 2013 relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) n° 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) n° 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (refonte), (JO L 180/1, du 29.6.2013)

15 Règlement (UE) n° 1024/2012 du Parlement européen et du Conseil du 25 octobre 2012 concernant la coopération administrative par l'intermédiaire du système d'information du marché intérieur et abrogeant la décision 2008/49/CE de la Commission (JO, L 316/1).

4.2.1. EURODAC

EURODAC est le 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.16

Nous avons organisé deux réunions à Bruxelles pour le groupe de coordination du contrôle d'EURODAC, l'une en avril et l'autre en novembre 201317. Le groupe, composé de représentants des autorités nationales chargées de la protection des données et du CEPD, a fondé ses activités sur ce programme de travail 2013-2014.

Le groupe de coordination du contrôle d'EURODAC a établi son programme de travail pour 2013-2014. Ce programme se concentre sur la nécessité de superviser la transition vers les règles EURODAC qui entreront en vigueur en juin 2015 en vertu des nouvelles dispositions relatives à EURODAC18. Le groupe a également partagé des informations relatives à des inspections nationales dans différents États membres et la Commission l'a informé des évolutions récentes.

Rapport sur les empreintes digitales illisibles[19]

Fondé sur l'analyse des réponses reçues, le rapport contient plusieurs recommandations adressées aux autorités compétentes des États membres en vue d'établir des procédures claires et contraignantes.

Ces recommandations devraient permettre aux demandeurs d'asile de profiter de mesures harmonisées au sein de l'Union (pour éviter les possibilités de discrimination). Les procédures devraient préciser que les empreintes digitales illisibles ne peuvent pas être utilisées en elles-mêmes contre les demandeurs, mais que toute conséquence négative pour les demandeurs doit être justifiée par des preuves suffisantes.

L'une des recommandations des bonnes pratiques est d'obliger les autorités compétentes des États membres à relever une nouvelle fois les empreintes digitales après un certain délai (par exemple, deux semaines) afin de permettre aux stries de se régénérer et, si possible, de faire participer à la procédure un spécialiste en médecine légale ou un opérateur technique. Afin de réduire les charges administratives et le stress qui y est lié, il convient d'établir un délai minimum commun avant de relever à nouveau les empreintes digitales. Cela profitera aux demandeurs d'asile ainsi qu'aux autorités nationales. Il convient aussi de décider si, lorsqu'il est détenu, le demandeur doit être informé du fait que ses empreintes digitales seront relevées à nouveau.

Il convient également de veiller à garantir aux demandeurs d'asile le droit de déposer une plainte contre les autorités nationales pertinentes voire les autorités de contrôle nationales en matière de protection des données.

La prochaine réunion du groupe de coordination du contrôle d'EURODAC aura lieu au printemps 2014.

4.2.2. VIS

Le système d'information sur les visas (VIS) est une base de données contenant des informations, dont des données biométriques, sur les demandes de visas par les ressortissants des pays tiers. Ces informations sont collectées lorsqu'une demande de visa est introduite auprès d'un consulat de l'UE et

16 Islande, Norvège, Suisse et Liechtenstein.

17 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/13-10-16_Eurodac_SCG_Summary_EN.pdf

18 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:180:0001:0030:FR:PDF

19 https://secure.edps.europa.eu/EDPSWEB/edps/cache/off/Supervision/Eurodac

servent à empêcher la fraude en matière de visas ainsi que les demandes de visas multiples dans les divers États membres («visa shopping»), à faciliter l'identification des détenteurs de visas au sein de l'Union européenne et à vérifier que le demandeur et l'utilisateur du visa sont la même personne. Le VIS a été déployé sur une base régionale et est d'abord devenu opérationnel en Afrique du Nord le 11 octobre 2011. Le VIS a depuis lors été mis en œuvre dans huit autres régions.[20]

Le groupe de coordination du contrôle du VIS est composé de représentants des autorités nationales chargées de la protection des données et du CEPD. Nous avons organisé deux réunions relatives au groupe de coordination du contrôle du VIS à Bruxelles, l'une en avril et l'autre en novembre 2013[21]. Il s'agissait de réunions groupées avec les groupes de coordination du contrôle d'EURODAC et du SIS II.

Le groupe de coordination du contrôle du VIS a adopté son règlement intérieur et son programme de travail pour 2013-2014. Le programme de travail est axé sur le renforcement de la coopération en matière d'inspections en établissant un format commun pour les inspections nationales ainsi que sur l'étude de la coopération entre les États membres et les fournisseurs externes et de la manière dont la protection des données est appliquée dans le traitement des demandes de visas.

20 http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/borders-and-visas/visa-information-system/index_en.htm

21 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/SupervisionVIS/13-10-16_VIS_SCG_Summary_EN.pdf

Plusieurs membres du groupe ont été chargés de commencer des travaux sur une étude sur la coopération entre les États membres et les fournisseurs externes et de discuter des perspectives à long terme du contrôle du VIS.

Les membres du groupe de coordination du contrôle du VIS ont aussi échangé des informations sur les inspections nationales dans les différents États membres. Le groupe a été informé par la Commission de l'évolution du déploiement du VIS et des autres évolutions ayant des incidences sur la protection des données.

La prochaine réunion du groupe de coordination du contrôle du VIS aura lieu au printemps 2014. Il s'agira d'une réunion groupée avec les groupes de coordination du contrôle des autres systèmes informatiques à grande échelle (EURODAC et SIS II).

4.2.3. SID

Le système d'information douanier (SID) a pour objectif de créer un système d'alerte dans le cadre de la lutte antifraude afin de permettre aux États membres 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 dans le système.

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 (ACC) composée de représentants des autorités nationales chargées de la protection des données.

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

Ce groupe de coordination:

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

En 2013, nous avons organisé deux réunions à Bruxelles pour le groupe de coordination du contrôle du SID.

La sixième réunion du groupe de coordination du contrôle du SID s'est tenue en juin 2013. Étant donné que les mandats du président et du vice-président étaient arrivés à terme, un vote à bulletin secret a été organisé. M. Giovanni Buttarelli, président du groupe, et M. Gregor König, vice-président du groupe, ont tous deux été réélus.

Le groupe a également étudié le projet de rapport sur l'inspection coordonnée de la liste des autorités ayant accès au SID et au FIDE et le projet de rapport sur les droits des personnes concernées dans le SID.

Lors de la réunion de décembre 2013, en raison du départ du vice-président Gregor Konig, un nouveau vice-président a été élu. Nous avons informé le groupe quant à l'inspection du SID. La Commission a présenté les évolutions récentes concernant le règlement (CE) n° 515/97 du Conseil: sur les évolutions techniques du SID et, en particulier, sur l'état d'avancement de la publication de la liste des autorités ayant accès au SID/FIDE. Le groupe a réfléchi aux éventuels sujets à intégrer dans le programme de travail pour 2014-2015.

22 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.

4.2.4. Système d'information Schengen (SIS II)

Le système d'information Schengen (SIS) est un système d'information à grande échelle créé à la suite de l'abolition des contrôles aux frontières intérieures de l'espace Schengen. Le SIS permet aux autorités compétentes des États membres d'échanger des informations sur la réalisation de contrôles sur des personnes et objets aux frontières extérieures ou sur le territoire, ainsi que pour la délivrance de visas et de permis de résidence.

Le système d'information Schengen de deuxième génération (SIS II) est devenu opérationnel en mai 2013 et il a dès lors remplacé le SIS susmentionné. Il s'agit d'une base de données centrale, dénommée Système central d'information Schengen (C-SIS). La Commission est responsable de la gestion opérationnelle de cette base de données, connectée aux points d'accès nationaux définis par chaque État membre (NI-SIS).

Le groupe de coordination du contrôle du SIS II est constitué d'une plate-forme pour les autorités chargées de la protection des données responsables du contrôle du SIS en vertu du règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération et de la décision 2007/533/JAI du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération. Le CEPD et les autorités nationales chargées de la protection des données collaborent dans le respect de leurs priorités afin de garantir le contrôle coordonné du SIS.

Ce groupe de coordination:

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

En avril 2013, le groupe de coordination du contrôle du SIS II a pris le relais de l'autorité de contrôle commune du SIS. Sa première réunion s'est tenue en juin et sa deuxième en octobre, toutes deux à Bruxelles. Lors de la réunion de juin, des questions administratives figuraient à l'ordre du jour: l'élection d'un président et d'un vice-président, lors de laquelle Mme Clara Guerra, représentant l'APD du Portugal, et M. David Cauchi, représentant l'APD de Malte, ont été élus; l'adoption du règlement intérieur du groupe et la reconnaissance du statut d'observateur de la Bulgarie, de Chypre, de l'Irlande, de la Roumanie et du Royaume-Uni.

Des questions plus importantes ont également été abordées comme le piratage du NI-SIS danois, l'avancement de la procédure d e migration du SIS et une campagne d'information sur le SIS II. Les participants à cette réunion ont également abordé des mesures futures que la Commission et eu-LISA devront prendre concernant la politique de sécurité du SIS II en particulier et les activités futures du groupe de coordination du contrôle pour 2013-2014.

Lors de la réunion d'octobre, le groupe a une nouvelle fois abordé le piratage du NI-SIS danois et la participation nécessaire du groupe de coordination du contrôle du SIS II au suivi de cet incident. La Commission s'est vu souligner ce point; elle participait à la réunion pour présenter les résultats des travaux du sous-groupe «Sécurité» du SIS II qu'elle a constitué à la suite du piratage.

Le projet de programme de travail du SIS II a également été abordé par le groupe ainsi qu'une possibilité de cadre pour les audits commun aux groupes de coordination du contrôle du SIS II, du VIS et d'EURODAC et la création d'un sous-groupe d'experts commun à ces groupes.

4.3. Conférence européenne

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

En 2013, la conférence européenne des commissaires à la protection des données a eu lieu à Lisbonne les 16 et 17 mai. Elle était axée sur plusieurs thèmes liés aux évolutions récentes dans la modernisation des cadres de protection des données de l'Union, du Conseil de l'Europe et de l'Organisation de coopération et de développement économiques (OCDE). Les discussions ont plus particulièrement porté sur les notions de données à caractère personnel, de droits des personnes sur l'internet et de sécurité des informations.

La conférence a également abordé la question de savoir comment renforcer la supervision et la coopération des autorités chargées de la protection des données, la cohérence en ce qui concerne le rôle et les compétences des autorités chargées de la protection des données et comment elles pourraient mieux coopérer et assurer la direction.

Cette conférence a adopté trois résolutions, une sur l'avenir de la protection des données en Europe, une autre sur la protection des données dans une zone de libre-échange transatlantique et la troisième sur un niveau adéquat de protection au sein d'Europol.

4.4. Conférence internationale

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

La 35e conférence annuelle des commissaires à la protection des données et à la protection de la vie privée s'est tenue à Varsovie du 22 au 26 septembre 2013. Cette conférence s'est principalement concentrée sur les réformes en matière de protection des données mises en place partout dans le monde (en particulier, au sein de l'Union, du Conseil de l'Europe et de l'OCDE), sur l'interaction avec les technologies ainsi que sur les rôles et perspectives de différents acteurs, y compris les personnes concernées, les responsables du traitement et les autorités de contrôle. Peter Hustinx, contrôleur, et Giovanni Buttarelli, contrôleur adjoint, faisaient partie des orateurs.

Lors de cette conférence, une série de résolutions ont été adoptées, y compris celles sur l'«appification» de la société, sur le profilage et sur la coordination de la mise en application au niveau international.

La coordination de la mise en application au niveau international a été abordée lors de la conférence précédente qui avait lieu en Uruguay et son importance a été confirmée par les travaux en cours du groupe de travail sur la coordination de la mise en application (IEWG), chargé de trouver des points communs en vue de la coopération entre les autorités de contrôle du monde entier. Nous participons à ce groupe de travail et nous contribuons à l'analyse des options pour la coopération en matière de mise en application et des obstacles existant dans ce domaine. La prochaine conférence en la matière aura lieu les 3 et 4 avril 2014 à Manchester.

En outre, une résolution a été adoptée sur l'ancrage de la protection des données et de la protection de la vie privée dans la législation internationale. Cette résolution constitue une réaction aux révélations de la surveillance mondiale par les services de renseignements américains au cours de l'été, afin de veiller à la reconnaissance de ces valeurs fondamentales au niveau international.

De nombreuses manifestations connexes ont été organisées avant ou parallèlement à cette conférence, comme par exemple la conférence Public Voice, avec la participation de la société civile, et la conférence Phaedra consacrée au développement de la coopération en matière de mise en application au niveau international.

La 36e conférence internationale aura lieu à l'Ile Maurice, en octobre 2014.

4.5. Autres coopérations internationales

4.5.1. Conseil de l'Europe

La Convention du Conseil de l'Europe pour la protection des données (Convention 108) de 1981 est l'instrument international contraignant le plus ancien en la matière et il a également inspiré la directive 95/46/CE. Elle vise à renforcer la protection des données pour les particuliers à la lumière de la communication transfrontalière croissante de données dans le cadre des processus automatisés. En notre qualité d'observateur habilité à intervenir, nous avons assisté à deux réunions du Comité consultatif de la convention 108, l'une en mai et l'autre en octobre 2013. Il était particulièrement important pour nous de participer à ces réunions afin de pouvoir suivre et participer à la modernisation en cours de la Convention.

Depuis l'adoption du protocole modifiant la Convention, lors de la réunion du Comité consultatif de la Convention pour la protection des personnes en ce qui concerne le traitement automatisé des données à caractère personnel (T-PD) de novembre 2012, nos observations sont axées sur le rapport explicatif. Nous avons également participé en tant qu'observateur aux réunions du comité ad hoc sur la protection des données (CAHDATA) qui approfondit les travaux du T-PD au niveau ministériel. Nous avons formulé des observations visant à renforcer la protection des données en harmonisant le texte proposé de façon à assurer la cohérence interne de la Convention et celle du futur cadre européen en matière de protection des données.

Outre le suivi des travaux du T-PD et du CAHDATA, nous avons participé aux discussions du comité de la Convention sur la cybercriminalité. En tant que rapporteur, nous avons contribué à des observations écrites sur l'éventuelle révision de la Convention sur la cybercriminalité transmise par le groupe de travail «Article 29» au bureau du comité. Nous

avons aussi suivi les travaux du comité de pilotage «Médias et société de l'information» (CDMSI).

4.5.2. OCDE

Nous avons participé aux travaux du groupe d'experts chargé de mettre à jour les lignes directrices de l'OCDE sur la protection de la vie privée (Groupe de volontaires sur la vie privée - Groupe de travail sur la sécurité de l'information et la vie privée). Ce groupe d'experts, présidé par la commissaire à la protection de la vie privée du Canada, Jennifer Stoddart, était composé de représentants de gouvernements, d'autorités chargées de l'application des législations protégeant la vie privée, d'universitaires, de l'industrie, de la société civile et de la communauté technique de l'internet.

En tant que membres de ce groupe, nous avons participé à plusieurs réunions et avons contribué par des observations écrites au projet de mise à jour des lignes directrices. Parmi les sujets abordés figuraient le renforcement du rôle des autorités de contrôle, la responsabilité des responsables du traitement et l'amélioration de la sécurité juridique en ce qui concerne les transferts de données. Les lignes directrices révisées ont été adoptées le 11 juillet 2013[23].

4.5.3. CEAP

Les 21 pays de la Coopération économique Asie-Pacifique (CEAP), dont les États-Unis, le Canada, le Japon, la Chine, la Russie, la Corée du Sud et l'Australie, ont mis au point un système de règles transfrontalières de protection de la vie privée (CBPR) en vue de protéger la vie privée et de garantir les transferts de données.

Ces règles sont similaires à certains égards aux règles d'entreprise contraignantes (BCR) qui sont utilisées pour les transferts de données au sein de l'Union. Par exemple, ces deux types de règles s'appliquent aux transferts internationaux développés par les entreprises et sont d'abord révisées par les autorités chargées de la protection des données ou par des tiers autorisés.

Le groupe de travail «Article 29» a suivi de près l'évolution des CBPR et, de concert avec les pays de la CEAP, il a analysé l'adoption possible d'une référence commune pour l'industrie, soulignant les similitudes et les divergences entre les deux systèmes. Dans ce contexte, en 2013, nous avons considérablement contribué aux discussions et aux travaux de rédaction du sous-groupe de la CEAP consacré à la protection de la vie privée et aux réunions UE-CEAP visant une «certification» double pour les procédures de respect des CBPR et des BCR.

4.5.4. Association Francophone (AFAPDP)

Les objectifs principaux de l'Association francophone des autorités de protection des données personnelles sont: le lancement d'un débat sur les défis en matière de protection des données dans les régions francophones, ainsi que la création d'un réseau visant l'échange et la coopération entre les autorités indépendantes de protection des données.

L'une de nos contributions aux réunions annuelles de l'Association a été d'expliquer le cadre européen aux pays où la législation relative à la protection

23 Les lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

des données est en cours d'élaboration, comme le Maroc et le Burkina Faso. L'an dernier, la réunion de l'Association a eu lieu à Marrakech les 20 et 21 novembre 2013.

4.5.5. Groupe de Berlin

Le groupe de travail international sur la protection des données dans les télécommunications (IWG-DPT, aussi connu sous le nom «Groupe de Berlin») est composé d'experts en protection des données et en protection de la vie privée originaires d'Europe, des Amériques et d'Asie ainsi que d'experts en la matière provenant du secteur de l'industrie.

Nous participons aux réunions de ce groupe et contribuons aux documents qu'il prépare. En 2013, ces documents ont inclus des documents de travail sur le suivi et l'indexation sur l'internet et sur les drones de surveillance aérienne. Un document de travail sur le droit au respect de la vie privée dans le domaine des télécommunications a servi de base à une résolution présentée lors de la conférence internationale.

5 SUIVI DE LA TECHNOLOGIE

Notre objectif stratégique

Évaluer les risques liés à la vie privée induits par l'utilisation des nouvelles technologies en collectant et en analysant les informations appropriées.

5.1. Évolution technologique et protection des données

En 2012, nous avons ajusté notre structure organisationnelle interne et créé une équipe «Politique IT» afin de disposer des connaissances et de l'expertise nécessaires et de renforcer notre aptitude à suivre les évolutions technologiques. L'année 2013 a été la première année complète d'activité de l'équipe, au cours de laquelle elle a évalué les impacts de l'évolution technologique sur la protection des données et le respect de la vie privée. Ce suivi continu nous a permis de développer et de maintenir les connaissances nécessaires pour exercer correctement les tâches de supervision, de consultation et de coopération qui exigent une analyse technique.

L'équipe «Politique IT» examine également en profondeur les choix qu'il convient d'opérer pour nos propres besoins informatiques, afin de garantir que nous suivons nos propres recommandations, mais également que nous appliquons les meilleures pratiques en matière de protection des données.

L'un des principaux problèmes dans l'évolution de la technologie internet est que les développeurs de nouveaux services, outils et standards reçoivent actuellement peu de conseils de la part des experts de la protection des données sur la manière de mettre en œuvre des solutions respectueuses de la vie privée. Une discussion plus vaste sur l'approche technique à adopter à l'égard de la vie privée pourrait permettre d'expliquer les principes aux développeurs et d'explorer les options pour intégrer systématiquement la protection des données lors du processus de développement, et aider les programmeurs à comprendre comment ils peuvent intégrer le principe de la protection de la vie privée dès la conception dans l'exercice pratique de leurs fonctions.

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

Le renforcement de nos contacts avec les experts en technologie dans les organes de l'Union sous notre supervision, ainsi que dans le secteur privé, le milieu universitaire et d'autres secteurs, pourrait donc contribuer à améliorer le soutien technique en matière de protection des données et présenter les options techniques aux experts de la vie privée. À titre d'exemple, les travaux préparatoires sur nos lignes directrices pour les sites internet et l'utilisation d'appareils mobiles ont déjà conduit à des discussions plus ciblées sur des questions spécifiques sur les aspects techniques et de la protection des données.

La participation à ces discussions et la promotion de technologies respectueuses de la vie privée, en coopération avec d'autres autorités responsables de la protection des données, resteront des domaines d'activité importants.

Ce chapitre présente les observations résultant de notre suivi de la technologie et met en évidence certains développements intéressants pour le respect de la vie privée et la protection des données

5.2. Sécurité et surveillance de l'internet

La sécurisation de l'internet fait l'objet d'un effort permanent depuis sa création; la nature changeante d'internet (taille et utilisation) ainsi que des menaces, garantit que la sécurité continuera de préoccuper les différentes communautés. Cependant, les derniers rapports sur la surveillance généralisée du trafic internet en ont surpris plus d'un, étant donné que son ampleur n'avait pas été prévue dans la conception de nombreux protocoles internet. Ces révélations ont montré que de nombreuses pratiques appliquées à l'heure actuelle renforcent la vulnérabilité des utilisateurs finaux et ébranlent leur confiance dans le marché numérique. Bien que certaines de ces attaques soient assez sophistiquées, la majorité d'entre elles exploite des failles de sécurité plutôt basiques qui sont régulièrement révélées lorsque des violations de données se produisent.

Dans cette section, nous mettrons l'accent sur les aspects techniques, en particulier sur les domaines où la sécurité de l'internet a été menacée. Les progrès dans ces domaines permettront d'améliorer la protection contre un large éventail d'attaques, de compliquer les accès non autorisés et d'augmenter les coûts pour les personnes responsables des attaques. Lors de la réunion de l'*Internet Engineering Task Force* (IETF) qui s'est tenue à Vancouver en novembre 2013[24], les ingénieurs qui conçoivent les protocoles internet ont convenu que l'accès massif aux métadonnées (données de trafic et de localisation) relatives à l'heure et au lieu des communications et l'accès au contenu réel des communications devaient être considérés comme une attaque et que leur modèle de menace devait être adaptés en conséquence.

5.2.1. Primitives cryptographiques

Les primitives cryptographiques sont des algorithmes cryptographiques bien établis, de bas niveau (codés) qui sont fréquemment utilisés pour créer des systèmes de sécurité informatique. La sécurité d'internet repose sur des primitives cryptographiques solides, telles que les fonctions de hachage, les générateurs de nombres aléatoires, les algorithmes d'intégrité et de chiffrement, etc. Ces primitives constituent la base pour une communication sécurisée sur l'internet et servent de fondement pour des systèmes plus complexes. La crypto-analyse vise à briser ces systèmes de sécurité et des chercheurs ont réalisé certains progrès (avec des codes tels que RC4), mais l'ensemble des capacités et des connaissances dans ce domaine restent méconnues. Outre les progrès éventuels dans la crypto-analyse, des rumeurs sur des accès dérobés dans des courbes elliptiques spécifiques et des générateurs de nombres aléatoires ont créé une certaine incertitude au sujet des algorithmes dont l'utilisation est «sûre» et de l'influence sur le processus de standardisation.

24 http://www.ietf.org/mail-archive/web/ietf/current/msg83857.html

5.2.2. Protocoles et architecture

La communication sur l'internet repose en grande partie sur des protocoles standardisés – un système de règles numériques pour l'échange de messages au sein ou entre des ordinateurs – tels que le protocole HTTP utilisé pour la plate-forme internet, le protocole TLS utilisé comme un outil commun pour sécuriser les transactions sur l'internet, ainsi que tous les protocoles de messagerie. Les primitives cryptographiques sont les éléments de base de ces protocoles de communication. Derrière ces protocoles se trouve une architecture qui permet la communication à l'échelle de l'internet.

Une architecture combine un certain nombre d'éléments de base individuels pour créer un système plus grand. Par exemple, l'architecture internet 2.0 utilise non seulement le protocole HTTP mais s'appuie également sur HTML, sur l'utilisation de JavaScript et sur le protocole TLS pour la sécurité.

Les tendances dans l'industrie ont conduit à une conception plus centrée sur le serveur où les données sont souvent stockées dans un service central en nuage (au lieu de suivre un modèle poste-à-poste). L'interconnexion de différentes applications sur l'internet est devenue la norme dans ce que l'on appelle des «mash-ups». Cela a toutefois simplifié l'interception et la surveillance, étant donné que les données peuvent être recueillies à grande échelle à partir d'un petit nombre d'entreprises.

Dans la conception de certaines architectures de communication, tels que la téléphonie par internet ou même les messages électroniques, peu de mesures ont été prises pour éviter la collecte facile de données relatives au trafic. Ce type de données, souvent mentionné dans le débat public comme étant les métadonnées plutôt que le contenu réel de la communication, fournit des informations sur l'heure et le lieu d'une interaction, ainsi que sur les personnes qui y participent. Il s'avère que ces données relatives au trafic ont en elles-mêmes une grande valeur pour les analystes.

Dans de nombreux cas, les utilisateurs finaux se retrouvent avec un choix qui se limite à charger leurs données sur une application ou à ne pas utiliser l'application du tout. Cette tendance devrait se poursuivre car les entreprises accordent également une grande valeur à l'analyse de données volumineuses qui nécessite une collecte massive de données à propos de leurs utilisateurs. Ces collectes massives de données sont bien évidemment des cibles très intéressantes pour les personnes menant des attaques.

5.2.3. Mise en application

Une fois que les protocoles et les architectures ont été développés (généralement par des organismes de standardisation), la spécification doit être transformée en code. Il est difficile de produire du code de haute qualité et cette production nécessite des programmeurs qualifiés et des processus qui garantissent des tests suffisants et des réactions rapides aux rapports de bogues.

Malheureusement, la mise en application peut révéler un certain nombre de lacunes en matière de sécurité, tels que le manque de fonctionnalités dans le domaine de la sécurité, y compris des failles de sécurité (comme l'illustrent les dix principales failles de sécurité des applications internet), la faiblesse des générateurs de nombres pseudo-aléatoires et même l'introduction de chevaux de Troie dans le matériel avant qu'il soit envoyé aux clients. Des accès dérobés peuvent également être ajoutés aux logiciels, d'autant que de nombreuses mises en application de produits ne sont pas disponibles publiquement.

Ces failles de sécurité peuvent être exploitées par un certain nombre d'acteurs, y compris des criminels.

5.2.4. Déploiement

Une fois qu'un produit ou un service a été mis en application, il peut être déployé, par exemple via une application pour téléphone intelligent ou un service internet. De nombreuses décisions de conception importantes qui doivent être prises au cours de cette phase peuvent avoir une incidence sur la vie privée et la sécurité. Par exemple, un fournisseur de messagerie peut définir l'emplacement de son infrastructure serveur, déterminer si la protection de la confidentialité sera mise à la disposition de chaque communication et définir le degré d'authentification. Pour d'autres produits, les décisions doivent être prises au sujet de la plate-forme matérielle et logicielle.

En raison des pratiques des entreprises en matière de sécurité et de la mauvaise sécurité des produits, il est devenu plus facile de compromettre des réseaux et des données d'utilisateur. Cette situation a gravement ébranlé la confiance dans les communications sur internet.

En réponse, les chercheurs et les architectes de protocoles internet réfléchissent à la façon de concevoir un système qui profite à la société, mais qui protège également les particuliers.

La liste des actions éventuelles inclut:

- l'utilisation de la transparence et de l'ouverture dans les processus de standardisation afin de garantir qu'un seul participant n'est pas en mesure de détourner le processus et d'influencer négativement les résultats de la standardisation;
- l'utilisation accrue de logiciels à source ouverte, qui permettent à ceux qui le souhaitent d'examiner le code source des produits et compliquent l'installation d'accès dérobés et augmentent souvent la qualité du code;
- l'augmentation de la sécurité et du respect de la vie privée dans la conception de protocoles internet. Cette action comprend la conception de meilleures techniques de sécurité de bout en bout et des architectures de communication différentes qui produisent moins de métadonnées au niveau des intermédiaires;
- la promotion d'initiatives publiques visant à améliorer le déploiement de services respectueux de la sécurité et de la vie privée;
- l'augmentation de la diversité des offres de services. Par exemple, avec un plus grand nombre de fournisseurs de messagerie et de réseaux sociaux, il serait nécessaire d'attaquer plusieurs cibles pour accéder aux données d'un nombre équivalent d'utilisateurs d'internet.

Dans le même temps, les entreprises doivent modifier leurs pratiques et se pencher plus sérieusement sur la sécurité d'internet et le respect de la vie privée. Dans le cas contraire, les consommateurs hésiteront à télécharger une application pour téléphone intelligent ou à s'inscrire au dernier service internet.

5.2.5. Anonymisation

Avec la réforme de la protection des données en cours, certains sujets tels que le droit à l'oubli et le profilage ont fait l'objet d'un débat intense. L'anonymisation des données aura une incidence profonde en raison de la nouvelle législation, étant donné qu'il s'agit d'un concept essentiel de la protection des données: comment définir les données à caractère personnel et les données parfaitement anonymes[25]?

Dans ce débat, certains pensent qu'il existe différents types de données qui doivent être protégées en fonction du risque estimé pour ces données, ce qui correspond à *l'approche fondée sur le risque*. Dans le cadre de cette approche, les données anonymes, par définition, ne peuvent pas être utilisées pour remonter à une personne ou, en réalité, il est très difficile de s'en servir pour ré-identifier une personne. Dès lors, elles peuvent être traitées librement et ne nécessitent pas un niveau élevé de protection. Par contre, les données qui se rapportent à une personne identifiable doivent respecter le cadre de la protection des données.

Cette situation a suscité un débat visant à assouplir le traitement des informations personnelles en introduisant la notion de données pseudonymes. Dans un ensemble de données pseudonymes, les informations d'identification seraient remplacées par un pseudonyme. L'identification d'une personne particulière serait dès lors plus difficile. Il convient toutefois de noter que, puisque les données pseudonymisées peuvent être reliées à une personne, elles restent des données à caractère personnel. Un exemple typique est la recherche médicale où les chercheurs ne connaissent pas directement les patients, mais uniquement leurs caractéristiques médicales. Un numéro est utilisé pour distinguer les données de chaque patient et un nombre limité de personnes est autorisé à connaître la correspondance entre ce numéro, le nom et la date de naissance du patient.

Des efforts ont été déployés pour inclure une définition des données pseudonymes dans le nouveau règlement sur la protection des données. Toutefois, les avis sont partagés sur la question: certains estiment que cette approche affaiblit la protection des données[26]. En revanche, certaines entreprises anticipent les possibilités commerciales liées à l'introduc-

25 http://www.theguardian.com/news/datablog/2013/aug/12/europe-data-protection-directive-eu

26 http://www.edri.org/eudatap-issuesheets#defi
http://www.cepis.org/index.jsp?p=636&n=639&a=4696

tion de données pseudonymes qui permettront le traitement étendu des données[27].

Jusqu'à récemment, on pensait que cette dépersonnalisation pouvait constituer un outil puissant pour protéger la vie privée. Cependant, la quantité accrue de données volumineuses rend la dépersonnalisation de plus en plus difficile. Étant donné qu'une quantité croissante de données sera recueillie à l'avenir, il pourrait très bien devenir impossible de rendre les données anonymes[28].

Du point de vue de la protection des données, l'utilisation de données pseudonymes pourrait servir de contrôle supplémentaire pour protéger les informations personnelles et minimiser les risques, mais il convient de souligner que les données pseudonymes restent des données à caractère personnel et doivent être protégées en conséquence[29].

Il reste toutefois à effectuer une analyse détaillée des techniques utilisées pour dépersonnaliser les données et à poursuivre les travaux sur la façon de mettre en œuvre ces techniques. Par exemple, l'une des techniques de pointe est *le respect différentiel de la vie privée*. Le respect différentiel de la vie privée permet à un tiers de consulter une base de données grâce à une couche intermédiaire qui fausse (dans une certaine mesure) les résultats de manière à protéger l'identité de la personne concernée. Plus une tierce partie consulte la base de données, plus les données sont faussées. Cette technique est étudiée depuis plusieurs années et est fondée sur des bases mathématiques. Cependant, la mise en œuvre de cette technique n'est pas une mince affaire[30] et elle pourrait ne pas convenir à tous les types de données à caractère personnel.

En outre, pour certains types de données, comme les données sur la localisation, la dépersonnalisation peut s'avérer incroyablement difficile, comme le montre une étude récente du MIT[31]. Cette étude a analysé les données relatives à la localisation de personnes (recueillies par exemple à partir de connexions de téléphones portables à des antennes-relais). Étonnamment, 95 % des personnes concernées peuvent être identifiées avec seulement quatre entrées dans un ensemble de données constitué de 15 mois de coordonnées de mobilité de 1,5 million de personnes dans l'espace et le temps pour une superficie comparable à une région d'un État membre.

D'autres discussions sont nécessaires dans ce domaine et il conviendra d'élaborer des lignes directrices pour expliquer aux responsables du traitement des données comment rendre anonymes les différents types de données à caractère personnel, telles que des données financières, de santé et de télécommunications[32].

Bien qu'il soit nécessaire de développer et de promouvoir les techniques pour minimiser les risques de ré-identification, il est primordial que la protection prévue par le cadre juridique reste intacte. De nombreux acteurs aimeraient traiter davantage de données avec moins de contrôles et cherchent à obtenir des autorisations légales pour utiliser des moyens novateurs afin de traiter des informations transformées en des ensembles de données qui ne peuvent identifier qu'indirectement des personnes.

Les législateurs ne doivent pas redéfinir le cadre couvrant les données à caractère personnel, ce qui réduirait la protection des personnes. La ré-identification de ces ensembles de données resterait possible, et les risques pour la vie privée augmenteraient davantage, étant donné la propension accrue à recueillir de grandes quantités d'informations sur tout un chacun.

5.2.6. Suivi

Chaque accès à une page internet peut être suivi par le serveur internet

De nombreux internautes ne sont pas conscients que la navigation sur un site internet implique une interaction entre leur appareil (PC, tablette, téléphone intelligent, etc.) et le serveur fournissant le contenu internet. Contrairement à une émission télévisée ou

27 http://euobserver.com/justice/119148

28 https://www.eff.org/deeplinks/2009/09/what-information-personally-identifiable

29 http://pdpecho.wordpress.com/2013/03/13/reding-on-pseudonymous-data-we-should-encourage-companies-to-use-pseudonyms-rather-than-the-actual-names/

https://www.huntonprivacyblog.com/2013/03/articles/european-data-protection-supervisor-issues-additional-comments-on-eu-data-protection-reform-package/

http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227_statement_dp_reform_package_en.pdf

30 http://www.cis.upenn.edu/~ahae/papers/fuzz-sec2011.pdf

31 http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html

32 En 2013, le groupe de travail «Article 29» a commencé à travailler sur ces lignes directrices.

radiodiffusée, à un livre imprimé ou un journal, à un panneau ou une affiche dans la rue, une page internet est seulement disponible à la suite d'une requête individuelle envoyée à partir du navigateur de l'utilisateur. Cette requête doit identifier l'appareil de l'utilisateur, sinon le serveur n'aurait aucune indication de l'endroit où envoyer la page demandée. Cette interaction directe permet une forme de suivi à son niveau le plus élémentaire, c'est-à-dire la conservation d'une trace de chaque requête concernant une page internet particulière à un moment précis.

L'écosystème internet a considérablement évolué depuis l'époque où les pages internet étaient statiques et étaient identiques pour tout le monde. Aujourd'hui, les pages sont généralement adaptées à chaque utilisateur et présentent un contenu ciblé, souvent dans le but d'augmenter la valeur économique de la page, en affichant des offres commerciales attrayantes ou des publicités qui attirent l'attention de l'utilisateur.

Cette personnalisation des pages nécessite beaucoup plus d'informations sur l'utilisateur que celles fournies par une simple requête d'une page internet et elle a entraîné le développement et l'utilisation de mécanismes de suivi plus sophistiqués. En outre, le contenu des pages n'est plus fourni par un seul serveur, mais par plusieurs acteurs; par exemple, le contenu principal sur les sites d'actualités est composé d'actualités, tandis que différents fournisseurs de publicité remplissent les autres parties de l'écran. Tous espèrent attirer au maximum l'attention de l'utilisateur pendant sa période de navigation limitée.

Un des outils les plus courants, à savoir les «cookies», a été normalisé en 1995 pour permettre le stockage d'informations sur les préférences et le comportement d'un utilisateur dans ses sessions. Des inquiétudes sur l'augmentation du suivi sont apparues simultanément et des idées concernant un mécanisme «Do Not Track (DNT)» ont été présentées par des groupes de consommateurs pour la première fois en 2007.

Au niveau de la législation, les modifications de 2009 apportées à la directive «vie privée et communications électroniques» de l'Union européenne visaient à accroître la transparence et le contrôle de l'utilisateur concernant les cookies et d'autres mécanismes de suivi qui stockent des informations sur l'appareil de l'utilisateur. Jusqu'à présent, ces objectifs n'ont pas été pleinement atteints, étant donné qu'à l'heure actuelle, de nombreux sites internet ne fournissent aux utilisateurs qu'une bannière d'information générale indiquant l'utilisation de cookies, mais fournissent peu de détails ou n'offrent pas d'autre choix que celui de ne pas utiliser le site internet du tout

L'augmentation des activités en ligne a entraîné une augmentation du suivi. Des règles plus strictes sur les cookies ont conduit au développement de nouveaux mécanismes de suivi, afin de contourner ces règles.

La capture d'empreintes numériques *(device fingerprinting)* est une solution pour remplacer les cookies. Ce système implique la collecte d'autant de caractéristiques de l'appareil de l'utilisateur que possible, y compris les éléments techniques tels que la taille de l'écran, le navigateur et le type et la version du système d'exploitation, les polices et les outils complémentaires installés, ainsi que les paramètres de préférences de l'utilisateur, tels que la langue, le facteur de zoom, le codage de caractères, etc.

Plus le nombre de caractéristiques collectées est élevé, plus il est probable que deux appareils d'utilisateurs différents n'auront pas le même profil. Bien que certains serveurs utilisent uniquement les caractéristiques que l'utilisateur, ou plutôt l'appareil de l'utilisateur, doit fournir pour recevoir une page internet adaptée à ses préférences et capacités (empreintes passives), d'autres indiquent au navigateur d'exécuter du code, tel que JavaScript, afin de révéler d'autres caractéristiques (empreintes actives) pour disposer d'un profil plus complet.

L'une des organisations responsables de l'élaboration de standards pour internet, le Worldwide Web Consortium (W3C), s'est efforcé de fournir aux utilisateurs un moyen de communiquer leur volonté de ne pas être suivis, et ce par la standardisation d'un en-tête DNT à l'intérieur du principal protocole internet HTTP. Ces efforts de standardisation ont accomplis des progrès lents et n'ont pas respecté plusieurs délais médiatisés, mais l'on peut espérer que la spécification technique finale sera disponible en 2014.

Malgré certains doutes sur la qualité du suivi, le recours à la capture d'empreintes numériques augmente, comme le montre une récente étude de la KU Leuven[33].

Dans le même temps, certains fabricants de navigateurs ont néanmoins inclus la prise en charge du

DNT dans leurs produits: Microsoft a annoncé que le DNT était activé par défaut dans Internet Explorer 10 et Internet Explorer 11. Depuis un certain temps, Apple n'autorise pas les cookies de tierces parties dans son navigateur Safari et, en février 2013, Mozilla a annoncé qu'il prévoyait de désactiver les cookies de tierces parties, mais ce projet a été reporté. Apple a même ajouté la prise en charge de l'en-tête DNT en dehors du navigateur dans les systèmes d'exploitation iOS 6 utilisés par leurs téléphones intelligents.

Toutefois, des méthodes de suivi complètement nouvelles ont également été mises au point et les ingénieurs ont fait preuve d'une grande créativité dans la production de méthodes de suivi de plus en plus sophistiquées, telles que le suivi du mouvement du curseur sur l'écran de l'utilisateur. Les solutions de gestion d'identité distribuée permettent d'effectuer un suivi dans plusieurs services internet. Avec la gestion d'identité, les utilisateurs se connectent à un site internet en utilisant leurs références de connexion (généralement un nom d'utilisateur et un mot de passe) et ils sont ainsi identifiés de manière unique, quel que soit l'appareil qu'ils utilisent. La gestion d'identité est nécessaire pour des services personnalisés, tels que les services de messagerie sur internet ou les réseaux sociaux.

Aujourd'hui, de plus en plus de services exigent une identification de l'utilisateur, tels que les jeux ou les flux de contenu. Comme il est peu probable que les utilisateurs se rappellent des mots de passe multiples et variés pour tous les sites sur lesquels ils se connectent, des systèmes de gestion d'identité distribuée sont apparus. Ces systèmes permettent aux utilisateurs de réutiliser leurs comptes, par exemple d'un service de réseau social, sur plusieurs sites sans devoir créer un nouveau compte sur chaque site.

Bien qu'il existe de nombreux services sur l'internet qui proposent une gestion d'identité réutilisable, les sites internet doivent configurer leur service pour chaque fournisseur d'identité. Afin de minimiser l'effort nécessaire, des fournisseurs limitent la prise en charge aux fournisseurs d'identité les plus populaires, de sorte que les identités les plus prises en charge proviennent de Facebook et Google.

Les solutions de gestion d'identité distribuée offrent des possibilités de suivi plus puissantes que les cookies et la capture d'empreintes numériques, étant donné qu'elles sont en mesure de suivre les utilisateurs sur plusieurs appareils.

33 http://www.kuleuven.be/english/news/several-top-websites-use-device-fingerprinting-to-secretly-track-users

Les navigateurs ne sont qu'un moyen parmi d'autres d'accéder à l'internet. Les utilisateurs de téléphones intelligents et de tablettes peuvent choisir des applications téléchargeables parmi d'immenses catalogues. Lorsque les applications sont exécutées sur l'appareil de l'utilisateur, elles sont en mesure d'accéder à un large éventail d'informations personnelles. Les fabricants de téléphones intelligents et de systèmes d'exploitation mobiles (OS), comme Apple, Google ou Microsoft, ont conçu des mécanismes de suivi dans le système d'exploitation et le matériel, afin de mettre en place une infrastructure qui permet une analyse approfondie des interactions suivies, en utilisant des identifiants uniques intégrés dans le matériel.

En outre, les développeurs d'applications peuvent également intégrer des logiciels d'analyse de tierces parties dans leurs applications. Ces logiciels suivent les utilisateurs tout au long de leur utilisation et fournissent aux développeurs d'applications des indications sur la façon dont ils peuvent rendre leurs applications plus conviviales, mais dans le même temps, ces logiciels donnent aux fournisseurs de logiciels d'analyse l'accès aux données de l'utilisateur via de nombreux appareils et applications.

Le prochain défi que les développeurs de logiciels de suivi devront relever sera d'aller au-delà de l'utilisation d'internet au travers des navigateurs et des applications, et d'appréhender le comportement en ligne et hors ligne.

Le suivi et la publicité sont encore en développement dans de nombreux domaines, notamment dans les systèmes de divertissement à domicile et les consoles de jeu dédiées qui offrent un nombre croissant de services aux applications, y compris des possibilités de gestion d'identité ainsi que des API publicitaires. L'utilisation de jeux, comme une sorte de laboratoire vivant, pour tester la réaction des utilisateurs à des stimuli est une occasion de trouver de toutes nouvelles méthodes de suivi, en utilisant des caméras intégrées, par exemple.

Les fonctionnalités intégrées de renseignement et de suivi d'autres appareils grand public ont également pris de l'ampleur. Le téléviseur traditionnel est remplacé par des appareils avec des fonctionnalités intégrées qui permettent de se connecter à internet et de rechercher des offres de programme sur des serveurs internet dédiés. Aujourd'hui, les modems par câble servent généralement aussi d'appareils pour naviguer sur internet et échangent des informations avec les serveurs de l'opérateur de réseau câblé, en identifiant systématiquement au moins le ménage,

afin de contrôler l'accès à des services à valeur ajoutée ou optionnels en fonction de leurs abonnements.

Ce système fournit également aux opérateurs de services de médias des données détaillées sur l'utilisation des médias par leurs clients, lesquelles permettent à leur tour d'effectuer une analyse précise et complète des intérêts, des habitudes, des préférences et des influences, en ce qui concerne un éventail de médias allant des programmes politiques aux clips publicitaires. Bien que les incidences de ces développements sur le respect de la vie privée et la protection des données aient fait l'objet de peu de recherches, les premières études ont suscité des inquiétudes considérables: une enquête de l'autorité néerlandaise de protection des données menée dans un réseau néerlandais de télévision connectée a mis en évidence des violations notables de la législation sur la protection des données.

La collecte de données relatives à la localisation et leur utilisation à différentes fins commerciales continuent d'augmenter. La concentration croissante dans le marché des appareils mobiles et des services de communication renforcera le rôle des très rares acteurs mondiaux qui collectent des données de localisation et des données liées à d'autres communications.

Le suivi accru en matière de géolocalisation concerne également d'autres domaines, tels que le suivi par bluetooth et WiFi, ou le suivi des téléphones mobiles à courte distance au moyen de leurs signaux radio ou lorsqu'ils sont placés en interaction. En outre, de nombreux autres appareils sont désormais équipés de fonctionnalités de communication et de suivi, y compris des capteurs biométriques utilisés dans le sport, des systèmes de navigation par satellite, des systèmes de paiement de péage automatiques et des systèmes de billets électroniques pour les transports publics (voir la section 5.2.7 sur l'internet des objets).

L'intégration croissante d'équipements de communication, de localisation et de traitement dans les véhicules automobiles, tels que visé par le déploiement complet d'un système eCall dans tous les nouveaux véhicules particuliers en Europe à partir de 2015, contribuera à promouvoir l'utilisation de cette plateforme à des fins autres que les services d'urgence. Les propositions relatives aux frais d'assurance automobile fondés sur les distances parcourues, en tenant compte de la zone précise de déplacement et du comportement du conducteur (par exemple, accélération et freinage fréquents), sont quelques-unes des idées créatives pour utiliser les données de déplacement. Il existe une demande croissante en ce qui concerne l'utilisation des données de reconnaissance de plaque d'immatriculation provenant des systèmes de péage existants à des fins d'application de la loi ou de celles provenant des systèmes de contrôle de vitesse qui identifient les plaques d'immatriculation des voitures entrant et sortant de l'autoroute afin de calculer la vitesse moyenne sur cette section.

Les outils de suivi utilisés à des fins commerciales servent également à la surveillance par les autorités publiques.

De récentes publications dans la presse montrent que les informations de suivi sont non seulement utilisées à des fins commerciales, mais également par les gouvernements dans des programmes de surveillance renforcée. Par exemple, le suivi de cookies peut être utilisé pour pirater l'appareil d'un utilisateur spécifique et y dissimuler un logiciel qui permet une utilisation à distance. Le cookie de suivi de Google, PREF, a été utilisé pour cibler des activités de communication sur les ordinateurs d'utilisateurs spécifiques, et la localisation d'utilisateurs mobiles a été suivie au moyen d'applications mobiles. Les répercussions du suivi commercial sur les droits fondamentaux en matière de respect de la vie privée et de protection des données ne sont pas limitées aux intérêts des entreprises.

5.2.7. L'internet des objets

La notion d'«internet des objets» (IdO) a été choisie pour désigner la vision d'un avenir dans lequel les objets du quotidien tels que les téléphones, les voitures, les appareils électroménagers, les vêtements, le transport et la logistique sont connectés sans fil l'un à l'autre grâce à la technologie d'internet, leur permettant ainsi de partager des données et d'interagir. Par exemple, l'IdO est utilisé dans des concepts novateurs tels que les «villes intelligentes» où les données sont recueillies dans le but d'atténuer les problèmes

urbains, tels que les embouteillages et la pollution environnementale. Cette vision de l'IdO a joué un rôle moteur dans les efforts politiques, de recherche et de développement visant à créer des structures de gouvernance et des principes communs pour une large gamme d'appareils et de services.

De nombreuses questions ont été soulevées au cours des dix dernières années. Comment l'IdO modifiera-t-il internet tel que nous le connaissons? De nouveaux protocoles seront-ils nécessaires pour les communications de l'IdO? Le modèle de gouvernance existant s'appliquera-t-il aux fabricants d'appareils de communication et aux fournisseurs de services ainsi qu'à tous les fabricants d'appareils grand public? De quelle manière les consommateurs (et les autres) seront-ils associés? Quelles standards sont-elles nécessaires?

Il n'existe actuellement aucune standard unique IdO (ou de machine à machine, M2M), mais un large éventail de standards différentes ont été développées à des fins diverses.

Au lieu d'attendre la mise en place de la nouvelle architecture globale d'IdO, de nombreuses entreprises ont mis au point des solutions opérationnelles IdO sur la base de protocoles internet existants, ainsi que des applications pour les connecter à l'infrastructure internet existante. Bien que cette approche pragmatique semble plutôt simple, on a longtemps cru que la multitude de petits capteurs et d'acteurs qui composent l'IdO nécessitaient de nouveaux mécanismes et standards spécifiques de communication.

Selon certains praticiens, le nombre croissant de solutions de travail démontrent que l'infrastructure existante en matière de protocole internet peut favoriser le développement de solutions IdO. Même si cette approche peut initialement mener à un certain nombre de solutions isolées, il semble que, pour certains secteurs ou domaines d'application par exemple, elle pourrait conduire à des modèles économiques viables qui offrent une concurrence sérieuse dans le développement d'un modèle holistique en ce qui concerne l'IdO.

En conséquence de cette approche pragmatique, nous avons vu l'émergence d'une large gamme d'appareils qui recueillent des informations sur les personnes et les chargent sur différents services internet, tels que des équipements portables de suivi utilisés pour le sport. Pour favoriser ces développements, les entreprises ont dû concevoir des systèmes capables de fonctionner avec les fonctionnalités limitées des petits appareils en l'absence d'un protocole et qui prennent en charge la communication directe entre divers types d'appareils produits par différents fabricants. Les capteurs interagissent rarement entre eux «de poste-à-poste», mais ils transmettent leurs données via des services centralisés dans des environnements d'informatique en nuage.

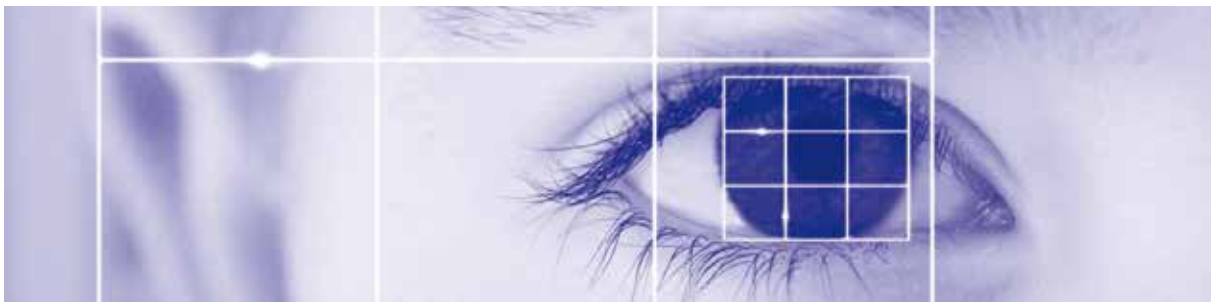
Bien que cette conception centralisée simplifie la gestion du contrôle d'accès et de sécurité, elle a une forte incidence sur la protection des données et le respect de la vie privée, étant donné qu'elle favorise d'énormes collectes de données à caractère personnel qui pourraient être utilisées pour une analyse et une utilisation plus approfondies. Les dispositifs IdO se comportent comme de nombreux autres services internet, en ce qu'un maximum de données disponibles sont recueillies plutôt que le minimum nécessaire. Les utilisateurs acceptent encore cette situation, mais les problèmes de confidentialité liés à l'informatique en nuage et aux analyses de données volumineuses s'appliquent également à l'IdO.

L'application des principes établis de protection des données, tels que la réduction des données au minimum et la limitation de la finalité, constituerait une protection efficace contre les principaux risques pour la vie privée. Malheureusement, ceux-ci n'ont pas été les principes directeurs pour le développement d'internet, ni pour la conception d'applications pour téléphones portables. La même approche indifférente est susceptible d'être également appliquée à l'IdO. À l'heure actuelle, il existe peu de mesures, voire aucune, incitant le fournisseur de services qui conçoit le logiciel pour des dispositifs IdO à prendre au sérieux les questions de confidentialité et de sécurité, d'autant plus que les standards en vigueur ne tiennent pas compte de ces objectifs.

La sécurité constitue également un défi. Les experts sont préoccupés par la mise au point de la prochaine génération d'infrastructure qui sera critique, mais également peu sûre en raison des pratiques souples liées aux dispositifs embarqués[34]. Pour réduire le coût de développement de ces petits dispositifs, des économies sont souvent réalisées dans le domaine de la sécurité. Il reste à voir si les efforts actuels destinés à sensibiliser à ce risque croissant encourageront la communauté mondiale du développement de l'IdO à adopter de meilleures pratiques en matière de sécurité.

Dans le même temps, des solutions technologiques de rechange existent dans le domaine des sources ouvertes. Des dispositifs abordables (environ 20-40 euros) permettent aux consommateurs disposant de peu de connaissances en matière d'IdO d'expérimenter eux-mêmes les idées relatives à l'IdO. Des dispositifs tels qu'Arduino et Raspberry Pi sont très populaires dans les écoles et sont utilisés pour présenter des concepts informatiques aux enfants et aux ado-

34 http://www.wired.com/Opinion/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/



lescents. En ce qui concerne les serveurs, il existe une énorme gamme de logiciels internet et en nuage. Les développeurs soucieux de la vie privée qui travaillent avec ces outils pourraient développer des solutions respectueuses de la vie privée pour servir d'exemples de bonnes pratiques ou comme solutions pour remplacer les produits de l'industrie.

5.3. Biométrie

5.3.1. Génomique personnelle

En 2003, une équipe de recherche scientifique a mené à bien le projet du génome humain, à savoir le séquençage de l'ensemble de l'information génétique humaine. Ainsi, les tests génétiques sont désormais largement disponibles. Le test porte sur une petite zone de l'ensemble du génome, mais les résultats, qui sont très précis, peuvent souvent être fournis en quelques jours.

La séquence de l'ADN dans nos gènes détermine notre capacité à survivre et à se reproduire. Chez l'être humain, environ trois milliards de paires de bases de l'ADN constituent le génome et en raison de minuscules variations, chaque personne dispose d'un code unique. Ce vaste volume d'informations dans le génome d'une personne est l'équivalent biométrique de son identité. Il peut servir d'élément d'identification biométrique car il est difficile de rendre les informations contenues dans un génome anonymes. Il est clair que la génomique personnelle représente un défi pour la protection des données à caractère personnel.

Les tests génétiques sont utilisés dans la recherche médicale pour identifier les mutations dans nos gènes afin de contribuer au développement de thérapies qui préviendront des maladies comme le cancer, la maladie d'Alzheimer, les maladies cardiaques, etc. Il existe de nombreuses autres utilisations possibles de l'information génétique, certaines ayant des répercussions importantes sur la vie privée. Par exemple, ces tests peuvent être utilisés pour restreindre l'accès à une assurance ou l'entrée en fonction de personnes en bonne santé connues pour être génétiquement prédisposées à une maladie, ou par des entreprises proposant des tests génétiques pour offrir des possibilités de réseautage social à des utilisateurs partageant un trait génétique afin qu'ils communiquent entre eux.

Lorsque des données génétiques sont disponibles sur une grande échelle, elles constituent une ressource précieuse pour les industries pharmaceutiques, les hôpitaux et même les gouvernements. Récemment, dans le cadre du projet du génome humain au Royaume-Uni, un appel a été lancé pour qu'un grand nombre de bénévoles partagent leurs données génétiques avec le reste du monde à des fins scientifiques. Comme l'information génétique est transmise et partagée au sein d'une famille, les participants ne seront pas les seuls à s'engager, car ils engageront également dans une certaine mesure leurs parents et leurs descendants. Les préoccupations et les risques en matière de protection de la vie privée qui s'appliquent aux bases de données informatiques à grande échelle stockant des informations de consommateurs s'appliquent également aux bases de données massives contenant l'information génétique, qu'elles soient gérées par des organisations commerciales ou par la communauté scientifique.

5.3.2. Reconnaissance faciale

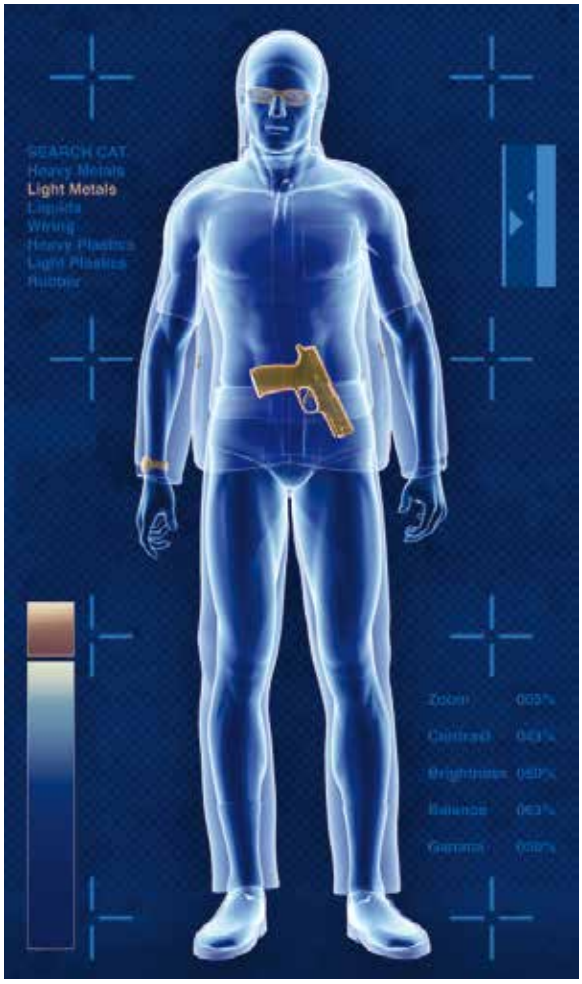
L'un des pivots entre les images de personnes et leurs informations personnelles est disponible sur les médias sociaux. Grâce aux progrès technologiques accomplis dans la reconnaissance faciale et la quantité toujours croissante d'informations visuelles[35] chargées sur internet, il devient plus facile de créer

35 En 2013, plus de 350 millions de photos ont été mises en ligne chaque jour en moyenne sur Facebook.

des profils de personnes à travers les images qui sont chargées et de les relier aux informations qu'elles transmettent ou qui sont transmises à leur sujet sur les médias sociaux et d'autres sites.

En raison de la prévalence des téléphones intelligents et d'autres appareils portables, la reconnaissance faciale, associée à des services d'informatique en nuage et des analyses de données volumineuses, pourrait être utilisée pour recueillir des informations publiques sur des personnes, de sorte que le profilage d'autres personnes soit une option accessible à tous. Étant donné que les progrès technologiques rendent cela possible, il est important d'envisager ce que devraient être les limites de ce traitement.

5.4. Frontières



Les efforts visant à sécuriser les frontières de l'Union européenne dépendent de la coopération entre les États membres. Toutefois, cette coopération repose souvent sur le traitement d'informations personnelles. Un certain nombre de bases de données informatiques à grande échelle existent déjà pour contrôler la circulation des voyageurs à destination de l'Union européenne (VIS, SIS II, EURODAC), lesquelles permettent également aux autorités chargées de l'application de la législation d'accéder aux informations contenues dans ces bases de données. La Commission européenne est en faveur de plus grandes bases de données[36]; as a result, the Entry-Exit system (EES) and the Regipar conséquent, le système d'entrée-sortie (SES) et le programme d'enregistrement des voyageurs (RTP) pourraient bientôt être opérationnels dans toute l'Europe.

Le SES vise à identifier les personnes qui dépassent la durée de séjour autorisée (les voyageurs qui ont obtenu un visa pour une certaine durée, mais qui restent dans l'Union après l'expiration de leur visa) en enregistrant le moment et le lieu d'entrée et de sortie des ressortissants de pays tiers voyageant dans l'Union européenne. Cela permettra aux douaniers de vérifier le statut d'un voyageur sans avoir à vérifier les cachets sur son passeport, vérification qui peut être longue et complexe. En temps voulu, les autorités chargées de l'application de la législation seront probablement également en mesure d'accéder aux données du SES[37].

Le RTP permettra aux voyageurs fréquents issus de pays tiers d'entrer dans l'Union européenne en se soumettant à des contrôles frontaliers simplifiés, sous réserve d'une pré-vérification et d'un filtrage. Cela signifie que les voyageurs qui fournissent leurs données à caractère personnel avant de voyager bénéficieront d'un processus plus rapide et simplifié lors des contrôles aux frontières.

Le débat continue en ce qui concerne les propositions relatives au RTP et au SES[38] (voir section 3.4.4). Les deux systèmes impliqueront la collecte de quantités croissantes de données à caractère personnel, y compris des informations biométriques – empreintes digitales – et l'intégration dans les contrôles automatisés aux frontières (contrôles automatisés des passagers aux postes frontaliers à l'aide de nouvelles technologies sous la surveillance de gardes-frontières).

Comme l'a démontré l'incident de sécurité de 2013 lié aux données du SIS [39] une faille de sécurité dans ces systèmes d'information à grande échelle pourrait avoir des conséquences sur les données à caractère

36 http://ec.europa.eu/commission_2010-2014/malmstrom/news/archives/2013/02/20130228_en.htm

37 http://database.statewatch.org/article.asp?aid=32381

38 http://www.dw.de/eu-smart-borders-plan-raises-big-brother-flags/a-16639437
Avis du CEPD sur le SEE et le RTP

39 http://www.theregister.co.uk/2013/06/07/pirate_bay_founder_named_as_suspect_in_paneuropean_police_database_hack/

personnel d'un nombre important de personnes à travers l'Union européenne. Étant donné que davantage de bases de données sont créées et que l'accès aux données qui y sont conservées est accordé plus largement, le risque que des informations personnelles soient compromises ou utilisées à mauvais escient augmente également.

5.5. Drones

Les drones, également appelés systèmes d'aéronefs pilotés à distance (Remotely piloted aircraft systems, RPAS) ou véhicules aériens sans pilote (unmanned aerial vehicles, UAV) sont des avions qui fonctionnent sans pilote à leur bord. Les drones ont principalement été utilisés à des fins militaires, mais leur utilisation s'étend désormais largement aux domaines scientifique et civil, dans des tâches qu'il est trop difficile ou coûteux de réaliser en utilisant la technologie aérienne existante. Les modèles récents de drones n'ont jamais été aussi stables et ils disposent de fonctionnalités de pilotage automatique, réduisant ainsi le temps, l'intervention humaine et le coût nécessaires pour les faire voler.

Les drones, qui sont équipés de caméras à haute définition, peuvent être utilisés pour la retransmission vidéo en direct et la surveillance en temps réel. Le risque éventuel pour la vie privée dépend donc en partie du type de capteurs qui équipe les drones, ainsi que de la taille et de la visibilité du dispositif porteur aérien.

Comme les drones peuvent être utilisés en dehors des espaces publics extérieurs, ils peuvent être très envahissants. Le contrôle qu'une personne peut avoir sur la surveillance par drone est extrêmement limité. Même quand il est détecté, il peut être difficile d'identifier l'opérateur ou l'objectif du drone, ou encore la technologie avec laquelle il est équipé.

Étant donné que la technologie des drones continue d'évoluer, les conséquences sur la vie privée demeurent une préoccupation importante. En dépit de cela, il existe encore peu de mesures incitant à respecter le principe de la vie privée dès la conception.

6 INFORMATION ET COMMUNICATION

Notre objectif stratégique

Développer une stratégie de communication efficace et créative

6.1. Introduction

Les activités d'information et de communication jouent un rôle clé en aidant à mieux faire connaître le mandat, les politiques et les décisions du CEPD tant au sein de l'administration de l'Union européenne qu'auprès du grand public. Nous utilisons une gamme d'outils et d'activités de communication adaptés à des publics différents et à leurs divers degrés de connaissance en matière de protection des données. Des communiqués de presse réguliers, des publications, des événements, des tweets et des mises à jour sur notre site internet sont quelques-unes des activités qui font partie de notre politique visant à sensibiliser à des sujets clés.

L'un des objectifs globaux de la stratégie du CEPD pour 2013-2014 est de sensibiliser l'opinion à la protection des données en tant que droit fondamental et élément essentiel d'une politique publique saine et de la bonne administration au sein des institutions de l'UE.

À cette fin, nous avons poursuivi, en 2013, notre objectif visant à sensibiliser le public aux travaux du CEPD – avis législatifs, avis de contrôle préalable, droits et obligations en matière de protection des données, formation des délégués à la protection des données de l'UE – et à la protection des données en général. Notre objectif est de promouvoir une «culture de protection des données» au sein des institutions et organes de l'UE de manière à ce qu'ils

soient conscients de leurs obligations et assument la responsabilité du respect des exigences relatives à la protection des données.

Au cours du second semestre, la réforme de la protection des données et les révélations sur la surveillance de masse ont fait la une de la presse, et par conséquent, les contrôleurs et le personnel yy ont consacré une attention toute particulièreparticulière – des questions des médias à des discours et des auditions, en passant par des interviews avec la presse et des demandes d'informations.

Notre visibilité accrue en tant qu'institution est confirmée par les indicateurs comme le nombre de demandesdemandes d'information soumises par les citoyens de l'UE, de questions des médias et de demandes d'entretien, le nombre d'abonnés à la newsletter, le nombre de personnes suivant le CEPD sur Twitter ainsi que le nombre d'invitations à venir s'exprimer à des conférences et le trafic sur le site internet. Tous ces éléments montrent bien que nous devenons de plus en plus un point de référence pour les questions de protection des données au niveau de l'Union européenne.

6.2. Caractéristiques de la communication

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

6.2.1. Principaux publics et groupes cibles

Alors que de nombreuses organisations, y compris les autres institutions et organes de l'Union, s'adressent à l'ensemble des citoyens européens et peuvent choisir leur public en fonction du groupe d'âge, de la profession, du sexe, de la situation de famille, du niveau scolaire, de la zone géographique, etc., notre champ d'action direct est plus restreint.

Notre supervision des institutions et organes de l'UE faitfait de ces derniers notre public cible et nous adaptons nos messages au personnel de l'Union en conséquence. D'autres groupes clés comprennent les personnes concernées en général, les acteurs politiques de l'UE et ceux de la communauté de la protection des données.

Il n'est donc pas nécessaire que notre politique de communication recoure à une «communication de masse». Au contraire, la sensibilisation des citoyens de l'UE aux questions de protection des données, au niveau des États membres, repose sur une approche plus indirecte passant par exemple par les autorités nationales chargées de la protection des données.

Nous communiquons avec le grand public grâce à un certain nombre d'outils (site internet, Twitter, publication de notre newsletter et de nos fiches d'information, et événements de sensibilisation), et nous entretenons des contacts réguliers avec les parties intéressées (par des visites d'étude, par exemple) et participons à des événements publics, réunions et conférences.

6.2.2. Politique linguistique

La stratégie du CEPD 2013-2014 tient compte du fait que les non-spécialistes perçoivent souvent les questions de protection des données comme relativement techniques et obscures. En conséquence, la stratégie met en évidence le fait que notre travail de communication utilisera un langage clair pour rendre les questions techniques plus accessibles.

En 2013, nous avons continué à accomplir d'énormes progrès à cet égard, notamment dans notre communication avec le grand public et la presse. Le principal objectif a été de remédier à l'image de la protection des données, qui passe pour une préoccupation excessivement juridique et technique.

Bien évidemment, lorsque nous nous adressons à des publics plus éclairés, comme des spécialistes de la protection des données, un langage plus spécialisé est approprié. Nous sommes bien conscients qu'il est important d'utiliser différents styles de communication et différentes approches linguistiques pour communiquer des faits identiques en fonction du public ciblé.

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

6.3. Relations avec les médias

Nous souhaitons être aussi accessibles que possible pour les journalistes, étant donné qu'ils représentent un canal majeur permettant au public de suivre notre travail. Des interactions régulières avec les

médias au moyen de communiqués de presse, d'interviews et de rencontres avec la presse nous aident à entretenir l'image d'un partenaire réactif et fiable et à promouvoir le CEPD en tant que point de référence indépendant et officiel pour la protection des données au niveau de l'UE.

La gestion des demandes formulées par les médias permet d'entretenir des contacts supplémentaires avec ceux-ci, et en 2013, nous avons continué à mettre à jour et à maintenir notre liste de contacts parmi les médias.

6.3.1. Communiqués de presse

En 2013, nous avons publié 11 communiqués de presse. La majorité de ces communiqués concernaient nos travaux de consultation, et en particulier de nouveaux avis législatifs présentant un intérêt immédiat pour le grand public. Les sujets abordés par ces communiqués de presse ont notamment été la réforme de la protection des données dans l'UE, Europol, la cybersécurité, la lutte contre le blanchiment de capitaux, les frontières intelligentes et les communications électroniques.

Nos communiqués de presse sont publiés sur notre site internet et dans la base de données interinstitutionnelle des communiqués de presse de la Commission (RAPID) en anglais, en français et en allemand. Les communiqués de presse sont diffusés au sein de notre réseau régulièrement mis à jour de journalistes et de parties intéressées.

Les informations fournies dans nos communiqués de presse contribuent généralement à la production d'une couverture médiatique importante par la presse générale et spécialisée. De plus, nos communiqués de presse sont fréquemment publiés sur des sites internet institutionnels et non institutionnels, notamment ceux des institutions et organes de l'UE, des groupes de défense des libertés civiles, des institutions académiques et des entreprises de technologies de l'information et autres.

6.3.2. Interviews

En 2013, le CEPD et le contrôleur adjoint ont accordé 45 interviews directes à des journalistes de la presse écrite, de la radiotélévision et des médias électroniques, en Europe et au niveau international.

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

Ces interviews ont abordé des questions horizontales comme les défis actuels et à venir dans le domaine de la protection de la vie privée et des données. Elles ont également abordé les thèmes particuliers qui ont fait la une des journaux en 2013, comme la révision du cadre juridique européen de protection des données, le lobbying lié à cette révision, la surveillance de masse après les révélations de la NSA, la sécurité sur l'internet, le contrôle aux frontières, la conservation et la collecte des données, les données volumineuses, les autorités nationales de protection des données et la fin dudu mandat du CEPD

6.3.3. Conférences de presse

En 2013, nous avons organisé une conférence de presse de midi le 29 mai, juste après la présentation de notre rapport annuel 2012 à la commission LIBE du Parlement européen.

La conférence a été l'occasion pour les journalistes de discuter avec Peter Hustinx, contrôleur européen de la protection des données, et Giovanni Buttarelli, contrôleur adjoint, des conséquences de la réforme de la protection des données et en particulier du lobbying excessif dont fait l'objet le législateur de l'UE de la part de l'industrie et des pays tiers. La participation à la conférence a été satisfaisante et les discussions animées ont donné lieu à de nombreux reportages dans la presse européenne au sujet de notre position sur la réforme des règles de protection des données.

6.3.4. Demandes formulées par les médias

En 2013, le CEPD a reçu quelque 34 demandes écrites formulées par les médias qui comprenaient des demandes de commentaires et des demandes de clarification, de position ou d'information. L'attention des médias s'est portée sur de nombreux sujets, et plus particulièrement sur la surveillance de masse et la réforme des règles de protection des données dans l'UE. D'autres sujets d'intérêt comprenaient le CEPD lui-même, EURODAC, le système eCall, les frontières intelligentes, le suivi par adresse

IP, la dénonciation, INDECT, les violations en matière de données, les données volumineuses, la cybersécurité, l'accès aux documents, le groupe de travail «Article 29», Google et le verrouillage par empreinte digitale de l'iPhone.

6.4. Demandes d'informations et de conseils

En 2013, nous avons traité 176 demandes d'informations ou d'assistance. Ce chiffre est supérieur à celui de 2012 (116 demandes) et il est considérable pour une petite organisation. La notoriété du CEPD dans le monde de la protection des données, renforcée par nos efforts de communication, par les améliorations importantes apportées à notre site internet, et par de nouveaux outils de communication comme les fiches d'information et l'utilisation de Twitter, montre que nous faisons passer notre message de façon plus efficace.

La majorité des demandes d'informations émanaient de personnes dont l'activité n'est pas liée aux institutions de l'UE et souhaitant obtenir plus d'informations sur les questions relatives à la protection de la vie privée ou demandant une assistance pour résoudre des problèmes, tels que la sécurité de leurs informations personnelles ou l'utilisation abusive de celles-ci. D'autres demandes provenaient d'un large éventail de parties, allant du personnel des institutions de l'Union à des avocats et des cabinets d'avocats, en passant par des entreprises privées et des associations de l'industrie, des étudiants et des ONG.

Un grand nombre de demandes reçues en 2013 concernait des réclamations de citoyens de l'UE pour lesquelles le CEPD n'est pas compétent. Ces réclamations portaient pour la plupart sur des violations présumées de la protection des données par des autorités publiques, des entreprises publiques ou privées et des services et technologies en ligne. D'autres portaient sur la protection des données dans les États membres, les transferts de données, la collecte excessive de données et le temps de réaction excessif des autorités chargées de la protection des données.

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

6.5. Visites d'étude

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

En 2013, nous avons accueilli 17 groupes. La majorité était des étudiants ou des universitaires provenant de l'Union européenne, ainsi que d'autres groupes originaires d'Islande, de Norvège et des États-Unis, mais nous avons également reçu la visite de journalistes européens et d'associations politiques.

La plupart des groupes souhaitaient en apprendre davantage sur le mandat et les activités du CEPD, mais des groupes ont également démontré un grand intérêt pour la réforme de la protection des données dans l'UE, la coopération internationale, l'informatique en nuage, le profilage en ligne et les conséquences de la conservation et de la surveillance de données sur le respect de la vie privée et la protection des données.

6.6. Outils d'information en ligne

6.6.1. Site internet

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

Depuis juin 2013, le site internet du CEPD repose sur le protocole https, de sorte que toutes les communications entre l'utilisateur et le site sont cryptées, conformément aux bonnes pratiques en matière de sécurité.

Trafic et navigation

Une analyse des données sur le trafic et la navigation montre que le site internet a accueilli environ 136 293 visiteurs uniques en 2013, ce qui représente une ***augmentation significative de 63 %*** *par rapport aux 83 618 visiteurs en 2012. Le nombre total de visites en 2013 était d'environ 293 029 par rapport à 179 542 en 2012, soit une augmentation de 63,2 %* [40].

Après la page d'accueil, les pages les plus fréquemment consultées étaient les rubriques «Consultation», «Supervision» et «Publications». Les statistiques indiquent que la plupart des visiteurs accèdent au site internet par l'intermédiaire d'un lien sur un autre site, par exemple le portail Europa ou le site internet d'une autorité nationale chargée de la protection des données. Environ 35 % des connexions se sont faites par une adresse directe, un onglet ou un lien contenu dans un courrier électronique. Quelques visiteurs seulement ont utilisé les liens proposés par un moteur de recherche.

6.6.2. Newsletter


Newsletter du CEPD

DANS CE NUMÉRO

FAITS MARQUANTS

SUPERVISION

CONSULTATION

IT POLICY

EVENEMENTS

DISCOURS ET PUBLICATIONS

DÉLÉGUÉS À LA PROTECTION DES DONNÉES

FAITS MARQUANTS

Respect de la vie privée et protection des données peuvent rétablir la confiance des consommateurs dans la société numérique

TEN-T EA : assurer la protection des lanceurs d'alerte

European Commission

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

Le format de nos newsletters a été introduit en octobre 2009, la mise en page de chaque numéro étant assurée par l'équipe «Information et communication». En automne 2013, nous avons présenté un nouveau graphisme pour nos newsletters, au terme d'un long processus avec l'Office des publications de l'Union européenne à Luxembourg visant à rafraîchir l'apparence de la newsletter et à accélérer et professionnaliser le processus de production. Nous avons lancé notre nouvelle newsletter en octobre 2013 et avons jusqu'ici reçu des commentaires positifs à son sujet.

Cinq numéros de la newsletter du CEPD ont été publiés en 2013, soit en moyenne un tous les deux mois (juillet et août exclus). Le nombre d'abonnés est passé de 1 750 fin 2012 à environ 1 950 avant la fin 2013. Parmi les abonnés figurent notamment des membres du Parlement européen, du personnel des institutions de l'UE et des autorités nationales chargées de la protection des données, ainsi que des journalistes, des universitaires, des sociétés du secteur des télécommunications et des cabinets juridiques.

6.6.3. Twitter

Twitter est un service de réseau social en ligne qui propose une messagerie instantanée sous forme de microblogs. Le format des messages est une caractéristique inhérente à Twitter car les utilisa-

40 En raison de données manquantes pour la période s'étendant de juin à décembre 2013, les chiffres totaux pour l'année ont été calculés en utilisant les informations pour la période de janvier à mai 2013 et le taux d'évolution pour la même période en 2012.

teurs postent des messages d'un maximum de 140 caractères, appelés «tweets». Il a été décrit comme le *service SMS de l'internet* et a acquis une popularité mondiale.

Le 1er juin 2012, le CEPD a rejoint la communauté Twitter (@EU_EDPS), notre premier pas vers une communication interactive en ligne. Avant cela, notre présence sur Twitter se limitait aux sujets liés au CEPD et à la protection des données qui apparaissaient régulièrement dans des messages Twitter postés par d'autres personnes.

Notre politique d'utilisation de Twitter est publiée sur notre site internet. Elle reflète notre approche progressive visant à maintenir un outil contemporain d'information et de communication qui reste gérable avec des ressources limitées. À la lumière de ces éléments, nous avons maintenu cette politique en 2013, et nous analyserons le succès de notre compte Twitter et actualiserons notre politique s'appliquant à Twitter comme il se doit en 2014.

Conformément à notre politique, nos tweets ont été axés sur nos communiqués de presse, nos nouveaux avis, nos nouvelles publications, nos discours et articles, nos vidéos, des liens vers des articles intéressants consacrés au CEPD et à la protection des données, ainsi que la participation à venir à des événements.

À la fin de l'année 2013, nous avions envoyé 228 tweets, nous suivions 322 autres utilisateurs de Twitter et comptions 952 suiveurs.

6.6.4. LinkedIn

LinkedIn est un réseau professionnel en ligne qui compte plus de 225 millions d'utilisateurs à travers le monde. Le réseau est destiné aux particuliers. Cependant, environ trois millions d'entreprises (entreprises et organisations professionnelles) ont des pages d'entreprises LinkedIn, y compris de nombreuses institutions de l'UE et autorités chargées de la protection des données.

Une page d'entreprise a été automatiquement créée par LinkedIn pour le CEPD, lorsque les concepteurs du réseau se sont rendus compte, par l'intermédiaire des informations transmises par les utilisateurs, que le CEPD était un employeur. Étant donné que les informations contenues sur cette page étaient basiques et inexactes, nous avons pris possession de cette page en décembre 2013 afin de la mettre à jour et de maintenir une image professionnelle sur le site.

La page est un autre moyen de promouvoir le CEPD en tant qu'institution, de renforcer notre présence en ligne et d'améliorer notre visibilité. À la fin de l'année 2013, nous comptions 104 suiveurs.

Le CEPD reste vigilant vis-à-vis des nombreux risques pour la vie privée liés à l'utilisation de services de réseautage social et nous suivons des règles claires dans l'utilisation de ces services.

6.7. Publications

6.7.1. Rapport annuel

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

l'administration, le budget et le personnel. Un chapitre est également consacré aux activités du délégué à la protection des données du CEPD.

Des commentaires montrentmontrent que ce rapport présente un intérêt particulier pour des groupes et des personnes spécifiques aux niveaux international, européen et national, les personnes concernées en général et les agents de l'UE en particulier, les institutions 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 2012 à la commission LIBE du Parlement européen le 29 mai 2013.

6.7.2. Publications thématiques

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

En 2013, nous avons publié trois nouvelles fiches d'information dans ces langues contenant des informations destinées au grand public et à d'autres parties intéressées:

- Fiche d'information 2 - *La transparence dans l'administration européenne: votrevotre droit d'accès aux documents*
- Fiche d'information 3 - *Superviser les institutions et organes de l'UE et faire respecter les principes de protection des données*
- Fiche d'information 4 - *Un œil sur la vidéosurveillance dans l'administration de l'Union européenne.*

6.8. Actions de sensibilisation

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

Alors que nos contrôleurs sont la vraie voix du CEPD, nous considérons que tous les membres du personnel sont les ambassadeurs de l'organisation et sont donc responsables de la communication de nos messages sur la protection des données lorsque nous entrons en contact avec des publics clés.

Nos contrôleurs sont invités à de nombreux événements au cours d'une année, et lorsqu'il est possible et approprié de le faire, ils acceptent d'y diffuser nos principaux messages.

En 2013, Peter Hustinx, contrôleur, a participé à environ 57 évènements, dont 50 au cours desquels il a été invité à prendre la parole. Giovanni Buttarelli, contrôleur adjoint, a assisté à environ 42 événements et a pris la parole à 33 d'entre eux.

Bien qu'un nombre important de ces événements ait porté sur la protection des données ou le respect de la vie privée, ces chiffres reflètent néanmoins la prise de conscience et l'intérêt grandissant pour la protection des données et pour notre institution en tant que point de référence dans le domainedans le domaine.

6.8.1. Journée de la protection des données 2013

Le 28 janvier 2013, les 47 pays membres du Conseil de l'Europe ainsi que les institutions, agences et organes de l'UE ont célébré la septième Journée européenne de la protection des données. Cette date marque l'anniversaire de la Convention 108 du Conseil de l'Europe pour la protection des données à caractère personnel, le premier instrument international juridiquement contraignant dans le domaine de la protection des données.

Cet événement annuel a été, cette année encore, l'occasion pour le CEPD et les délégués à la protection des données des institutions de l'UE de sensibiliser le personnel de l'UE et le grand public à leurs droits et obligations en matière de protection des données, dont la mise en œuvre au sein de l'administration de l'UE est contrôlée par le CEPD.

Dans le cadre de nos efforts de sensibilisation, nous avons réalisé un clipun clip vidéo afin d'illustrer, de manière divertissante et informative, certains droits et risques liés à la protection des données dans notre vie quotidienne.

Nous avons également organisé, en coopération avec le Parlement européen, une conférence commune intitulée *What will the data protection reform change for EU officials and citizens?* («Quelles seront les incidences de la réforme de la protection des données pour les fonctionnaires et les citoyens de l'UE?»). Cette conférence a rencontré un franc succès, seules quelques places debout étaient encore disponibles quelques minutes avant le début du discours de bienvenue prononcé par le secrétaire général du PE, Klaus Welle.

Après quelques brèves présentations, Peter Hustinx, contrôleur, Giovanni Buttarelli, contrôleur adjoint, et Paul De Hert, professeur à la *Vrije Universiteit Brussel* ont participé à un débat.

Nous avons également co-sponsorisé l'exposition A look inside, une exposition d'œuvres d'art originales axée sur le respect de la vie privée et la surveillance, en collaboration avec la *Vrije Universiteit Brussel* et la commission belge de la protection de la vie privée.

6.8.2. Journée portes ouvertes de l'UE 2013

Le samedi 4 mai 2013, nous avons participé à la Journée portes ouvertes annuelle des institutions européennes à Bruxelles, qui marque l'anniversaire de la Déclaration Schuman. La Journée portes ouvertes de l'Union européenne nous offre une excellente occasion de sensibiliser le public à la nécessité de protéger la vie privée et les informations à caractère personnel, ainsi qu'au rôle du CEPD.

Notre stand, situé dans le bâtiment principal du Parlement européen, a connu un franc succès en raison de plusieurs animations que nous proposions. Le personnel du CEPD a travaillé sans relâche pour répondre aux questions relatives à la protection des données et aux droits des citoyens de l'UE en matière de respect de la vie privée.

Un drone équipé d'une caméra diffusait des images en direct (qui n'ont pas été enregistrées) autour de notre stand sur un écran de télévision. Notre objectif était de présenter l'utilisation de drones (voir section 5.5) et de mettre en évidence, d'une manière attractive, les conséquences des nouvelles technologies sur la vie privée. Nous avons également placé deux ordinateurs sur notre stand, sur lesquels était installée une application internet de suivi. Les visiteurs ont pu se faire une idée de la façon dont une grande partie de leurs activités en ligne est suivie lorsqu'ils naviguent sur l'internet, et le personnel du CEPD était présent pour répondre aux questions et donner des conseils.

Les visiteurs ont également pu participer à notre questionnaire sur la protection des données et emporter de la documentation.

7 ADMINISTRATION, BUDGET ET PERSONNEL

Notre objectif stratégique

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

Notre principe directeur

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

7.1. Introduction

Dans le climat actuel d'austérité économique et d'assainissement budgétaire, le CEPD a dû *«faire plus avec moins»* pour la deuxième année consécutive. Pour ce faire, nous avons poursuivi nos efforts en faveur d'une meilleure planification, d'un meilleur suivi et d'une répartition des ressources plus efficace.

Ce climat d'austérité a rendu l'élaboration du projet de budget pour 2014 relativement difficile, étant donné que celle-ci coïncidait avec l'élaboration du nouveau cadre financier pluriannuel pour 2014-2020. Cet exercice de planification prévisionnelle s'est avéré compliqué en raison de l'issue incertaine de la révision du cadre européen en matière de protection des données et de son incidence sur le rôle et les responsabilités du CEPD.

En 2013, nous avons déployé des efforts importants et investi des ressources considérables dans la poursuite de la professionnalisation de la fonction RH, dans le but de libérer des ressources affectées à des tâches purement administratives et bureaucratiques en faveur de processus RH plus substantiels. Par exemple, SYSPER2 s'est vu doté, avec succès, de nouveaux modules pour la gestion du personnel, tels que NDP (Numérisation de Dossier Personnel) qui donne au personnel du CEPD un accès direct à leur dossier personnel.

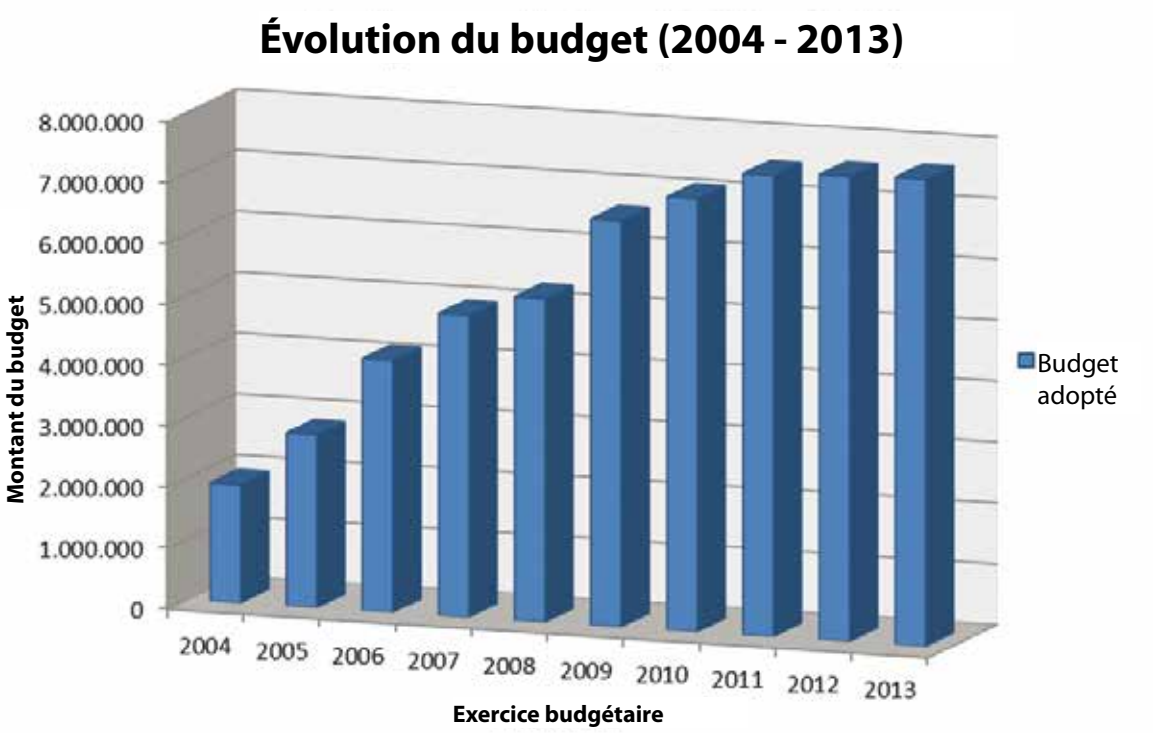
Compte tenu de nos ressources limitées, il peut s'avérer difficile d'établir un équilibre entre les attentes stratégiques et les objectifs qu'il est réellement possible d'atteindre.

7.2. Budget, finances et marchés publics

7.2.1. Budget

Le budget du CEPD s'établissait à 7 661 409 EUR pour l'exercice 2013, soit une hausse de 0,49 % par rapport au budget 2012. Vu le taux d'inflation de 1,9 % pour 2013, ce chiffre représente en fait une diminution nominale.

Pour la deuxième année, notre budget a diminué au cours d'une phase de croissance. Le budget du CEPD est faible par rapport à d'autres institutions, de sorte que la proportion des salaires du personnel représente 51 % du budget total et notre marge



de manœuvre est limitée en conséquence. Néanmoins, en réduisant ou en gelant une grande majorité de nos crédits à 0 %, nous avons réussi à appliquer une politique d'austérité qui allait au-delà du plafond de 1,9 % fixé par la Commission; en plus du crédit supplémentaire concernant les nouveaux salaires, l'augmentation globale du budget du CEPD a été limitée à 0,49 %.

Ce résultat a été rendu possible grâce à un effort considérable pour établir des priorités, un redéploiement stratégique des ressources ainsi qu'une volonté continue de «faire plus avec moins». Les examens trimestriels de l'exécution de notre budget ont permis d'améliorer les taux d'exécution, lesquelles s'améliorent d'année en année: 76,9 % en 2011, 83,2 % en 2012 et 84,7 % en 2013[41].

En raison des spécificités du budget du CEPD mentionnées ci-dessus, il est extrêmement difficile d'atteindre un taux d'exécution supérieur à 85 %, en raison principalement d'événements inévitables, comme le renouvellement du personnel au cours de la seconde moitié de l'année qui a eu une incidence énorme sur le taux global d'exécution.

41 Afin d'être cohérent avec l'ensemble des indicateurs clé de performance mis en place pour suivre la mise en œuvre de la stratégie 2013-2014 (voir page 20), le CEPD a adopté, en 2013, une nouvelle méthode de calcul du taux d'exécution du budget. Selon cette méthode, le taux actuel s'appuie sur les crédits de paiement exécutés en 2013 en ce qui concerne le budget de 2013, tandis que la méthode précédente comprenait, en outre, l'exécution estimée de ces crédits de paiement reportés à l'année suivante.

En outre, la décision inattendue de la Cour de justice de l'Union européenne sur l'ajustement des salaires a eu une incidence négative sur le taux d'exécution final. Si l'ajustement des salaires de 2011 avait été versé en 2013, le taux d'exécution du budget 2013 aurait augmenté pour atteindre 87,2 %.

Grâce à la politique menée en faveur d'une croissance modérée mais durable, comme prévu dans les perspectives financières pour la période 2007-2013, nous avons complété avec succès le tableau des effectifs du CEPD avec les deux postes accordés par l'autorité budgétaire pour contribuer à la réalisation des activités de base suivantes:

- renforcer les efforts de supervision et de mise en application;
- fournir des ressources pour un nouveau secteur «Politique IT» chargé de veiller à ce que les progrès technologiques dans les technologies de l'information soient dûment pris en considération;
- contribuer aux discussions en cours au sujet du nouveau cadre juridique de protection des données, en particulier la révision du règlement (CE) n° 45/2001;
- renforcer la coopération avec les autorités nationales de contrôle dans la supervision coordonnée de systèmes d'information à grande échelle, à savoir trois nouveaux systèmes dans le cadre du mandat du CEPD en 2012 et 2013;
- mettre en place des mécanismes adéquats pour une meilleure planification, une meilleure coor-

dination, ainsi qu'une répartition et une utilisation plus efficaces des ressources afin d'être en mesure de faire plus avec les mêmes ressources, voire moins, à l'avenir.

En ce qui concerne l'avenir, les discussions en cours au sein du Conseil et du Parlement sur le nouveau cadre juridique de la protection des données proposé par la Commission le 25 janvier 2012 pourraient aboutir à de nouveaux rôles et responsabilités pour le CEPD, notamment à la fourniture d'un secrétariat indépendant pour un nouveau comité européen de la protection des données qui aura pour tâche d'assurer la coordination et la cohérence de la protection des données au niveau de l'UE.

Afin de souligner l'incidence que cette réforme pourrait avoir sur les ressources de notre petite institution, un nouveau titre III a été ajouté à notre budget. Cependant, comme les négociations entre le Conseil et le Parlement sont en cours, aucun crédit supplémentaire n'a été demandé pour le nouveau titre III pour l'exercice 2013.

7.2.2. Finances

La déclaration d'assurance de la Cour des comptes européenne concernant l'exercice financier 2012 (DAS 2012) n'a pas fait état de préoccupations concernant le CEPD ni formulé de recommandations à son intention. Néanmoins, dans le cadre d'une gestion financière saine et en vue d'améliorer la fiabilité et la qualité de nos données financières:

a. les chartes des missions et responsabilités des ordonnateurs délégués et subdélégués ont été signées au cours du premier semestre 2013;

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

c. une décision établissant les règles relatives au remboursement des experts externes engagés pour effectuer des tâches spécifiques a été adoptée en juillet 2013.

En 2013, la Commission a continué de nous 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. Un accord de niveau de service en la matière ainsi que pour l'utilisation du système comptable informatique de la Commission (ABAC) a été signé avec la DG Budget de la Commission en mai 2013.

Les chartes concernant les ordonnateurs délégués et subdélégués ont été élaborées et signées par le directeur du CEPD et le chef de l'unité RHBA.

7.2.3. Marchés publics

À la suite de l'entrée en vigueur du nouveau règlement financier le 1er janvier 2013, une version mise à jour de nos lignes directrices pas à pas en matière de marchés publics pour les contrats de faible valeur a été adoptée le 30 janvier 2013. Cependant, aucune procédure d'adjudication n'a été lancée en 2013.

Dans le cadre de nos efforts en faveur d'une plus grande autonomie, nous avons commencé à prendre part au processus interinstitutionnel concernant les appels d'offres. Cela nous a permis de conclure des contrats spécifiques directement avec les entreprises auxquelles ces contrats-cadres ont été attribués, plutôt que de compter sur les grandes institutions agissant comme intermédiaires pour faciliter l'attribution de contrats en notre nom. La majorité des appels d'offres qui nous intéresse relève de domaines techniques et informatiques.

7.3. Ressources humaines

7.3.1. Recrutement

Le recrutement est l'une des principales activités dans les ressources humaines (RH) et une fonction stratégique pour notre institution. Cette tâche associe l'équipe des ressources humaines ainsi que les responsables hiérarchiques et les collègues participant au comité de sélection. Il s'agit d'une activité qui prend du temps, mais elle est importante afin de trouver la personne adéquate pour occuper un poste vacant aussi rapidement que possible.

Indépendamment de notre taille relativement petite, nous sommes soumis aux mêmes normes élevées de recrutement que les grandes institutions européennes (qui disposent de personnel affecté à temps plein aux activités de sélection et de recrutement) et aux mêmes règles énoncées dans le statut des fonctionnaires de l'Union européenne. Cela implique un degré élevé de polyvalence dans les fonctions exercées par notre personnel RH, lequel possède une variété de responsabilités qui seraient traitées par différentes unités ou directions au sein des grandes institutions.

Conformément au statut des fonctionnaires, les membres du personnel du CEPD sont recrutés en tant que fonctionnaires ou agents contractuels. Le CEPD recrute aussi du personnel externe, tel que des

experts nationaux détachés, des intérimaires, des stagiaires, etc.

Les fonctionnaires sont recrutés auprès des autres institutions européennes par des transferts interinstitutionnels, ou à partir de listes de réserve des lauréats des concours généraux de l'Office européen de sélection du personnel (EPSO). Au cours des quatre dernières années, la majorité des fonctionnaires spécialisés dans la protection des données a été recrutée à partir d'une liste de lauréats d'un concours dans le domaine de la protection des données organisé par EPSO à la demande du CEPD. Ces listes ont été clôturées à la fin de l'année 2013. Compte tenu de la proposition d'augmenter, à l'avenir, les effectifs du secrétariat, nous avons entrepris des discussions avec EPSO sur l'organisation éventuelle d'un concours dans le domaine de la protection des données en vue d'engager de nouveaux spécialistes à l'avenir.

Au cours du dernier trimestre 2013, l'autorité budgétaire nous a accordé deux nouveaux postes de fonctionnaires qui ont été mis en attente jusqu'en 2014, selon les ajustements exigés par l'autorité budgétaire en vue de réaliser des coupes progressives mais significatives dans le tableau des effectifs (le nombre de membres du personnel autorisé par institution et le budget associé). Ces ajustements s'appliquent à toutes les institutions de l'UE dans le cadre du nouveau statut des fonctionnaires, qui est entré en vigueur le 1er janvier 2014.

En 2013, nous avons recruté un fonctionnaire européen pour notre équipe «Politique législative et consultation». En outre, nous avons recruté huit agents contractuels pour l'ensemble des équipes, à l'exception de l'équipe «Politique IT».

Les agents contractuels sont recrutés pour une période qui varie de quelques mois à trois ans, afin de couvrir nos besoins à court terme (remplacements de congés de maternité, par exemple) ou pour aider à gérer les charges de travail stratégiques que le personnel existant n'est pas en mesure de couvrir seul.

Outre les activités de recrutement liées au renouvellement du personnel, cet élément explique le taux de croissance stable des effectifs en 2013. Voir le graphique ci-dessous.

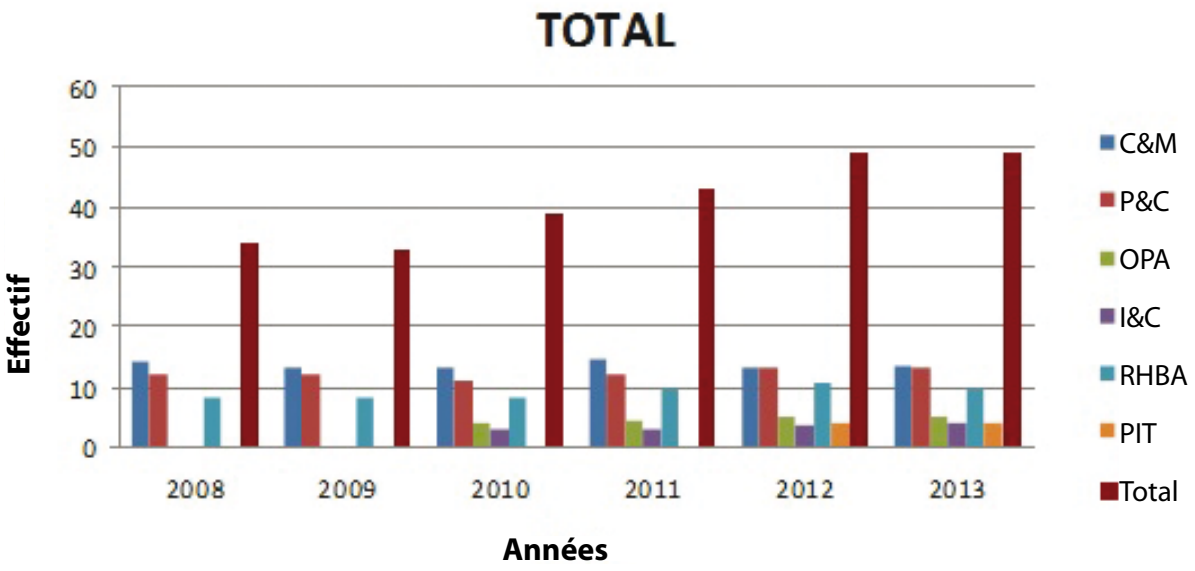
7.3.2. Professionnalisation de la fonction RH

En février 2013, l'équipe RH a soumis son deuxième rapport décrivant ses indicateurs et ses activités passées et à venir au conseil d'administration du CEPD.

L'équipe RH a suivi de près les activités du programme de professionnalisation RH de la Commission européenne, en assistant à plusieurs séminaires et cours. Le conseiller principal de la DG RH de la Commission européenne, qui est responsable de ce programme, a interrogé l'ensemble du personnel du CEPD sur son engagement, et l'analyse des résultats de cette enquête nous a permis d'élaborer un plan d'action qui a été adopté en décembre 2013. Ce plan devrait, entre autres, améliorer notre communication interne et les conditions de travail.

Toutes ces activités contribuent à une professionnalisation accrue de la fonction RH au sein de notre institution compacte.

Évolution du personnel du CEPD sur la période 2008-2013



7.3.3. Programme de stages

En 2013, notre organisation a continué d'investir dans le programme de stages créé en 2005, Ce programme donne aux diplômés universitaires récents l'occasion de mettre en pratique les connaissances acquises à l'université. Les stages permettent également d'acquérir de l'expérience pratique dans nos activités au quotidien au sein des unités opérationnelles ainsi que dans l'unité «Ressources humaines, budget et administration» (RHBA) et le secteur «Information et communication» (I&C).

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

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

7.3.4. Programme pour les experts nationaux détachés

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

En 2012, le détachement d'un expert national allemand est arrivé à son terme et un nouvel expert national a été recruté auprès de l'autorité britannique de protection des données (ICO). Étant donné que le contrat de l'expert britannique prendra fin en avril 2014, nous avons lancé, fin 2013, la procédure de sélection visant à recruter un nouvel expert national.

7.3.5. Organigramme

Outre un léger changement, le partage et le repositionnement des fonctions de gestion de la planification et des dossiers, l'organigramme du CEPD est resté stable en 2013.

7.3.6. Conditions de travail

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

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

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

La phase pilote de notre décision relative au télétravail a été prolongée jusqu'à la fin juin 2013 et puis légèrement modifiée. Il est possible de choisir entre deux régimes de télétravail: structurel et occasionnel. Le télétravail structurel est récurrent (maximum un jour ou deux demi-journées par semaine), tandis que le télétravail occasionnel est conçu pour les situations dans lesquelles un membre du personnel n'est pas en mesure de se rendre au bureau pour une raison légitime mais est malgré tout capable de travailler (maximum 12 jours par an).

En 2013, cinq membres du personnel ont eu recours au télétravail structurel et soixante-dix demandes de télétravail occasionnel ont été déposées.

7.3.7. Apprentissage et développement des compétences

L'apprentissage et le développement des compétences ont continué à croître en 2013. L'importance de la formation a été soulignée dans la stratégie 2013-2014 du CEPD et constitue un indicateur clé de performance, mesurant le nombre de jours de formation achevés par le personnel.

En 2013, sur 277,5 jours de formation prévus dans les plans de formation de notre personnel, 235,85 avaient été pris avant la fin décembre 2013. Cela correspond à un taux d'exécution de 85 %.

Le tableau ci-dessous indique le nombre de jours de formation accomplis par chaque équipe (les sessions de formation pour notre nouveau système de gestion des dossiers ne sont pas prises en considération):

Équipe	Taux d'exécution
C&M	**68,07 %**
P&C	**64,31 %**
PIT	**79,56 %**
OPA	**42,61 %**
I&C	**43,62 %**
RHBA	**82,25 %**
Directeur	**100,00 %**

Le tableau ci-dessous indique les raisons pour lesquelles la formation n'a pas pu être ou n'a pas été suivie en 2013, ainsi que les conséquences (en nombre de jours et budget):

Raisons	Nombre de jours	Budget
Départ parmi le personnel	18	3 025
Congé de maternité	9	1 485
Aucune session de formation disponible (ou complète, ou ne convenant pas)	12	3 110
Personne pas acceptée (aucune dérogation présentée concernant les conditions de recevabilité)	1,5	0
Cours remplacé par un autre	3,5 (différence entre les 2 cours)	856 (différence entre les 2 cours)
Cours prévu trop semblable à un autre déjà suivi	3	500
Changement de la durée du cours (nécessité d'annuler en raison d'un horaire à temps partiel)	0,5	0
Cours annulé par les organisateurs (manque de participants)	2	600
Cours annulé par le participant (raison lié au travail)	2	335
Total	**51,5**	**9 911**

En 2013, une formation sur mesure en matière de planification et de suivi a été organisée pour l'équipe de gestion.

7.3.8. Activités sociales et questions familiales

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 mentor, ils rencontrent aussi les membres de l'unité RHBA, budget et administration, qui leur remettent notre guide administratif et leur communiquent les informations concernant nos propres procédures.

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

En 2013, diverses activités sociales ont été organisées avec la participation du comité du personnel du CEPD.

The Cloud, une salle consacrée aux activités sociales et située dans notre nouveau bâtiment, a été utilisé pour un certain nombre d'activités, dont des fêtes d'anniversaire, des petits déjeuners et un cours de Pilates hebdomadaire. C'est également dans cette salle qu'ont lieu les réunions du comité du personnel.

7.4. Fonctions de contrôle

7.4.1. Contrôle interne

Notre système de contrôle interne, en vigueur depuis 2006, gère le risque de non-réalisation des objectifs. En 2012, nous avons élargi la liste des actions afin de garantir un contrôle interne plus efficace des processus en place. Une décision révisée des normes de contrôle interne a été adoptée en janvier 2013 pour simplifier l'approche, augmenter l'appropriation et renforcer l'efficacité de ces normes. L'outil utilisé pour assurer le suivi de la mise en œuvre des normes de contrôle interne a été entièrement révisé en conformité avec la nouvelle décision en la matière. Lors de la réunion sur l'évaluation globale des risques qui a eu lieu en 2013, le service d'audit interne (SAI) de la Commission européenne a jugé que cet outil était efficace.

En conséquence de la décision sur la gestion des risques adoptée par le CEPD en juillet 2012 (où nous nous sommes appuyés sur notre système d'évaluation des risques destiné à les gérer, en explorant les moyens de surmonter ces risques), le premier registre des risques a été ajouté à notre plan de gestion annuel (PGA) en janvier 2013. À la suite de réunions organisées au début de l'année avec tous les chefs d'équipes afin d'identifier les risques, un rapport d'avancement sur la gestion des risques a été publié en juillet 2013.

Le coordinateur du contrôle interne du CEPD a reconnu les efforts considérables déployés par toutes les équipes pour mettre en œuvre la plupart des vérifications et des contrôles définis au cours des réunions. Les risques associés aux lourdes charges de travail en raison d'une planification trop ambitieuse et de la pression inhérente à la fin du mandat de nos contrôleurs sont atténués par les vérifications et les contrôles mis en place par toutes les équipes, ce qui a profité à l'institution de manière significative.

La gestion des risques est un élément essentiel de notre stratégie globale de gestion de la qualité totale (GQT) et notre coordinateur du contrôle interne a suivi une formation relative au cadre commun d'évaluation en 2013, dans le cadre de la stratégie GQT. Un questionnaire d'auto-évaluation qui analyse tous les processus opérationnels et administratifs d'une organisation doit être rempli. Ce questionnaire est accompagné d'une liste de critères. Le cadre commun d'évaluation nous donnera un aperçu complet et mettra en évidence les processus qui doivent être affinés.

Compte tenu de notre rapport annuel d'activité et de la déclaration d'assurance signée par l'ordonnateur délégué, nous estimons que les systèmes de contrôle interne mis en place fournissent une assu-

rance raisonnable quant à la légalité et à la régularité des opérations dont nous sommes responsables.

7.4.2. Audit interne

L'auditeur interne de la Commission, le chef du SAI, est également l'auditeur interne du CEPD.

En octobre 2013, le SAI a publié le rapport annuel d'audit interne (RAAI – article 99, paragraphe 3, du règlement financier) pour 2012, qui résumait les activités d'audit effectuées en 2012 au CEPD.

La volonté du SAI d'effectuer un audit des ressources humaines en 2013, qui ne s'est pas concrétisée, a entraîné la réalisation d'un examen interne au sein de la fonction RH, conduisant à des améliorations tangibles.

Une visite d'audit de suivi effectuée par le SAI en juin 2013 a conclu que:

- deux recommandations importantes découlant de l'examen limité des normes de contrôle interne par le SAI avaient été mises en œuvre de manière adéquate (contrôles des procédures de mission et de la supervision des dossiers du personnel);
- une recommandation souhaitable formulée lors de l'audit du SAI sur l'unité Supervision et Mise en application avait été mise en œuvre de manière adéquate;
- six recommandations formulées lors de l'audit du SAI sur l'unité Supervision et Mise en application n'étaient pas prêtes à être examinées au moment de la visite de suivi et n'ont donc pas été évaluées. Cependant, en juillet 2013, la nouvelle version de notre manuel traitant des contrôles préalables comprenait certaines modifications apportées en réponse à ces recommandations.

Une recommandation en attente concerne un système d'archivage de dossiers. Comme décrit dans la section 7.6.2, le système de gestion des dossiers du CEPD est devenu opérationnel en octobre 2013; il est donc raisonnable de s'attendre à ce que cette recommandation soit clôturée dans un avenir proche.

En plus de cet audit de suivi, le SAI a rendu visite au CEPD en septembre-octobre 2013 pour entreprendre une évaluation globale des risques de nos activités. Dans ses conclusions générales, le SAI a estimé qu'il était évident que nous avions déployé des efforts considérables qui avaient abouti à des améliorations substantielles depuis la dernière évaluation en 2011. La plupart des processus qui étaient précédemment considérés comme insuffisamment matures ou sous contrôle se sont améliorés et les quelques processus encore considérés comme insuffisamment matures sont examinés (travaux en cours).

7.4.3. Audit externe

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

Pour la décharge relative à l'année 2012, le CEPD a répondu de façon satisfaisante aux questions posées par la Cour. En juin 2013, pour la deuxième année consécutive, la Cour a envoyé au CEPD une lettre indiquant que «l'audit effectué n'a donné lieu à aucune observation».

La Cour des comptes (article 162 du règlement financier) a déclaré n'avoir repéré aucun point faible significatif dans les domaines audités et affirmé que les mesures mises en œuvre à la suite de son audit (allocations sociales) étaient effectives. Nous avons pris acte de l'analyse de la Cour et continuerons d'améliorer nos systèmes en vue d'un suivi et d'un contrôle en temps utile.

Le 22 janvier 2013, le directeur du CEPD a participé à la réunion de décharge de la commission du contrôle budgétaire du Parlement européen et répondu aux questions posées par les membres de cette commission. Le Parlement européen a accordé la décharge au CEPD pour l'exécution de notre budget pour l'exercice 2011.

7.5. Infrastructure

Les bureaux du CEPD se situent dans l'un des bâtiments du Parlement européen, et nous étions heureux de déménager dans nos nouveaux bureaux, Rue Montoyer 30 à Bruxelles, au début du mois d'octobre 2012. Le loyer et les autres coûts connexes sont pris en charge par notre institution et celle-ci continue de gérer l'inventaire de son mobilier de manière indépendante. La DG ITEC du Parlement nous apporte également un soutien en matière d'informatique et d'infrastructure sur la base d'une taxe

forfaitaire mutuellement approuvée pour les services informatiques.

En 2013, nous avons réalisé un certain nombre de travaux de décoration dans nos nouveaux bureaux, dont l'amélioration de la grande salle de réunion au rez-de-chaussée utilisée pour organiser des ateliers et des séminaires. L'acquisition et l'installation d'un système de vidéoconférence nous a permis de participer à de nombreuses réunions externes à des endroits plus éloignés sans quitter nos bureaux, ce qui nous a permis de réaliser des économies sur les frais de voyage et d'hébergement.

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

7.6. Environnement administratif

7.6.1. Assistance administrative et coopération interinstitutionnelle

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

En 2012, dans la perspective de notre déménagement imminent vers de nouveaux bureaux, le Parlement européen a proposé de réviser l'accord administratif général signé avec le CEPD, ainsi que les annexes relatives à l'infrastructure, à la sécurité, à l'informatique, etc. afin de mieux refléter les besoins et les obligations des deux parties et de simplifier et d'uniformiser ces textes. Les aspects techniques du nouvel accord administratif ont été conclus en 2012 et l'accord a été officiellement signé en juillet 2013. Cette coopération administrative est essentielle pour nous dans la mesure où elle augmente l'efficacité et permet des économies d'échelle.

Outre le déménagement dans nos nouveaux bureaux, nous avons mis en place un nouveau plan de continuité des activités au début 2013, en étroite coopération avec le Parlement européen.

Une nouvelle décision en matière de sécurité a été élaborée et sera adoptée au début 2014.

En 2013, nous avons poursuivi notre coopération interinstitutionnelle étroite avec diverses directions générales de la Commission (DG «Personnel et administration», DG «Budget», service d'audit interne, DG «Éducation et culture»), l'Office des paiements (PMO), l'École européenne d'administration (EEA) et le Centre de traduction des organes de l'Union européenne. Cette coopération se fait au moyen d'accords de niveau de service, qui sont régulièrement mis à jour.

Nous avons également continué de participer aux appels d'offres interinstitutionnels, accroissant ainsi l'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 d'EPSO, la commission paritaire commune et le comité de préparation pour les affaires sociales.

7.6.2. Gestion des documents

Notre nouveau système de gestion des dossiers est devenu opérationnel en octobre 2013. Le système a été choisi à la suite d'une évaluation de plusieurs produits sur le marché et une analyse approfondie des besoins du CEPD, y compris les fonctionnalités, les opérations, les aspects économiques, la sécurité et les besoins en matière de protection des données. En plus des négociations commerciales et de la personnalisation fonctionnelle, nous avons évalué les systèmes de gestion de la sécurité des fournisseurs et fixé les détails en matière de sécurité et de protection des données dans les contrats et les accords de niveaux de service.

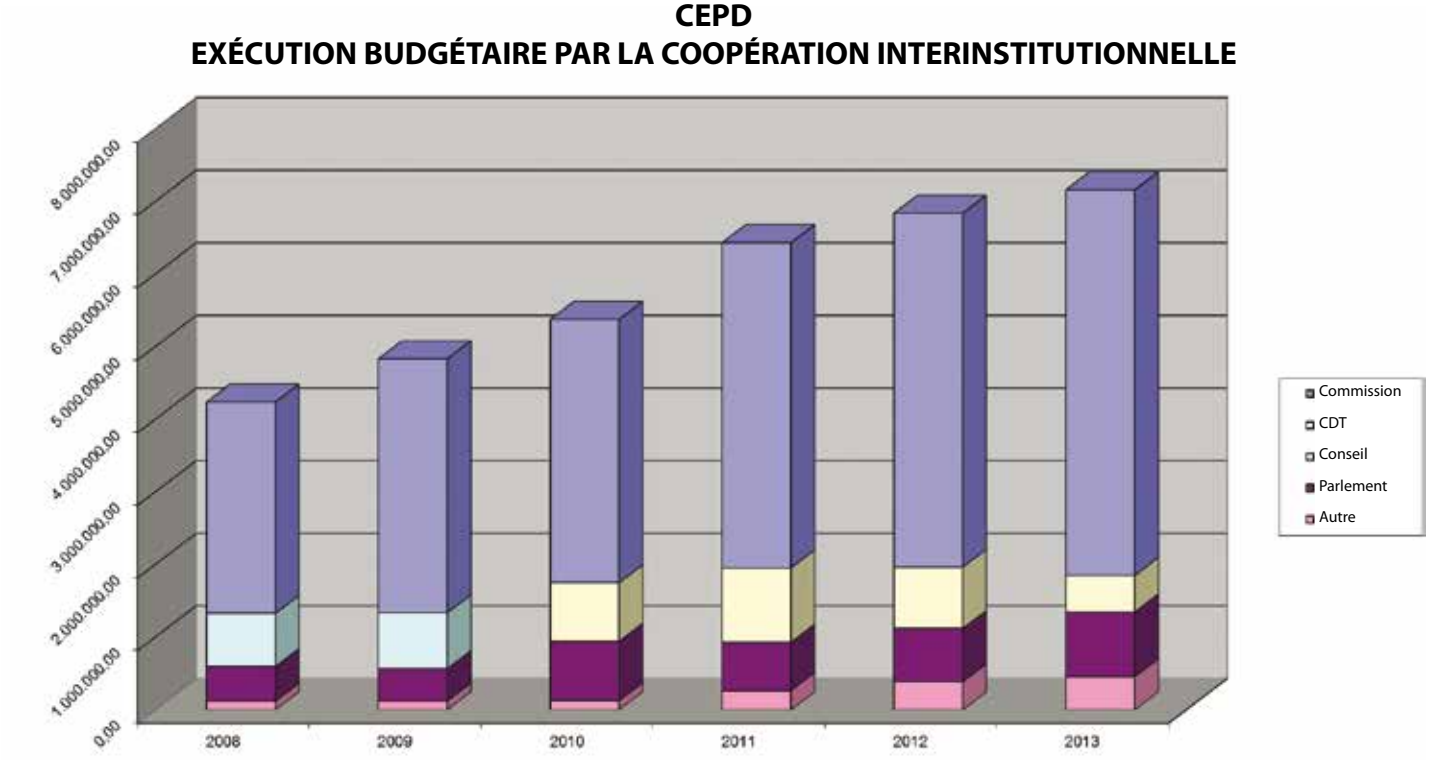
Au cours de l'année 2013, l'ensemble du répertoire des dossiers du CEPD a été transféré avec succès vers le système de gestion des dossiers et les opérations ont pu se poursuivre sans interruption. Des fonctionnalités supplémentaires seront progressivement intégrées dans le système en temps voulu.

Certaines modifications organisationnelles ont été opérées pour soutenir le lancement du système de gestion des dossiers. Notre équipe «Politique IT» est responsable des opérations, de la sécurité et de la gestion de projets liées au système de gestion des

dossiers. Par conséquent, un poste de gestionnaire des documents/archiviste a été créé au sein de l'équipe avec la responsabilité principale de garantir la fonctionnalité du système et la prise en charge des processus opérationnels par celui-ci. Le poste intègre également la fonction d'administrateur opérationnel du système de gestion des dossiers et d'assistance interne de deuxième niveau.

L'assistance de premier niveau est assurée par un membre de chaque équipe, nommé «super-utilisateur». Ces super-utilisateurs reçoivent une formation et un encadrement spécifiques afin qu'ils puissent aider leurs collègues lorsqu'ils rencontrent des problèmes qui n'ont pas été abordés dans la formation introductive au système de gestion des dossiers. Les super-utilisateurs transmettent des commentaires au gestionnaire des documents sur le fonctionnement du système et l'aident à déterminer les modifications qu'il convient éventuellement d'apporter.

CEPD
EXÉCUTION BUDGÉTAIRE PAR LA COOPÉRATION INTERINSTITUTIONNELLE



8 DÉLÉGUÉ À LA PROTECTION DES DONNÉES DU CEPD

8.1. Le DPD du CEPD

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 qui sont spécialisés dans les questions de protection des données et y sont sensibles, et apporter des solutions susceptibles de servir de références aux autres institutions.

Pour renforcer cette indépendance et consolider son expertise, le DPD possède le titre de *Certified Information Privacy Professional/Europe* (CIPP/E) et cherchera à obtenir une autre certification en 2014, à savoir celle de *Certified Information Privacy Manager* (CIPM).

Notification des traitements

8.2. Le registre des traitements

En vertu de l'article 26 du règlement, le DPD doit tenir un registre de tous les traitements qui lui sont notifiés. Le registre comprend tous les traitements pertinents au sein de l'institution et répertorie chaque notification relative à ces traitements.

Après la révision de toutes les notifications relatives aux traitements du CEPD en 2011 – si un changement se produit dans les conditions d'un traitement et a des conséquences sur des données à caractère personnel, la notification de ce traitement devrait être révisée – ainsi que la mise à jour de l'inventaire (qui répertorie tous les traitements de l'institution, l'équipe en charge du processus et la date de la notification) et sa mise en œuvre en 2012, l'année 2013 a été consacrée à la mise en œuvre de l'inventaire. Il y a eu 4 nouvelles notifications et 4 révisions de notifications existantes.

De ce fait, 97,7 % de l'inventaire ont été notifiés et mis en œuvre.

Conformément aux lignes directrices du CEPD, le DPD s'est chargé des notifications soumises au CEPD au titre de l'article 27, paragraphe 2, du règlement (CE) n° 45/2011. Cependant, très peu de notifications ont relevé de cette disposition en 2013.

> L'article 27, paragraphe 2, du règlement dresse une liste non exhaustive des traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées. Ceux-ci sont soumis au contrôle préalable du CEPD (article 27, paragraphe 1).

Le principal objectif du DPD pour 2014 est de traiter la révision de toutes les notifications relatives aux procédures en matière de RH qui sont liées à la mise en œuvre du nouveau statut des fonction-

naires. Les procédures relatives aux enquêtes administratives, aux procédures disciplinaires et aux procédures anti-harcèlement seront également notifiées une fois qu'elles auront été approuvées au cours de l'année 2014.

8.3. Enquête de 2013 du CEPD sur le statut des DPD

En juin 2013, le CEPD a lancé un questionnaire sur le statut des DPD afin de contrôler le respect, par les institutions et organes de l'Union européenne, de l'article 24 du règlement (CE) n° 45/2001. En juillet, le directeur du CEPD a répondu à l'enquête en donnant une vue d'ensemble complète du statut et de l'évolution de la fonction de DPD au sein du CEPD lui-même.

Les informations fournies concernent l'inventaire des traitements, le registre établi en vertu de l'article 26, la formation en matière de protection des données fournie au personnel, les clauses contractuelles pour les sous-traitants, la participation du DPD à la conception de nouveaux traitements et les transferts à des destinataires qui ne sont pas soumis aux dispositions nationales mettant en œuvre la directive 95/46/CE.

8.4. Information et sensibilisation

De gauche à droite: Peter Hustinx, Contrôleur; Sylvie Picard, Déléguée à la protection des données; Giovanni Buttarelli, Contrôleur adjoint

Le DPD accorde une grande importance à la sensibilisation du personnel participant aux différents traitements et à la communication du respect des règles de protection des données au sein du CEPD.

La rubrique consacrée au DPD sur le site internet du CEPD constitue une partie des activités de communication externe du CEPD auxquelles le DPD participe (voir également la section 2.7.3). Le site internet du CEPD fournit des informations sur le rôle et les activités du DPD et est actualisé régulièrement afin que le public puisse consulter le registre actualisé et toutes les notifications.

Les DPD des institutions et organes de l'Union européenne se réunissent à intervalles réguliers pour partager leurs expériences et discuter de sujets pertinents. Dans le cadre de ce réseau productif, le DPD a pris part à la réunion du réseau des DPD qui s'est tenue à Lisbonne en mars 2013 et a accueilli la réunion du réseau des DPD à Bruxelles en novembre. Ces réunions sont une occasion unique de créer des réseaux, d'évoquer les préoccupations communes et d'échanger les bonnes pratiques.

L'organisation de la réunion des DPD à Bruxelles a constitué un défi intéressant qui a permis au DPD de renforcer son réseau et de veiller à ce que les questions importantes pour les DPD soient discutées et présentées aux contrôleurs du CEPD au cours de la deuxième journée de la réunion.

La relation intéressante entre le règlement (CE) n° 45/2001 sur la protection des données et le règlement (CE) n° 1049/2001 relatif à l'accès du public aux documents a été examinée au cours des ateliers. L'accent a été mis en particulier sur les questions suivantes:

1. l'accès aux dossiers contenant les noms des personnes et les détails de leur statut (fonctionnaires en service actif/inactif - personnel AD/AST / personnel externe);

2. l'accès aux dossiers contenant d'autres types de données à caractère personnel (par exemple, l'évaluation ou le statut du personnel);

3. la nécessité de transférer les données à caractère personnel et le préjudice éventuel causé aux intérêts légitimes de la personne concernée conformément à l'article 8 du règlement (CE) n° 45/2001;

4. l'accès à de grandes quantités de données ou de documents et le principe de l'effort raisonnable;

5. le rôle du consentement et de l'information dans le processus d'accès aux documents.

Les ateliers de la réunion ont permis à tous les DPD de partager leur expérience pratique sur ce sujet.

La réunion de Bruxelles a été la dernière réunion des DPD à laquelle a assisté Peter Hustinx, qui a dirigé le réseau au cours des 10 dernières années, avant la fin de son mandat de contrôleur. Une réception d'adieu informelle a permis aux DPD de partager leurs impressions et anecdotes avec lui.

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

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

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

9 PRINCIPAUX OBJECTIFS POUR 2014

Les objectifs suivants ont été sélectionnés pour 2014 dans le cadre de la stratégie générale pour 2013-2014. Les résultats obtenus figureront dans le rapport de 2015.

9.1. Supervision et mise en application

Nous continuerons à promouvoir le principe de la responsabilisationresponsabilisation, tel que proposé parmi les changements à apporter au cadre juridique de la protection des données. Cela signifie que l'administration de l'Union européenne devra prendre toutes les mesures nécessaires pour assurer la conformité avec le règlement relatif à la protection des données et devra conserver la documentation qui démontre la conformité.

- **Orientations et formation**

Les DPD et les CPD jouent un rôle essentiel pour garantir la pleine responsabilité. Nous continuerons donc à développer les formations et orientations destinées aux DPD et aux CPD, et à favoriser des contacts étroits avec les DPD et leur réseau.

À cet égard, nous avons l'intention d'organiser des activités de formation pour les nouveaux DPD, ainsi qu'un atelier sur les droits des personnes concernées, et d'adopter des lignes directrices sur des sujets tels que la déclaration d'intérêts, les transferts de données et les communications électroniques. Nous comptons également mettre à jour les lignes directrices existantes en tenant compte des évolutions récentes. Dans le cadre de notre plan de soutien aux DPD, nous poursuivrons nos travaux sur le programme de certification de l'Institut européen d'administration publique (IEAP) pour les DPD.

- **Visites**

Au sein de l'administration de l'Union, l'engagement de la direction et la vigilance des personnes responsables du traitement des données constituent des conditions essentielles pour garantir le respect effectif de la protection des données. Nous continuerons donc à investir des ressources pour mener des actions de sensibilisation à tous les niveaux et pour obtenir l'engagement de la direction, principalement au moyen de visites.

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

L'une des difficultés permanentes que nous rencontrons dans nos activités de supervision consiste à garantir le respect approprié des règles en matière de protection des données, en tenant compte des contraintes liées à l'administration de l'Union. Dès lors, nous poursuivrons non seulement le dialogue avec les responsables du traitement des données, mais nous améliorerons également la formulation de nos avis afin de promouvoir une application pragmatique et pratique du règlement. Nous veillerons par ailleurs à améliorer la présentation de nos avis afin de rendre leur contenu aussi accessible que possible.

- **Inspections**

Les inspections resteront un élément important de la politique de conformité et de mise en application du CEPD, sur la base des critères définis dans notre stratégie d'inspection adoptée en 2013.

- **Suivi relatif à nos avis et décisions**

Ces dernières années, le nombre d'avis relatifs à des contrôles préalables a connu une augmentation considérable, en raison du délai applicable aux contrôles préalables ex post, fixé à juin 2013. Le défi pour 2014 consiste à faire en sorte que les recommandations formulées dans ces avis soient effectivement suivies. Ce sera le cas pour les contrôles préalables, ainsi que pour les réclamations, les consultations sur des décisions administratives, les inspections et les visites.

9.2. Politique et consultation

Le principal objectif de notre fonction consultative est de faire en sorte que le législateur européen ait conscience des normes applicables en matière de protection des données, intègre des mesures de protection des données dans les nouvelles législations et expose les mesures conçues pour atteindre cet objectif.

Nous devrons remplir notre rôle sans cesse croissantcroissant dans la procédure législative et proposer en temps utile des conseils faisant autorité, le tout avec des moyens de plus en plus limités. Dans cette perspective, notre inventaire a été élaboré en sélectionnant les questions d'importance stratégique qui formeront la pierre angulaire de notre travail consultatif pour 2014 (l'inventaire et une note d'accompagnement sont publiés sur notre site internet).

- **Nouveau cadre juridique de protection des données**

Nous continuerons d'interagir avec l'ensemble des acteurs concernés dans la procédure législative en cours destinée à l'élaboration d'un nouveau cadre juridique, ainsi qu'avec les parties prenantes et les parties intéressées à tous les niveaux afin de garantir une adoption rapide du paquet législatif.

- **Rétablir la confiance dans les flux internationaux de données à la suite de l'affaire PRISM**

Nous suivrons de près l'évolution de l'affaire PRISM et apporterons notre contribution aux initiatives prises par les institutions de l'Union, et notamment par la Commission, en vue de rétablir la confiance dans les flux internationaux de données.

- **Initiatives visant à soutenir la croissance économique et la stratégie numérique**

La majeure partie des travaux prévus par la Commission dans le domaine de la société de l'information et des nouvelles technologies pour 2014 figuraient déjà dans le programme de travail de 2013. Une attention particulière sera accordée à l'objectif visant à soutenir la croissance économique dans l'Union. Certaines des initiatives envisagées sont

susceptibles de présenter une pertinence particulière pour la protection des données.

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

L'année 2014 marquera la fin du programme pour l'espace de liberté, de sécurité et de justice adopté en 2010 à Stockholm. Une nouvelle série d'orientations stratégiques et une feuille de route pluriannuelle seront adoptées; elles incluront certaines politiques lancées en 2013 qu'il convient de reporter.

- **Réformes du secteur financier**

Depuis le début de la crise économique, la Commission a entrepris une réforme complète du règlement financier et du contrôle exercé à son égard. En 2013, nous avons suivi attentivement les évolutions concernant la législation financière. Hormis la proposition pour une «*nouvelle approche européenne en matière de défaillances et d'insolvabilité des entreprises*», au sujet de laquelle nous pourrions publier une observation ou un avis, la majorité des mesures prévues pour 2014 sont des éléments qui figuraient déjà dans le programme de 2013

- **Lutte contre la fraude fiscale et secteur bancaire**

Dans le prolongement de la tendance observée en 2013, les initiatives de lutte contre l'évasion fiscale et le secret bancaire élaborées au niveau de l'Union devraient avoir des répercussions sur la protection des données. À l'exception du cadre juridique de l'Union en matière de TVA, les politiques fiscales ne relèvent pas des compétences de l'Union. Néanmoins, cette dernière soutient, coordonne ou complète de plus en plus les actions entreprises par les États membres en matière de coopération administrative dans le domaine fiscal, et exerce ainsi la compétence qui lui est conférée par l'article 6 du traité sur le fonctionnement de l'Union européenne.

- **Autres initiatives**

Dans le cadre de notre stratégie visant à promouvoir une culture de protection des données au sein des institutions et organes de l'Union européenne et à intégrer le respect des principes de protection des données dans la législation et les politiques de l'Union, y compris dans des domaines tels que la concurrence, nous pourrions décider d'émettre des recommandations de notre propre initiative afin de contribuer aux débats sur les évolutions juridiques et sociales susceptibles d'avoir des incidences significatives sur la protection des données à caractère personnel. En publiant ces avis *préliminaires*, nous espérons lancer un dialogue éclairé sur ces sujets importants, ce qui pourrait permettre, à un stade ultérieur, de formuler un avis complet et des recommandations.

9.3. Coopération

Nous continuerons à accorder une attention particulière à la réalisation de la stratégie 2013-2014 concernant la coopération avec les autres autorités chargées de la protection des données en matière de supervision coordonnée et dans d'autres domaines importants. Nous continuerons également à suivre les développements pertinents dans les organisations internationales.

- **Supervision conjointe**

Nous continuerons d'assumer notre rôle de soutien dans la supervision coordonnée d'EURODAC, SID et VIS, en étroite collaboration avec les autorités des États membres chargées de la protection des données, et nous renforcerons notre rôle dans le cadre de SIS II. En 2014, les premières mesures de supervision coordonnée devraient également porter sur l'IMI.

- **Groupe de travail «Article 29»**

Nous continuerons de contribuer activement aux activités et au développement du groupe de travail «Article 29», en assurant cohérence et synergie entre le groupe de travail et nos propres activités, conformément à nos priorités respectives. Nous maintiendrons également nos bonnes relations avec les APD nationales. En tant que rapporteur sur certains dossiers particuliers, nous continuerons de diriger et de préparer l'adoption des avis du groupe de travail «Article 29».

- **Organisations internationales**

Les organisations internationales, telles que le Conseil de l'Europe et l'OCDE, jouent un rôle important en matière de normalisation et d'élaboration de politiques dans différents domaines, y compris la protection des données et les sujets qui y sont liés. En même temps, la plupart des organisations internationales ne sont pas soumises à la législation relative à la protection des données dans leur pays d'accueil, et elles ne disposent pas toutes de leurs propres règles appropriées en matière de protection des données. Nous continuerons par conséquent d'établir des contacts avec les organisations internationales, que ce soit pour participer à leurs travaux

de normalisation et d'élaboration de politiques, ou pour les amener à participer à des ateliers de sensibilisation et d'échange de bonnes pratiques.

9.4. Politique IT

Le suivi des évolutions des technologies de l'information qui ont des incidences sur la protection des données et les discussions correspondantes sur la politique en matière de technologies et sur les évolutions commerciales pertinentes nous permettront de prendre davantage en considération les éléments techniques dans le cadre de nos activités de supervision et dans nos observations relatives aux initiatives stratégiques de l'Union. Notre efficacité dans ce domaine bénéficiera d'une coopération étroite avec d'autres autorités chargées de la protection des données et d'experts externes.

Nous continuerons également à mener des actions de sensibilisation, dans les institutions de l'Union, sur la nécessité d'évaluer les risques liés au traitement des données à caractère personnel et sur les méthodologies à appliquer à cet effet. En collaboration avec des experts internes et externes aux institutions, nous veillerons à mettre en évidence la gamme d'outils et d'approches qui sont disponibles pour déterminer les mesures de protection techniques et organisationnelles appropriées pour gérer ces risques.

En collaboration avec les parties prenantes dans l'Union, ainsi que les administrations nationales et les autorités nationales chargées de la protection des données, nous continuerons également de contribuer aux initiatives spécifiques visant à évaluer et garantir la sécurité de certains systèmes IT de l'Union.

- **Lignes directrices à l'intention des institutions de l'Union**

À la suite de nos échanges de 2013 avec des gestionnaires IT, des experts en sécurité, des administrateurs de sites et d'autres acteurs des institutions et organes de l'Union, nous finaliserons nos lignes directrices relatives aux exigences juridiques et aux mesures techniques applicables à la protection des données à caractère personnel traitées sur les sites Internet de l'Union au moyen de dispositifs mobiles et dans des environnements d'informatique en nuage. Ces lignes directrices serviront également de base pour l'élaboration de méthodes et outils de contrôle systématique et régulier dans ces domaines.

- **Développement d'un internet respectueux de la vie privée**

Avec d'autres autorités de protection des données, nous œuvrerons pour améliorer la communication entre les experts de la protection des données et les communautés de développeurs au moyen d'ateliers, de conférences et de groupes de travail spécifiques, de sorte à favoriser une meilleure compréhension des besoins mutuels et à élaborer des moyens concrets d'intégrer les exigences relatives à la protection des données et à la vie privée dans les nouveaux protocoles, outils, composants et services, ainsi que dans les nouvelles applications.

Dans ce contexte, nous chercherons également des moyens de garantir que la formation des nouveaux ingénieurs et développeurs intègre davantage les notions de vie privée et de protection des données. Nous avons également pour objectif de conseiller les agences de recherche sur le soutien qu'elles peuvent apporter aux évolutions technologiques respectueuses de la vie privée.

- **Infrastructure des technologies de l'information**

Pour répondre à nos propres besoins IT, nous continuerons à renforcer l'efficacité de l'infrastructure et nous veillerons à ce qu'elle respecte toutes les exigences relatives à la protection des données et à la sécurité. Nous continuerons à améliorer nos procédures internes et intensifier la coopération avec nos prestataires de service.

Nous veillerons également à ce que les programmes d'apprentissage continu destinés au personnel du CEPD tiennent dûment compte de la dimension IT.

9.5. Autres domaines

Information et communication

Conformément à notre stratégie 2013-2014, nous continuerons non seulement à sensibiliser à la protection des données dans l'administration de l'Union, mais également à informer les particuliers de leurs droits fondamentaux en matière de vie privée et de protection des données. Pour ce faire, nous allons déployer des efforts pour améliorer la visibilité du CEPD en tant qu'expert de la protection des données, y compris dans la presse et dans l'opinion publique, afin d'obtenir tant la confiance du public que l'engagement des institutions de l'Union.

En 2014, nos activités de communication consisteront, entre autres:

- à mettre à jour notre site internet et à créer une section consacrée à nos observations en matière de politique IT;
- à réexaminer et à mettre à jour les outils d'information et de communication existants (publications,

site internet, etc.) en vue du nouveau mandat du CEPD;

- à continuer d'employer un langage simple pour rendre les questions techniques plus accessibles, en incluant des exemples auxquels le grand public peut s'identifier.

Gestion des ressources et professionnalisation de la fonction RH

L'année 2014 devrait marquer le début d'un troisième mandat du CEPD. Dix ans après sa création, le CEPD est une institution bien développée. Nous ne sommes plus confrontés aux défis liés à sa consolidation, mais plutôt à des questions de développement organisationnel, de gestion de la qualité, de planification stratégique et d'allocation des ressources, ainsi que de maintien et de motivation du personnel.

L'entrée en vigueur du nouveau statut des fonctionnaires en janvier 2014 entraînera la mise à jour de nombreuses mesures d'exécution liées à un ensemble de questions relatives aux ressources humaines (évaluation, gestion des congés, conditions de travail, etc.). Il s'agit d'une tâche administrative énorme qui nécessite une planification minutieuse, la consultation du comité du personnel du CEPD et la communication proactive avec tous les collèguescollègues.

Le nouveau mandat du CEPD est également susceptible d'entraîner une lourde charge de travail pour l'unité RHBA, non seulement parce que les nouveaux membres doivent connaître parfaitement les exigences élevées de notre petite institution, mais également parce qu'il convient de gérer et de mettre en œuvre toutes les modifications consécutives.

Nous poursuivrons les activités de ressources humaines commencées en 2013 (élaboration d'une politique d'apprentissage et de développement plus stratégique et révision du code de conduite), tout en entreprenant de nouvelles activités, telles que l'amélioration des procédures de recrutement.

Les actuelles équipes de ressources humaines et d'administration seront fusionnées afin d'améliorer les capacités en ressources humaines de l'organisation.

Comme les années précédentes, le personnel du CEPD continuera à être notre priorité. Nous veillerons à offrir au personnel les meilleures conditions de travail possibles dans les limites du statut des fonctionnaires, afin que le CEPD continue d'être considéré comme un lieu de travail idéal, doté d'un personnel très motivé et impliqué.

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[42].

Depuis l'entrée en vigueur du traité de Lisbonne, le 1er décembre 2009, l'article 16 du TFUE doit être considéré comme le fondement juridique du CEPD. L'article 16 souligne l'importance de la protection des données à caractère personnel d'une manière plus générale. L'article 16 TFUE et l'article 8 de la charte des droits fondamentaux de l'UE prévoient que le respect des règles en matière de protection des données soit soumis à un contrôle exercé par une autorité indépendante. Au niveau de l'UE, cette autorité est le CEPD.

Les autres actes pertinents 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».

[42] JO L 8 du 12.1.2001, p. 1.

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

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

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

Tâches et compétences du CEPD

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

Cette présentation des attributions, fonctions et compétences suit, pour l'essentiel, le même schéma que pour les autorités nationales de contrôle: entendre et examiner les réclamations, effectuer d'autres enquêtes, informer le responsable du traitement et les personnes concernées, effectuer des contrôles préalables lorsque les opérations de traitement présentent des risques particuliers, etc. Le règlement habilite le CEPD à obtenir accès à toutes les informations utiles et aux locaux pertinents lorsque cela est nécessaire pour ses enquêtes. Le CEPD peut aussi imposer des sanctions et saisir la Cour de justice. Ces activités de supervision sont examinées de façon plus approfondie au chapitre 2 du présent rapport.

Certaines tâches revêtent une nature particulière. La tâche consistant à conseiller la Commission et les autres institutions à propos des nouvelles dispositions législatives – confirmée à l'article 28, paragraphe 2, par l'obligation formelle qui est faite à la Commission de consulter le CEPD lorsqu'elle adopte une proposition de législation relative à la protection des données à caractère personnel – concerne aussi les projets de directive et les autres mesures destinées à s'appliquer au niveau national ou à être transposées en droit national. Il s'agit d'une fonction stratégique qui permet au CEPD de se pencher, très tôt, sur les implications possibles au regard de la protection de la vie privée et d'envisager d'autres solutions éventuelles, y compris dans les domaines qui faisaient partie de 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, tandis que les questions technologiques sont spécifiquement abordées dans le chapitre 5.

La coopération avec les autorités nationales de contrôle et avec les organes de contrôle relevant de l'ancien troisième pilier a une incidence similaire plus stratégique. 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, y compris les évolutions dans la supervision coordonnée, 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) coopère avec les autorités nationales de contrôle mentionnées à l'article 28 de la directive 95/46/CE des pays auxquels cette directive s'applique dans la mesure nécessaire à l'accomplissement de leurs devoirs respectifs, notamment en échangeant toutes informations utiles, en demandant à une telle autorité ou à un tel organe d'exercer ses pouvoirs ou en répondant à une demande d'une telle autorité ou d'un tel organe;

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

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

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

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

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

(k) établit son règlement intérieur.

Article 47 — Compétences

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

(a) conseiller les personnes concernées dans l'exercice de leurs droits;

(b) saisir le responsable du traitement en cas de violation alléguée des dispositions régissant le traitement des données à caractère personnel et, le cas échéant, formuler des propositions tendant à remédier à cette violation et à améliorer la protection des personnes concernées;

(c) ordonner que les demandes d'exercice de certains droits à l'égard des données soient satisfaites lorsque de telles demandes ont été rejetées en violation des articles 13 à 19;

(d) adresser un avertissement ou une admonestation au responsable du traitement;

(e) ordonner la rectification, le verrouillage, l'effacement ou la destruction de toutes les données lorsqu'elles ont été traitées en violation des dispositions régissant le traitement de données à caractère personnel et la notification de ces mesures aux tiers auxquels les données ont été divulguées;

(f) interdire temporairement ou définitivement un traitement;

(g) saisir l'institution ou l'organe concerné et, si nécessaire, le Parlement européen, le Conseil et la Commission;

(h) saisir la Cour de justice des Communautés européennes dans les conditions prévues par le traité;

(i) intervenir dans les affaires portées devant la Cour de justice des Communautés européennes.

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

(a) obtenir d'un responsable du traitement ou d'une institution ou d'un organe communautaire l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires à ses enquêtes;

(b) obtenir l'accès à tous les locaux dans lesquels un responsable du traitement ou une institution ou un organe communautaire exerce ses activités s'il existe un motif raisonnable de supposer que s'y exerce une activité visée par le présent règlement.

Annexe C — Liste des abréviations

ACAC	Accord commercial anti-contrefaçon
ACC	Autorité de contrôle commune
AEE	Agence européenne pour l'environnement
AESA	Agence européenne de la sécurité aérienne
APD	Autorité nationale de la protection des données
BCE	Banque centrale européenne
BEI	Banque européenne d'investissement
CC	Cour des comptes
CdR	Comité des régions
CE	Communautés européennes
CEDH	Convention européenne des droits de l'homme
CEPCM	Centre européen de prévention et de contrôle des maladies
CEPD	Contrôleur européen de la protection des données
CGAM	Comité de gestion du régime commun d'assurance maladie
CJUE	Cour de justice de l'Union européenne
CPAS	Comité de préparation pour les affaires sociales
CPD	Coordinateur de la protection des données
CSO	Centre de service et d'opération
DAS	Déclaration d'assurance
DEE	Décision d'enquête européenne
DG INFSO	Direction générale de la société de l'information et des médias
DG MARKT	Direction générale du marché intérieur et des services
DIGIT	Direction générale de l'informatique
DPD	Délégué à la protection des données
DPE	Décision de protection européenne
EEA	École européenne d'administration
EFSA	Autorité européenne de sécurité des aliments
END	Expert national détaché
ENISA	Agence européenne chargée de la sécurité des réseaux et de l'information
EPSO	Office européen de sélection du personnel
ERCEA	Agence exécutive du Conseil européen de la recherche
FRA	Agence des droits fondamentaux de l'Union européenne
GTPJ	Groupe de travail sur la police et la justice
HCR	Haut-commissariat des Nations unies pour les réfugiés
IMI	Système d'information du marché intérieur
JRC	Centre commun de recherche
LIBE	Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen
OCC	Organe de contrôle commun
OCR	Opération conjointe de retour
OHMI	Office de l'harmonisation dans le marché intérieur
OIM	Organisation internationale pour les migrations
OLAF	Office européen de lutte antifraude

OMD	Organisation mondiale des douanes
PNR	Données des dossiers passagers
RFID	Identification par radiofréquence
RH	Ressources humaines
RLS	Responsable local de la sécurité
RLSI	Responsable local de la sécurité informatique
SAI	Service d'audit interne
SAPR	Système d'alerte précoce et de réaction
SID	Système d'information douanier
SIS	Système d'information Schengen
SSI	Stratégie de sécurité intérieure
s-TESTA	Services télématiques transeuropéens sécurisés entre administrations
SWIFT	Société de télécommunications interbancaires mondiales
TFTP	Programme de surveillance du financement du terrorisme
TFTS	Système de surveillance du financement du terrorisme
TFUE	Traité sur le fonctionnement de l'Union européenne
TI	Technologies de l'information
TIC	Technologies de l'information et de la communication
TURBINE	TrUsted Revocable Biometrics IdeNtitiEs
UE	Union européenne
VIS	Système d'information sur les visas
WP 29	Groupe travail de l'article 29 sur la protection des données

Annexe D — Liste des délégués à la protection des données

ORGANISATION	NOM	ADRESSE ÉLECTRONIQUE
Parlement européen (PE)	Secondo SABBIONI	Data-Protection@europarl.europa.eu
Conseil de l'Union européenne (Consilium)	Carmen LOPEZ RUIZ	Data.Protection@consilium.europa.eu
Commission européenne (CE)	Philippe RENAUDIÈRE	Data-Protection-officer@ec.europa.eu
Cour de justice de l'Union européenne (CURIA)	Valerio Agostino PLACCO	Dataprotectionofficer@curia.europa.eu
Cour des comptes européenne (CC)	Johan VAN DAMME	Data-Protection@eca.europa.eu
Comité économique et social européen (CESE)	Lucas CAMARENA JANUZEC	Data.Protection@eesc.europa.eu
Comité des régions (CdR)	Rastislav SPÁC	Data.Protection@cor.europa.eu
Banque européenne d'investissement (BEI)	Alberto SOUTO DE MIRANDA	Dataprotectionofficer@eib.org
Service européen pour l'action extérieure (SEAE)	Carine CLAEYS	Ingrid.HVASS@eeas.europa.eu Carine.CLAEYS@eeas.europa.eu
Médiateur européen	Christina KARAKOSTA (DPD faisant fonction) Rosita AGNEW	DPO-euro-ombudsman@ombudsman.europa.eu
Contrôleur européen de la protection des données (CEPD)	Sylvie PICARD	Sylvie.picard@edps.europa.eu
Banque centrale européenne (BCE)	Frederik MALFRÈRE	DPO@ecb.int
Office européen de lutte antifraude (OLAF)	Laraine LAUDATI	Laraine.Laudati@ec.europa.eu
Centre de traduction des organes de l'Union européenne (CdT)	Martin GARNIER	Data-Protection@cdt.europa.eu
Office de l'harmonisation dans le marché intérieur (OHMI)	Gregor SCHNEIDER	DataProtectionOfficer@oami.europa.eu
Agence des droits fondamentaux de l'Union européenne (FRA)	Nikolaos FIKATAS	Nikolaos.Fikatas@fra.europa.eu
Agence européenne des médicaments (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

>>>

ORGANISATION	NOM	ADRESSE ÉLECTRONIQUE
Fondation européenne pour l'amélioration des conditions de vie et 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
Autorité européenne de sécurité des aliments (EFSA)	Claus RÉUNIS	Dataprotectionofficer@efsa.europa.eu
Agence européenne pour la sécurité maritime (EMSA)	Malgorzata NESTEROWICZ	Malgorzata.Nesterowicz@emsa.europa.eu
Centre européen pour le développement de la formation professionnelle (Cedefop)	Spyros ANTONIOU Jesus BUSTAMANTE	Spyros.Antoniou@cedefop.europa.eu Jesus.Bustamante@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 (EU-OSHA)	Emmanuelle BRUN	brun@osha.europa.eu
Agence européenne de contrôle des pêches (AECP)	Rieke ARNDT	cfca-dpo@cfca.europa.eu
Centre satellitaire de l'Union européenne (CSUE)	Jean-Baptiste TAUPIN	j.taupin@eusc.europa.eu
Institut européen pour l'égalité entre les hommes et les femmes (EIGE)	Ramunas LUNSKUS	Ramunas.Lunskus@eige.europa.eu
Agence du GNSS européen (GSA)	Triinu VOLMER	Triinu.Volmer@gsa.europa.eu
Agence ferroviaire européenne (AFE)	Zografia PYLORIDOU	Dataprotectionofficer@era.europa.eu
Agence exécutive pour les consommateurs, la santé et l'alimentation (CHAFEA)	Beata HARTWIG	Beata.Hartwig@ec.europa.eu
Centre européen de prévention et de 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)	Andrzej GRAS	Andrzej.gras@frontex.europa.eu
Agence européenne de la sécurité aérienne (AESA)	Francesca PAVESI	Francesca.Pavesi@easa.europa.eu
Agence exécutive pour la compétitivité et l'innovation (EACI)	Elena FIERRO SEDANO	Elena.Fierro-Sedano@ec.europa.eu

>>>

ORGANISATION	NOM	ADRESSE ÉLECTRONIQUE
Agence exécutive du réseau transeuropéen de transport (TEN-T EA)	Caroline MAION (DPD faisant fonction)	inea-dpo@ec.europa.eu caroline.maion@ec.europa.eu
Autorité bancaire européenne (ABE)	Joseph MIFSUD	Joseph.MIFSUD@eba.europa.eu
Agence européenne des produits chimiques (ECHA)	Bo BALDUYCK	data-protection-officer@echa.europa.eu
Agence exécutive du Conseil européen de la recherche (ERCEA)	Nadine KOLLOCZEK	Nadine.Kolloczek@ec.europa.eu
Agence exécutive pour la recherche (REA)	Evangelos TSAVALOPOULOS	Evangelos.Tsavalopoulos@ec.europa.eu
Comité européen du risque systémique (CERS)	Frederik MALFRÈRE	DPO@ecb.int
Entreprise commune Fusion for energy – F4E	Angela BARDENEWER-RATING	Angela.Bardenhewer@f4e.europa.eu
Entreprise commune SESAR	Daniella PAVKOVIC	Daniella.Pavkovic@sesarju.eu
Entreprise commune ARTEMIS	Anne SALAÜN	Anne.Salaun@artemis-ju.europa.eu
Entreprise commune Clean Sky	Bruno MASTANTUONO	Bruno.Mastantuono@cleansky.eu
Initiative Médicaments innovants (IMI)	Estefania RIBEIRO	Estefania.Ribeiro@imi.europa.eu
Entreprise commune Piles à combustible et hydrogène	Nicolas BRAHY	Nicolas.Brahy@fch.europa.eu
Autorité européenne des assurances et des pensions professionnelles (AEAPP)	Catherine COUCKE	catherine.coucke@eiopa.europa.eu
Collège européen de police (CEPOL)	Leelo KILG-THORNLEY	leelo.kilg-thornley@cepol.europa.eu
Institut européen d'innovation et de technologie (EIT)	Roberta MAGGIO	roberta.maggio@eit.europa.eu
Agence européenne de défense (AED)	Gabriele BORLA	alain-pierre.louis@eda.europa.eu
Entreprise commune ENIAC	Marc JEUNIAUX	Marc.Jeuniaux@eniac.europa.eu
Organe des régulateurs européens des communications électroniques (ORECE)	Michele Marco CHIODI	Michele-Marco.CHIODI@berec.europa.eu
Agence de coopération des régulateurs de l'énergie (ACER)	Paul MARTINET	Paul.MARTINET@acer.europa.eu
Bureau européen d'appui en matière d'asile (EASO)	Paula McCLURE	paula-mello.mcclure@ext.ec.europa.eu
Institut d'études de sécurité de l'Union européenne (IESUE)	Nikolaos CHATZIMICHALAKIS	nikolaos.chatzimichalakis@iss.europa.eu
eu-LISA	Luca ZAMPAGLIONE	Luca.ZAMPAGLIONE@ext.ec.europa.eu

Annexe E — Liste des avis de contrôle préalable et des avis sur l'absence de contrôle préalable

Gestion des congés et de l'horaire flexible - IMI

Avis du 20 décembre 2013 sur la notification en vue d'un contrôle préalable reçue du délégué à la protection des données de l'Initiative en matière de médicaments innovants concernant la gestion des congés et de l'horaire flexible (Dossier 2013-0463)

Passation de marchés publics - OHMI

Avis du 20 décembre 2013 sur la notification en vue d'un contrôle préalable concernant la passation de marchés publics à l'Office de l'harmonisation dans le marché intérieur (OHMI) (Dossier 2013-0668)

Enquête anonyme ciblant le personnel du Parlement Européen ayant un handicap - PE

Avis du 18 décembre 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données du Parlement Européen à propos du dossier «Enquête anonyme ciblant le personnel du Parlement Européen ayant un handicap» (Dossier 2013-0656)

Demandes et autorisations de congés - Office de l'ORECE

Avis du 18 décembre 2013 sur la notification en vue d'un contrôle préalable reçue du délégué à la protection des données de l'Office de l'ORECE concernant les demandes et autorisations de congés de tout type (y compris les congés spéciaux) (Dossier 2013-0405)

Passation de marchés publics - ECHA

Avis du 18 décembre 2013 sur la notification en vue d'un contrôle préalable concernant la passation de marchés publics (Dossier 2013-0010)

Évaluation du personnel - EIT

Avis du 16 décembre 2013 sur la notification d'un contrôle préalable concernant les rapports de stage du personnel de l'EIT (Dossier 2013-0813)

Procédure d'attestation - OHMI

Avis du 16 décembre 2013 sur la notification en vue d'un contrôle préalable concernant la procédure d'attestation de l'OHMI (anciennes catégories C et D) (Dossier 2013-0797)

Capacité à travailler dans une troisième langue - Cour de justice

Avis du 10 décembre 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Cour de justice de l'Union européenne à propos de la «capacité à travailler dans une troisième langue» (Dossier 2013-0771)

Évaluation du personnel et rapports de stage - SESAR

Avis du 2 décembre 2013 sur les notifications en vue d'un contrôle préalable reçues du délégué à la protection des données de l'entreprise commune SESAR concernant les procédures d'évaluation du personnel de l'entreprise commune et sa procédure relative aux rapports de stage (Dossiers 2013-0699 et 2013-0700)

Gestion des congés - AED

Avis du 21 novembre 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de l'Agence européenne de défense pour ce qui concerne la gestion des congés (Dossier 2013-0741)

Sélection, recrutement et gestion du personnel et des stagiaires – TEN-T EA

Avis du 21 novembre 2013 sur la notification en vue d'un contrôle préalable concernant la mobilité interne (Dossier 2013-0871), ainsi que la sélection, le recrutement et la gestion du personnel intérimaire (2013-0871), des stagiaires «livre bleu» (2013-0872) et des stagiaires atypiques (2013-0873) de l'Agence exécutive du réseau transeuropéen de transport.

Prévention du harcèlement et la sélection de conseillers confidentiels - F4E

Avis du 21 novembre 2013 sur la notification d'un contrôle préalable concernant les procédures de prévention du harcèlement et la sélection de conseillers confidentiels au sein de F4E (Dossier 2013-0326)

Subventions pour cours d'interprétation dans les centres universitaires - PE

Avis du 21 novembre 2013 sur la notification en vue d'un contrôle préalable relative au traitement des données à caractère personnel dans le cadre de la procédure pour l'octroi de «subventions pour cours d'interprétation dans les centres universitaires» (Dossier 2013-0653)

Passation de marchés publics - FRA

Avis du 19 novembre 2013 sur la notification en vue d'un contrôle préalable concernant la passation de marchés publics à l'Agence des droits fondamentaux (Dossier 2013-0660)

Gestion des congés et du temps de travail - ECHA

Avis du 14 novembre 2013 sur la notification en vue d'un contrôle préalable reçue du délégué à la protection des données de l'Agence européenne des produits chimiques au sujet de la gestion des congés et du temps de travail (Dossier 2013-0345)

Gestion des présences et des absences - ECDC

Avis du 14 novembre 2013 sur une notification en vue d'un contrôle préalable reçu du délégué à la protection des données du Centre européen de prévention et de contrôle des maladies concernant la gestion des présences et des absences (Dossier 2013-0362)

Sélection du président du conseil de surveillance - Parlement

Avis du 14 novembre 2013 sur une notification de contrôle préalable concernant la sélection du président du conseil de surveillance (Dossier 2013-1090)

Procédure de sélection et de recrutement - AED

Avis du 5 novembre 2013 sur une notification en vue d'un contrôle préalable concernant la procédure de sélection et de recrutement d'agents temporaires (AT), d'agents contractuels (AC), d'experts nationaux détachés (END) et de stagiaires de l'Agence européenne de défense (AED) (Dossier 2013-0743)

Procédures d'évaluation du personnel - AEE

Avis du 5 novembre 2013 sur une notification en vue d'un contrôle préalable reçue du délégué à la protection des données de l'Agence européenne pour l'environnement (AEE) concernant les procédures d'évaluation du personnel de l'AEE (Dossier 2013-0791)

Passation de marchés publics et octroi de subventions - EFSA

Avis du 31 octobre 2013 sur la notification en vue d'un contrôle préalable concernant la passation de marchés publics et l'octroi de subventions l'Autorité européenne de sécurité des aliments (Dossier 2012-0666)

Passation de marchés publics - AESA

Avis du 31 octobre 2013 sur la notification en vue d'un contrôle préalable concernant la passation de marchés publics et la gestion des contrats y afférents à l'Agence européenne de la sécurité aérienne (EASA) (Dossier 2012-0647)

Gestion des congés - Cour de Justice

Avis du 29 octobre 2013 sur les notifications de contrôle préalable reçues du délégué à la protection des données (DPD) de la Cour de justice de l'Union européenne à propos des dossiers relatifs à la gestion des congés spéciaux et des congés de maternité (Dossier 2013-0189), à la gestion de l'aménagement du temps de travail (temps partiel) (2013-0223), à la gestion des congés parentaux et des congés familiaux (2013-0267) et à la gestion des congés de convenance personnelle du personnel de la Cour (2013-0337)

Gestion des congés - CEPOL

Avis du 29 octobre 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données du Collège européen de police concernant la gestion des congés maladie, des congés annuels et des congés spéciaux et la gestion des heures de travail et de l'horaire flexible (Dossier 2013-0315)

Procédure de transmission d'informations - TEN-T EA

Avis du 28 octobre 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de l'Agence exécutive du réseau transeuropéen de transport (AE RTE-T) concernant une procédure de transmission d'informations en cas de dysfonctionnements graves (Dossier 2013-0916)

Passation de marchés publics - ERCEA

Avis du 21 octobre 2013 sur la notification en vue d'un contrôle préalable concernant la passation de marchés publics à l'Agence exécutive du Conseil européen de la recherche (Dossier 2012-0921)

Procédure de recrutement - AECP

Avis du 21 octobre 2013 sur la notification d'un contrôle préalable au sujet du traitement de données à caractère personnel dans le contexte de la procédure de recrutement d'agents temporaires, d'agents contractuels et d'experts nationaux détachés (Dossier 2013-0735) et de contrats de service de stagiaires conformément à l'accord de coopération éducative avec l'université de Vigo (Dossier 2013-0736) à l'Agence européenne de contrôle des pêches

Procédures de passation de marchés publics et d'octroi de subventions - ECDC

Avis du 17 octobre sur la notification de contrôle préalable concernant les procédures de passation de marchés publics et d'octroi de subventions à l'ECDC (Dossier 2012-1089)

Procédure d'évaluation du personnel - AED

Avis du 16 octobre 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de l'Agence européenne de défense (AED) concernant la «procédure d'évaluation du personnel» (Dossier 2013-0744)

Traitement de données à caractère personnel dans le contexte de stages - FRA

Avis du 16 octobre 2013 sur la notification d'un contrôle préalable concernant le traitement de données à caractère personnel dans le contexte de stages à l'Agence des droits fondamentaux de l'Union européenne (Dossier 2013-0654)

Rapports de stage pour les agents temporaires et contractuels - AEE

Avis du 14 octobre 2013 sur la notification en vue d'un contrôle préalable reçue du délégué à la protection des données de l'Agence européenne pour l'environnement (AEE) concernant les rapports de stage de l'AEE pour les agents temporaires et contractuels (Dossier 2013-0787)

Rapports de stage - AED

Avis du 14 octobre 2013 sur la notification de contrôle préalable concernant les rapports de stage de l'AED (Dossier 2013-0742)

Gestion des congés - Artemis

Avis du 14 octobre 2013 sur la notification d'un contrôle préalable reçue de la déléguée à la protection des données de l'entreprise commune Artemis concernant la gestion des congés (Dossier 2013-0346)

Attestation et certification - F4E

Avis du 14 octobre 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de l'entreprise commune européenne pour ITER et le développement de l'énergie de fusion concernant l'attestation et la certification (Dossier 2013-708)

Gestion des congés - EMSA

Avis du 8 octobre 2013 sur la notification d'un contrôle préalable reçue de la déléguée à la protection des données de l'Agence européenne pour la sécurité maritime concernant la gestion des congés (Dossier 2013-0474)

Gestion des congés - FEI

Avis du 2 octobre 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données du Fonds européen d'investissement («FEI») (Dossier 2013-0349)

Travail à temps partiel – Médiateur européen

Avis du 2 octobre 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données du Médiateur européen concernant des demandes de travail à temps partiel (Dossier 2013-0507)

Demandes de congés – F4E

Avis du 2 octobre 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de l'entreprise commune pour ITER et le développement de l'énergie de fusion concernant les demandes de congés (Dossier 2013-0323)

Enquêtes administratives et procédures disciplinaires - ENISA

Avis du 1er octobre 2013 sur la notification en vue d'un contrôle préalable concernant le traitement de données à caractère personnel réalisé dans le cadre des enquêtes administratives et des procédures disciplinaires au sein de l'ENISA (Dossier 2013-0715)

Évaluation du personnel stagiaire - Médiateur européen

Avis du 1er octobre 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données du Médiateur européen à propos de l'évaluation du personnel stagiaire (Dossier 2013-0533)

Sélection du président du conseil de surveillance - BCE

Avis du 20 septembre 2013 concernant une notification en vue d'un contrôle préalable concernant la sélection du président du conseil de surveillance de la BCE (Dossier 2013-1007)

Procédure de recrutement des agents intérimaires - PE

Avis du 10 septembre 2013 sur la notification de contrôle préalable concernant le traitement de données personnelles lors de la procédure de recrutement des agents intérimaires par le PE (Dossier 2013-0799)

Système de gestion des ressources humaines Allegro - EU-OSHA

Avis du 9 septembre 2013 concernant le système Allegro à l'Agence européenne pour la santé et la sécurité au travail, y compris Flexitime (Dossiers 2011-1102 et 2013-0236)

Procédure en cas de sous-performance - BCE

Avis du 30 août 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Banque centrale européenne concernant la procédure de la BCE en cas de sous-performance (Dossier 2013-0892)

Gestion des congés - AECP

Avis du 29 août 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de l'Agence européenne de contrôle des pêches concernant la gestion des congés, des absences pour maladie et des autres absences (Dossier 2013-0456)

Gestion du temps de récupération - DG Interprétation

Avis du 18 juillet 2013 sur une notification en vue d'un contrôle préalable reçue de la part du délégué à la protection des données de la Commission européenne concernant la gestion du temps de récupération des interprètes de la DG Interprétation via l'application «INDISPONIBILITÉ»

Investigative Data Consultation Platform - OLAF

Avis du 18 juillet 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de l'Office de lutte antifraude (OLAF) concernant la «Investigative Data Consultation Platform» (Dossier 2012-0280)

Recrutement de conseillers confidentiels - ECHA

Avis du 17 juillet 2013 sur la notification de contrôle préalable concernant le «recrutement de conseillers confidentiels» à l'Agence européenne des produits chimiques (ECHA) (Dossier 2013-0572)

Examens médicaux de contrôle - F4E

Avis du 16 juillet 2013 sur une notification de contrôle préalable concernant les traitements relatifs aux examens médicaux de contrôle lors d'une absence pour maladie ou accident réalisées par l'agence Fusion for Energy (F4E) (Dossier 2012-0864)

Procédure d'invalidité devant la commission d'invalidité - F4E

Avis du 16 juillet 2013 sur une notification de contrôle préalable reçue du délégué à la protection des données de l'agence F4E concernant la «procédure d'invalidité devant la commission d'invalidité» (Dossier 2012-0863)

Plans de déploiement communs dans les eaux européennes - AECP

Avis du 16 juillet 2013 sur une notification de contrôle préalable reçue du délégué à la protection des données de l'Agence européenne de contrôle des pêches concernant le «traitement des rapports d'inspection relatifs aux plans de déploiement communs dans les eaux européennes» (Dossier 2013-0539)

Système de vidéosurveillance - EFSA

Avis du 16 Juillet 2013 relatif à la notification d'un contrôle préalable sur le système de vidéosurveillance de l'Autorité européenne de sécurité des aliments (EFSA) (Dossier 2013-0429)

Gestion des congés et des absences - ETF

Avis du 4 juillet 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Fondation européenne pour la formation concernant la gestion des congés et des absences (Dossier 2013-0234)

Gestion des congés - FRA

Avis du 4 juillet 2013 sur une notification en vue d'un contrôle préalable reçue du délégué à la protection des données de l'Agence des droits fondamentaux de l'Union européenne concernant le traitement de données à caractère personnel dans le cadre de la gestion des congés (Dossier 2013-0352)

Gestion des congés - Cedefop

Avis du 3 juillet 2013 sur la notification en vue d'un contrôle préalable transmise par le délégué à la protection des données du Centre européen pour le développement de la formation professionnelle concernant la gestion des congés (Dossier 2012-0265)

Gestion des congés et des absences - ERCEA

Avis du 21 juin 2013 sur la notification en vue d'un contrôle préalable transmise par le délégué à la protection des données du Conseil européen de la recherche concernant la gestion des congés et des absences (Dossier 2013-0327)

Congé et horaire flexible - EACEA

Avis du 21 juin 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de l'Agence exécutive «Éducation, audiovisuel et culture» concernant le traitement de données à caractère personnel en matière de congé et d'horaire flexible (Dossier 2013-0336)

Gestion des congés - AESA

Avis du 20 juin 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de l'Agence européenne de la sécurité aérienne concernant la gestion des congés (Dossier 2011-1096)

Enregistrement des conversations téléphoniques dans les salles de sécurité et au standard téléphonique - BEI

Avis du 20 juin 2013 relatif à la notification en vue d'un contrôle préalable reçue du délégué à la protection des données de la Banque européenne d'investissement concernant l'enregistrement des conversations téléphoniques dans les salles de sécurité et au standard téléphonique (Dossier 2013-0297)

Gestion des congés – EACI

Avis du 20 juin 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de l'Agence exécutive pour la compétitivité et l'innovation concernant la gestion des congés (Dossier 2013-0335)

Contrôle de fiabilité de sécurité - JRC

Avis du 19 juin 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Commission sur le contrôle de fiabilité de sécurité au Centre commun de recherche d'Ispra (Dossier 2012-1090)

Recrutement de personnel - CE

Avis du 19 décembre 2013 sur la notification en vue d'un contrôle préalable concernant les procédures de sélection pour le recrutement de personnel de la DG HOME destiné à l'agence européenne eu-LISA (Dossier 2013-0156)

Gestion des absences et du travail - Comité des régions

Avis du 18 juin 2013 sur la notification de contrôle préalable du délégué à la protection des données du Comité des Régions en ce qui concerne la gestion des absences et dispenses de services et des prestations de travail (Dossier 2013-0342)

PERSEO - Médiateur européen

Avis du 12 juin 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données du Médiateur européen concernant PERSEO (Dossier 2013-0235)

Système de gestion des contrats - BEI

Avis du 7 juin 2013 sur une notification d'un contrôle préalable reçue du délégué à la protection des données de la Banque européenne d'investissement concernant le PJ-CMS – système de gestion des contrats de la Direction des projets (PJ) avec registre de consultants intégré (Dossier 2013-0034)

Formules de travail, congés et gestion des présences - REA

Avis du 4 juin 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de l'Agence exécutive pour la recherche concernant les formules de travail, les congés et la gestion des présences (Dossier 2012-0952)

Gestion des congés - AEE

Avis du 4 juin 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de l'Agence européenne pour l'environnement concernant la gestion des congés (Dossier 2011-0851)

Gestion des conflits d'intérêts potentiels entre les membres du comité exécutif - F4E

Avis du 30 mai 2013 sur une notification en vue d'un contrôle préalable reçue du délégué à la protection des données de Fusion for Energy, l'entreprise commune européenne pour ITER et le développement de l'énergie de fusion, au sujet des modalités pratiques de la gestion des conflits d'intérêts potentiels entre les membres du comité exécutif de Fusion for Energy (Dossier 2013-0269)

Gestion des congés de maladie et des congés familiaux – entreprise commune PCH (FCH JU)

Avis du 27 mai 2013 sur la notification en vue d'un contrôle préalable reçue du délégué à la protection des données de l'Entreprise commune Piles à combustible et Hydrogène (FCH JU) concernant la gestion des congés de maladie et des congés familiaux (Dossier 2011-0836)

Évaluation annuelle - SEAE

Avis du 23 mai 2013 sur la notification en vue d'un contrôle préalable reçue du délégué à la protection des données du Service européen pour l'action extérieure concernant l'évaluation annuelle (Dossier 2013-0206)

Gestion des congés - EU-OSHA

Avis du 14 mai 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de l'Agence européenne pour la sécurité et la santé au travail concernant la gestion des congés (Dossier 2013-0281)

Congé spécial - Eurofound

Avis du 8 mai 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Fondation européenne pour l'amélioration des conditions de vie et de travail au sujet du congé spécial (Dossier 2013-0272)

Procédures de congé - EASO

Avis du 29 avril 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données du Bureau européen d'appui en matière d'asile au sujet des procédures de congé (Dossier 2013-0248)

Traitements relatifs à l'utilisation d'un badge - EFSA

Avis du 9 avril 2013 sur la notification de contrôle préalable concernant les traitements relatifs à l'utilisation d'un badge comme outil informant le personnel de sa présence au bureau dans le cadre de l'enregistrement du temps (Dossier 2013-0171)

Harcèlement - AFE

Avis du 9 avril 2013 sur la notification de contrôle préalable concernant les traitements relatifs à la procédure informelle pour les cas de harcèlement psychologique et sexuel, et la sélection de conseillers confidentiels pour la procédure informelle dans les cas de harcèlement à l'Agence ferroviaire européenne (AFE) (Dossiers 2012-0902/3)

Candidatures spontanées - ERCEA

Avis du 9 février 2013 sur la notification en vue d'un contrôle préalable concernant les «candidatures spontanées» à l'Agence exécutive du Conseil européen de la recherche (Dossier 2013-0181)

Procédure d'attestation - Médiateur Européen

Avis du 9 avril 2013 sur la notification d'un contrôle préalable du CEPD concernant la procédure d'attestation au Médiateur Européen (Dossier 2013-0217)

Suivi de la production individuelle - Conseil

Avis du 25 Mars 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données du Conseil de l'Union européenne concernant le traitement de données à caractère personnel dans le cadre du «suivi de la production individuelle» (Dossier 2013-0017)

Enquêtes de sécurité - Centre commun de recherche de Petten

Avis du 19 mars 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Commission sur les enquêtes de sécurité au Centre commun de recherche de Petten (Dossier 2012-0782)

Questionnaire de perception de soi - «PERFORMANSE»

Avis du 15 mars 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Commission européenne concernant un questionnaire de perception de soi intitulé «PERFORMANSE» organisé par l'École européenne d'administration (Dossier 2012-0590)

Analyse et transfert d'informations liées à une fraude à l'OLAF

Avis du 14 mars 2013 sur une notification de contrôle préalable reçue du délégué à la protection des données de l'EACI concernant «l'analyse et le transfert d'informations liées à une fraude à l'OLAF» (Dossier 2012-0652)

Sélection et recrutement d'experts nationaux détachés - ERCEA

Avis du 28 février 2013 sur une notification en vue d'un contrôle préalable concernant le traitement de données à caractère personnel dans le cadre de la sélection et du recrutement d'experts nationaux détachés (END), de stagiaires et d'agents intéri-

maires à l'Agence exécutive du Conseil européen de la recherche (Dossier 2012-0997)

Enquêtes administratives et procédures disciplinaires - ECDC

Avis du 27 février 2013 sur la notification d'un contrôle préalable concernant le traitement des enquêtes administratives et des procédures disciplinaires menées au Centre européen de prévention et de contrôle des maladies (ECDC) (Dossier 2012-1088)

Centre de développement externe - Conseil de l'Union européenne

Avis du 25 février 2013 sur la notification d'un contrôle préalable reçue du Délégué à la protection des données du Conseil de l'Union Européenne concernant la participation des agents du Secrétariat Général à un centre de développement externe (Dossier 2012-0773)

Traitement des données LBC-FT - BEI

Avis du 7 février 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Banque européenne d'investissement au sujet du traitement des données LBC-FT (Dossier 2012-0326)

Enquêtes en matière de sécurité - SEAE

Avis du 1er février 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données du service européen pour l'action extérieure sur les enquêtes en matière de sécurité (Dossier 2011-1059)

Système de gestion de la qualité et contrôles de qualité ex post - OHMI

Avis du 29 janvier 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de l'Office de l'harmonisation dans le marché intérieur («OHMI») au sujet du système de gestion de la qualité et des contrôles de qualité ex post de l'OHMI (Dossier 2012-0999)

Procédures d'évaluation du personnel - ECDC

Avis conjoint du 11 janvier 2013 sur les notifications de contrôle préalable reçues du délégué à la protection des données du Centre européen de prévention et de contrôle des maladies concernant des procédures d'évaluation du personnel (Dossiers 2012-881, 2012-883 et 2012-884)

Liste de cas non soumis à un contrôle préalable

Nomination du président et du vice-président du mécanisme de surveillance unique - Conseil de l'UE

Lettre du 20 décembre 2013 sur la notification d'un contrôle préalable concernant la nomination du président et du vice-président du conseil de surveillance (mécanisme de surveillance unique) (Dossier 2013-1238)

L'instauration de droits individuels - AESA

Lettre du 20 décembre 2013 sur la notification en vue d'un contrôle préalable concernant l'instauration de droits individuels pour les membres du personnel de l'Agence européenne de la sécurité aérienne (EASA) (Dossier 2013-1222)

Procédure de sélection du CEPD - Conseil de l'UE

Réponse du 20 décembre 2013 relative aux traitements concernant la procédure de sélection du contrôleur européen de la protection des données et du contrôleur adjoint (Dossier 2013-1243)

Gestion de Sysper 2 - TEN-T EA

Lettre du 19 décembre 2013 sur la notification en vue d'un contrôle préalable concernant la gestion de Sysper 2 par l'Agence exécutive du réseau transeuropéen de transport (TEN-T EA) (Dossier 2013-1287)

Procédure de sélection du CEPD - Commission

Lettre du 16 décembre 2013 concernant la mise à jour d'une notification concernant la sélection de candidats pour le poste de contrôleur européen de la protection des données (CEPD) et le poste de Contrôleur adjoint (Dossier 2013-1334)

Agents locaux - BEI

Avis du 5 novembre 2013 sur la notification en vue d'un contrôle préalable concernant les agents locaux de la BEI (Dossier 2013-0606)

Traitement de données à caractère personnel concernant le paiement des factures de téléphone portable du personnel de l'ENISA

Lettre du 31 octobre 2013 sur la notification d'un contrôle préalable concernant un traitement de données à caractère personnel concernant le paiement des factures de téléphone portable du personnel de l'ENISA (Dossier 2013-1156)

Audits ex post – EACI

Lettre du 9 octobre 2013 concernant la notification de contrôle préalable de l'EACI concernant des audits ex post (Dossier 2013-0826)

Contrôle d'accès aux locaux - AED

Lettre du 1er octobre 2013 sur la notification de contrôle préalable concernant le contrôle de l'accès aux locaux de l'Agence européenne de défense (Dossier 2013-0765)

Établissement de droits au moment de la nomination/ du départ du personnel - F4E

Lettre du 10 septembre 2013 concernant la notification de contrôle préalable concernant l'établissement de droits au moment du départ du personnel (Dossier 2013-0728) et l'établissement de droits au moment du recrutement/de la nomination du personnel de Fusion for Energy (Dossier 2013-0729)

Réclamations et demandes - F4E

Lettre du 10 septembre 2013 concernant la notification en vue d'un contrôle préalable a posteriori concernant les «réclamations et demandes» de F4E (Dossier 2013-0709)

Gestion de l'habilitation de sécurité - AED

Lettre du 10 septembre 2013 concernant la notification en vue d'un contrôle préalable concernant la gestion des habilitations de sécurité d'établissement (HSE) et des habilitations de sécurité du personnel (HSP) à l'Agence européenne de défense (Dossiers 2013-0763 et 2013-0764)

Transfert de droits à pension - F4E

Lettre du 5 septembre 2013 concernant la notification en vue d'un contrôle préalable concernant des «demandes de transfert de droits à pension» à Fusion for Energy (Dossier 2013-0706)

Gestion des dossiers personnels - AEE

Lettre du 2 septembre 2013 concernant la notification de contrôle préalable concernant la gestion des dossiers personnels au sein de l'Agence européenne pour l'environnement (Dossier 2013-0793)

Aptitudes du personnel - ERCEA

Lettre du 7 mai 2013 concernant la notification de contrôle préalable concernant les traitements relatifs à la liste du département B de l'ERCEA sur les aptitudes du personnel (Dossier 2013-0166)

Utilisation d'un badge - EFSA

Lettre du 9 avril sur la notification de contrôle préalable concernant les traitements relatifs à l'utilisation d'un badge comme outil informant le personnel de sa présence au bureau dans le cadre de l'enregistrement du temps (Dossier 2013-0171)

Transfert de données au conseil scientifique - ERCEA

Lettre du 8 avril 2013 sur la notification en vue d'un contrôle préalable concernant le «transfert de données au conseil scientifique» par l'ERCEA (Dossier 2012-0831)

Autorisation d'exercer une activité extérieure - AESA

Lettre du 28 février 2013 sur la notification en vue d'un contrôle préalable des traitements concernant l'«autorisation d'exercer une activité extérieure ou de remplir un mandat en dehors de l'Union accordée par l'AESA» (dossier 2012-1039)

Annexe F — Liste des avis et des observations formelles sur des propositions législatives

Avis sur des propositions législatives

Services de paiement

Avis du 5 décembre 2013 sur une proposition de directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2006/48/CE et 2009/110/CE et abrogeant la directive 2007/64/CE, ainsi qu'une proposition de règlement du Parlement européen et du Conseil relatif aux commissions d'interchange pour les opérations de paiement liées à une carte

Marché unique européen des communications électroniques

Avis du 14 novembre 2013 concernant la proposition de règlement du Parlement européen et du Conseil établissant des mesures relatives au marché unique européen des communications électroniques et visant à faire de l'Europe un continent connecté, et modifiant les directives 2002/20/CE, 2002/21/CE et 2002/22/CE ainsi que les règlements (CE) n° 1211/2009 et (UE) n° 531/2012

Facturation électronique dans le cadre des marchés publics

Avis du 11 novembre 2013 sur la proposition de directive du Parlement européen et du Conseil relative à la facturation électronique dans le cadre des marchés publics adoptée par la Commission

Déploiement du système eCall

Avis du 29 octobre 2013 sur la proposition de règlement du Parlement européen et du Conseil concernant les exigences en matière de réception par type pour le déploiement du système eCall embarqué et modifiant la directive 2007/46/CE

Données des dossiers passagers - Accord entre le Canada et l'Union européenne

Avis du 30 septembre 2013 sur les propositions de décisions du Conseil relatives à la conclusion et à la signature de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers

Système d'entrée/sortie et programme d'enregistrement des voyageurs

Avis du 18 juillet 2013 sur les propositions de règlement portant création d'un système d'entrée/sortie (EES) et de règlement portant création d'un programme d'enregistrement des voyageurs (RTP)

Marque communautaire

Avis du 11 juillet 2013 sur la proposition de directive du Parlement européen et du Conseil rapprochant les législations des États membres sur les marques (refonte) et sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (CE) n° 207/2009 sur la marque communautaire

Prévention du blanchiment de capitaux et du financement du terrorisme

Avis du 4 juillet 2013 sur une proposition de directive du Parlement européen et du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, et une proposition de règlement du Parlement européen et du Conseil sur les informations accompagnant les virements de fonds

Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé

Avis du 14 juin 2013 sur la communication conjointe de la Commission et de la haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité intitulée «Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé» et sur la proposition de directive de la Commission concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

Agence de l'Union européenne pour la coopération et la formation des services répressifs (Europol)

Avis du 31 mai 2013 sur la proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la coopération et la formation des services répressifs (Europol) et abrogeant les décisions 2009/371/JAI et 2005/681/JAI

Transparence des mesures régissant la fixation des prix des médicaments

Avis du 30 mai 2013 sur la proposition modifiée de directive de la Commission relative à la transparence des mesures régissant la fixation des prix des médicaments à usage humain et leur inclusion dans le champ d'application des systèmes publics d'assurance-maladie

Surveillance du marché

Avis du 30 mai 2013 sur la proposition de la Commission de règlement du Parlement européen et du Conseil concernant la surveillance du marché des produits et modifiant différents instruments législatifs du Parlement européen et du Conseil

Modèle européen en matière d'échange d'informations (EIXM)

Avis du 29 avril 2013 sur la communication de la Commission au Parlement européen et au Conseil intitulée «Renforcer la coopération dans le domaine de la répression au sein de l'UE: le modèle européen en matière d'échange d'informations (EIXM)»

Précurseurs de drogues

Avis du 23 avril 2013 sur la proposition de décision du Conseil relative à la conclusion de l'accord entre l'Union européenne et la Fédération de Russie concernant les précurseurs de drogues

Aviation civile

Avis du 10 avril 2013 sur la proposition de règlement de la Commission concernant les comptes rendus d'évènements dans l'aviation civile et abrogeant la directive 2003/42/CE, le règlement (CE) n° 1321/2007 de la Commission, le règlement (CE) n° 1330/2007 de la Commission et l'article 19 du règlement (UE) n° 996/2010

Une stratégie numérique pour l'Europe

Avis du 10 avril 2013 sur la communication «Une stratégie numérique pour l'Europe: faire du numérique un moteur de la croissance européenne» de la Commission

Procédures d'insolvabilité

Avis du 27 mars 2013 du Contrôleur européen de la protection des données sur la proposition de règlement de la Commission modifiant le règlement (CE) n° 1346/2000 du Conseil relatif aux procédures d'insolvabilité

Plan d'action pour la santé en ligne 2012-2020

Avis du 26 mars 2013 sur la communication de la Commission relative au «Plan d'action pour la santé en ligne 2012-2020 — des soins de santé innovants pour le XXIe siècle»

Dispositifs médicaux de diagnostic in vitro

Avis du 8 février 2013 sur les propositions de la Commission concernant un règlement relatif aux dispositifs médicaux, et modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009, et un règlement relatif aux dispositifs médicaux de diagnostic in vitro

Précurseurs de drogues

Avis du 18 janvier 2013 sur la proposition de règlement modifiant le règlement (CE) n° 273/2004 relatif aux précurseurs de drogues et sur la proposition de règlement modifiant le règlement (CE) n° 111/2005 du Conseil fixant des règles pour la surveillance du commerce des précurseurs des drogues entre la Communauté et les pays tiers

Observations formelles sur des propositions législatives

Règlement général sur la protection des données

Observations du CEPD du 9 décembre 2013 sur l'application du règlement général sur la protection des données (RGPD) proposé aux institutions et organes de l'Union européenne

Lignes directrices pour la réutilisation des informations du secteur public

Observations du CEPD du 22 novembre 2013 en réponse à la consultation publique, lancée par la Commission européenne, sur les orientations prévues sur les licences-types recommandées, les ensembles de données et la tarification pour la réutilisation des informations du secteur public

Contrôle sur Europol

Lettre du 13 novembre 2013 à la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen concernant le contrôle de la protection des données chez Europol

Coopération administrative dans le domaine fiscal

Observations du CEPD du 5 novembre 2013 sur la proposition de directive du Conseil modifiant la directive 2011/16/UE relative à la coopération administrative dans le domaine fiscal

Se préparer à un monde audiovisuel totalement convergent: croissance, création et valeurs

Observations du CEPD du 30 août 2013 sur le livre vert de la Commission: «Se préparer à un monde audiovisuel totalement convergent: croissance, création et valeurs».

Vente de contrefaçons sur l'internet

Observations du CEPD du 11 juillet 2013 sur le rapport de la Commission au Parlement européen et au Conseil concernant le fonctionnement du protocole d'accord sur la vente de contrefaçons sur l'internet

Comptes de paiement

Observations du CEPD du 27 juin 2013 sur la consultation sur une proposition de directive du Parlement européen et du Conseil sur la comparabilité des frais liés aux comptes de paiement, le changement de compte de paiement et l'accès à un compte de paiement assorti de prestations de base

Systèmes de transport intelligents

Observations du CEPD du 13 juin 2013 sur les règlements délégués de la Commission complétant la

directive 2010/40/UE du Parlement européen et du Conseil en ce qui concerne «les données et procédures pour la fourniture, dans la mesure du possible, d'informations minimales universelles sur la circulation liées à la sécurité routière gratuites pour les usagers» et «la mise à disposition de services d'informations concernant les aires de stationnement sûres et sécurisées pour les camions et les véhicules commerciaux»

Droit européen des sociétés et gouvernance d'entreprise

Observations du CEPD du 27 mars 2013 sur le Plan d'Action: droit européen des sociétés et gouvernance d'entreprise - un cadre juridique moderne pour une plus grande implication des actionnaires et une meilleure viabilité des entreprises

Paquet de mesures pour une réforme de la protection des données

Observations complémentaires du CEPD du 15 mars 2013 sur le paquet de mesures pour une réforme de la protection des données

Harmonisation des législations des États membres

Observations du CEPD du 27 février 2013 sur une proposition de directive «relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements hertziens» visant à remplacer la directive 1999/5/CE dite «R&TTE»

Annexe G — Discours du contrôleur et du contrôleur adjoint en 2013

En 2013, le contrôleur et le contrôleur adjoint ont continué de consacrer beaucoup de temps et d'efforts à l'explication de leur mission et à la sensibilisation à la protection des données en général. Ils ont également abordé un certain nombre de questions particulières dans des discours prononcés lors de différentes manifestations organisées dans les institutions de l'Union européenne, dans les États membres et au-delà.

Parlement européen

10 janvier	Contrôleur adjoint, commission LIBE, réforme de la protection des données (Bruxelles) (*)
28 janvier	Contrôleur et contrôleur adjoint, conférence sur la journée de la protection des données (Bruxelles)
19 février	Contrôleur, conférence STOA sur l'e-gouvernement (Bruxelles) (*)
19 mars	Contrôleur, rapporteurs de la commission LIBE, réforme de la protection des données (Bruxelles)
20 mars	Contrôleur, commission LIBE, réforme de la protection des données (Bruxelles)
29 mai	Contrôleur et contrôleur adjoint, commission LIBE, rapport annuel 2012 (Bruxelles)
19 juin	Contrôleur, plate-forme de la vie privée, définition des données à caractère personnel (Bruxelles)
20 juin	Contrôleur, commission interparlementaire, programme de Stockholm (Bruxelles) (*)
7 octobre	Contrôleur, commission LIBE, enquête sur la surveillance électronique de masse (Strasbourg) (*)
28 novembre	Contrôleur, commission IMCO, règlement e-Call (Bruxelles)
5 décembre	Contrôleur, conférence du groupe des Verts, lutte contre le blanchiment d'argent (Bruxelles)

Conseil

22 janvier	Contrôleur, représentation permanente de la Pologne, journée de la protection des données (Bruxelles)
25 avril	Contrôleur adjoint, groupe de travail sur les procédures d'insolvabilité (Bruxelles)
5 septembre	Contrôleur, groupe de travail sur le règlement proposé sur Europol (Bruxelles)
17 septembre	Contrôleur, conférence de la Présidence sur le procureur européen (Vilnius)

Commission européenne

19 mars	Contrôleur adjoint, réunion du groupe des directeurs Ressources (Bruxelles)
14 juin	Contrôleur, conférence de midi de l'École européenne d'administration (Bruxelles)
15 octobre	Contrôleur, groupe européen d'éthique, réforme de la protection des données (Bruxelles)
18 octobre	Contrôleur, conférence du coordinateur européen de la lutte contre la traite des êtres humains (Vilnius)
14 novembre	Contrôleur, conférence de midi de l'École européenne d'administration (Bruxelles)

Autres institutions et organes de l'Union européenne

22 janvier	Contrôleur et contrôleur adjoint, révision stratégique du CEPD (Bruxelles)
28 janvier	Contrôleur, journée de la protection des données - exposition artistique (Bruxelles) (*)
6 mars	Contrôleur, conférence du CESE sur une utilisation plus responsable de l'internet (Bruxelles) (*)
17 avril	Contrôleur adjoint, formation destinée aux délégués européens à la protection des données (Bruxelles)
12 juin	Contrôleur adjoint, atelier du CEPD sur les communications électroniques (Bruxelles)

24/26 juin	Contrôleur et contrôleur adjoint, programme de formation et de certification de la protection des données de l'IEAP (Maastricht)
4 juillet	Contrôleur, université d'été de l'IUE, législation européenne en matière de protection des données (Florence)
19 septembre	Contrôleur adjoint, atelier du CEPD sur les sites internet et les dispositifs mobiles (Bruxelles)
11 octobre	Contrôleur, conférence de Frontex sur le contrôle automatisé aux frontières (Varsovie)
18 novembre	Contrôleur, conférence de l'AFE, législation européenne en matière de protection des données (Trèves) (*)
2 décembre	Contrôleur, forum d'experts sur l'internet et la protection des données à la CJUE (Luxembourg)
11 décembre	Contrôleur, conférence de l'ENISA sur la cybersécurité (Bruxelles)

Conférences internationales

9 janvier	Contrôleur, conférence sur les aspects éthiques du respect de la vie privée (Tallinn) (*)
25 janvier	Contrôleur, conférence «Ordinateurs, vie privée et protection des données» (Bruxelles)
31 janvier	Contrôleur adjoint, atelier international du Taiex sur la protection des données (Zagreb)
21 mars	Contrôleur, conférence de CONSENT sur la réforme de la protection des données (Malte)
24 avril	Contrôleur, conférence «Intensive» de l'IAPP sur la réforme de la protection des données (Londres)
14 mai	Contrôleur, journée européenne de la protection des données (Berlin)
16 mai	Contrôleur et contrôleur adjoint, conférence européenne sur la protection des données (Lisbonne)
30 mai	Contrôleur, conférence de l'ONU sur l'e-gouvernement (Helsinki)
26 septembre	Contrôleur, conférence internationale sur la protection des données (Varsovie) (*)
10 octobre	Contrôleur, forum de l'IIC sur les télécommunications et les médias (Londres)
24 octobre	Contrôleur adjoint, protection des données dans le système judiciaire (Budapest) (*)
6 décembre	Contrôleur, Conseil de l'Europe, conférence sur la cybercriminalité (Strasbourg)
11 décembre	Contrôleur, table ronde de l'IAPP sur les flux de données transfrontaliers (Bruxelles)

Autres événements

23 janvier	Contrôleur, audition sur la réforme de la protection des données au Parlement néerlandais (La Haye)
23 janvier	Contrôleur, forum de «Future of privacy» sur la réforme de la protection des données (Bruxelles)
23 janvier	Contrôleur adjoint, conférence «Ordinateurs, vie privée et protection des données» (Bruxelles)
8 février	Contrôleur, conférence de SURF sur la réforme de la protection des données (Amsterdam)
19 février	Contrôleur, atelier du CIPL sur l'analyse (Bruxelles)
21 février	Contrôleur, atelier sur la responsabilisation (Varsovie)
22 février	Contrôleur adjoint, Sénat italien, réforme de l'UE et données en matière de santé (Rome)
5 mars	Contrôleur adjoint, forum de «Future of Privacy» sur la prise en considération du respect de la vie privée dès la conception (Washington DC)
5 mars	Contrôleur adjoint, séance d'information aux représentants des États membres de l'UE sur la réforme de l'UE (Washington DC)
8 mars	Contrôleur adjoint, sommet mondial sur la vie privée de l'IAPP (Washington DC)

14 mars	Contrôleur, ministère néerlandais de la justice, réforme de la protection des données (La Haye)
15 mars	Contrôleur, association du barreau français, législation européenne en matière de protection des données (Bruxelles) (*)
26 mars	Contrôleur, e-Forum de Westminster, réforme de la protection des données (Londres)
27 mars	Contrôleur, C-PET, réforme de la protection des données (Bruxelles)
28 mars	Contrôleur, conférence du Point, maison connectée et intelligente (Paris) (*)
4/5 avril	Contrôleur et contrôleur adjoint, la protection des données dans les procédures pénales (Barcelone)
8 avril	Contrôleur adjoint, forum numérique du CEPS sur le traitement des données en ligne (Bruxelles)
13 avril	Contrôleur adjoint, vie privée et ouverture, système judiciaire administratif italien (Rome)
16 avril	Contrôleur, Forum UE/États-Unis sur les affaires juridiques et économiques (Bruxelles)
19 avril	Contrôleur adjoint, école supérieure italienne d'économie et de finance (Rome)
23 avril	Contrôleur, séminaire d'EMC sur les données volumineuses (Breukelen)
23 avril	Contrôleur, Hogan Lovells, réforme de la protection des données (Londres)
24 avril	Contrôleur adjoint, association du barreau français (Paris) (*)
13 mai	Contrôleur, conférence à l'HUB, réforme de la protection des données (Bruxelles)
20 mai	Contrôleur, forum sur le droit de la vie privée (Chantilly)
21 mai	Contrôleur adjoint, ministère lituanien de la justice, réforme de la protection des données (Vilnius)
23 mai	Contrôleur adjoint, Privacy Day Forum (Pise)
30 mai	Contrôleur adjoint, Customer in Control in an Age of Ubiquitous Data (Bruxelles)
5 juin	Contrôleur, Health Privacy Summit (Washington DC)
13 juin	Contrôleur, séminaire de Covington sur la protection des données et la concurrence (Bruxelles) (*)
20 juin	Contrôleur, présentation du livre de Wilson & Sonsini (Bruxelles)
2 juillet	Contrôleur, atelier d'EFC sur la protection des données et la recherche (Bruxelles)
5 juillet	Contrôleur adjoint, conférence sur la réforme européenne de la protection des données (Barcelone)
9 juillet	Contrôleur adjoint, université d'Amsterdam, institut pour le droit de l'information (Amsterdam)
10 juillet	Contrôleur, EPC, programme post-Stockholm (Bruxelles)
3 septembre	Contrôleur, CEPS, réunion politique sur les frontières intelligentes (Bruxelles)
4 septembre	Contrôleur, atelier de l'EPIF sur la lutte contre le blanchiment d'argent (Bruxelles)
10 septembre	Contrôleur, 12e conférence annuelle sur la protection des données (Londres)
12 septembre	Contrôleur, Forum UE/États-Unis sur les affaires juridiques et économiques (Berlin)
17 septembre	Contrôleur adjoint, 4e conférence annuelle sur la protection des données et le respect de la vie privée (Bruxelles)
18 septembre	Contrôleur, DMEXCO, vie privée sur l'internet (Cologne)
19 septembre	Contrôleur, Digital Enlightenment Forum (Bruxelles) (*)
20 septembre	Contrôleur, fédération bancaire européenne (Bruxelles)
24 septembre	Contrôleur adjoint, premier atelier du projet Phaedra (Varsovie)

30 septembre	Contrôleur, Freedom - Not Fear (Bruxelles)
30 septembre	Contrôleur, Rotary, la protection des données après l'affaire Snowden (Tervuren)
2 octobre	Contrôleur adjoint, fondation Benzi, biotechnologies et sciences innovantes (Bari)
4 octobre	Contrôleur adjoint, confédération de l'industrie, réforme de l'UE (Rome)
14 octobre	Contrôleur, Compliance Week, réforme de la protection des données (Bruxelles)
22 octobre	Contrôleur, European Voice, conférence sur la protection des données (Paris)
25 octobre	Contrôleur, protection des données dans les procédures pénales (Barcelone)
30 octobre	Contrôleur, institut Europa, conférence sur la réforme de la protection des données (Zurich) (*)
31 octobre	Contrôleur, université de Zurich, conférence sur les données volumineuses (Zurich)
7 novembre	Contrôleur, séminaire BBA, réforme de la protection des données (Londres)
12 novembre	Contrôleur, conférence sur la protection des données (Valence-Castellón)
25 novembre	Contrôleur, association des anciens étudiants de King's College (Bruxelles)
30 novembre	Contrôleur, réunion plénière du CCBE, surveillance de masse (Bruxelles)
3 décembre	Contrôleur et contrôleur adjoint, AECA, réforme de la protection des données (Bruxelles)
12 décembre	Contrôleur adjoint, congrès 2013 d'IAPP Europe sur la protection des données (Bruxelles)

(*) Texte disponible sur le site internet du CEPD

Annexe H — Composition du secrétariat du CEPD

Directeur, chef du Secrétariat

Christopher DOCKSEY

• Supervision et mise en application

Sophie LOUVEAUX *Chef d'unité faisant fonction*	Maria Verónica PEREZ ASINARI *Responsable consultations administratives*
Delphine HAROU *Responsable contrôles préalables*	Stephen ANDREWS *Assistant supervision et mise en application*
Raffaele DI GIOVANNI BEZZI* *Juriste*	Daniela GUADAGNO *Juriste / Expert national détaché*
Ute KALLENBERGER *Juriste*	Xanthi KAPSOSIDERI *Juriste*
Owe LANGFELDT *Juriste*	Antje PRISKER *Juriste*
Bénédicte RAEVENS *Juriste*	Dario ROSSI *Assistant supervision et mise en application* *Correspondant comptabilité* *Vérificateur financier ex-post*
Tereza STRUNCOVA *Juriste*	Michaël VANFLETEREN *Juriste*

• Politique législative et consultation

Hielke HIJMANS *Chef d'unité*	Anna BUCHTA *Responsable contentieux et politique législative*
Herke KRANENBORG* *Responsable contentieux et politique législative*	Anne-Christine LACOSTE *Responsable coopération internationale et politique législative*
Zsuzsanna BELENYESSY *Juriste*	Gabriel Cristian BLAJ *Juriste*
Alba BOSCH MOLINE *Juriste*	Isabelle CHATELIER *Juriste*
Christian D'CUNHA *Juriste*	Priscilla DE LOCHT *Juriste*
Elena JENARO *Juriste*	Amanda JOYCE *Assistante politique et consultation*
Elise LATIFY *Juriste*	Per JOHANSSON *Juriste*
Vera POZZATO *Juriste*	Galina SAMARAS* *Assistante politique et consultation*

• Politique IT

Achim KLABUNDE *Chef de secteur*	Massimo ATTORESI *Conseiller technologie et sécurité*
Andy GOLDSTEIN *Conseiller technologie et sécurité RLSI*	Luisa PALLA *Gestionnaire des documents/archiviste*
Bart DE SCHUITENEER *Conseiller technologie*	Hannes TSCHOFENIG* *Conseiller technologie*

• Groupe de gestion des documents

Andrea BEACH* *Chef de secteur*	Marta CORDOBA-HERNANDEZ *Assistante administrative*
Kim DAUPHIN* *Assistante administrative / intérimaire*	Alicia DUARTE *Assistante administrative*
Milena KEMILEVA *Assistante administrative*	Milan KUTRA* *Assistante administrative*
Kim Thien LÊ *Assistante administrative*	Séverine NUYTEN *Assistante administrative*
Ewa THOMSON* *Assistante administrative*	

(*) Membres du personnel ayant quitté le CEPD dans le courant de l'année 2013

• Information et communication

Olivier ROSSIGNOL *Chef de secteur*	Parminder MUDHAR *Conseiller information et communication*
Agnieszka NYKA *Conseiller information et communication*	Benoît PIRONET *Développeur web*

• Ressources humaines, budget et administration

Leonardo CERVERA NAVAS *Chef d'unité*	Maria SANCHEZ LOPEZ *Responsable finances*
Pascale BEECKMANS *Assistante finances* *GEMI*	Laetitia BOUAZZA-ALVAREZ *Assistante administrative*
Fabienne DUCAUD *Assistante administrative*	Anne LEVÊCQUE *Assistante ressources humaines & gestion des congés*
Vittorio MASTROJENI *Conseiller ressources humaines*	Julia MOLERO *Assistante finances*
Daniela OTTAVI *Conseiller finances et passation de marchés*	Aida PASCU *Assistante administrative* *RLS*
Sylvie PICARD *Déléguée à la protection des données* *Coordinatrice du contrôle interne*	Anne-Françoise REYNDERS *Assistante ressources humaines & coordinatrice formation*

Contrôleur européen de la protection des données

Rapport annuel 2013

Luxembourg: Office des publications de l'Union européenne, 2014

2013 — 138 pp. — 21 × 29.7 cm

ISBN 978-92-95076-85-3
doi: 10.2804/58291

COMMENT VOUS PROCURER LES PUBLICATIONS DE L'UNION EUROPÉENNE?

Publications gratuites:

- un seul exemplaire: sur le site EU Bookshop (http://bookshop.europa.eu);
- exemplaires multiples/posters/cartes:
  auprès des représentations de l'Union européenne (http://ec.europa.eu/represent_fr.htm),
  des délégations dans les pays hors UE (http://eeas.europa.eu/delegations/index_fr.htm),
  en contactant le réseau Europe Direct (http://europa.eu/europedirect/index_fr.htm)
  ou le numéro 00 800 6 7 8 9 10 11 (gratuit dans toute l'UE) (*).

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

Publications payantes:

- sur le site EU Bookshop (http://bookshop.europa.eu).

Abonnements:

- auprès des bureaux de vente de l'Office des publications de l'Union européenne (http://publications.europa.eu/others/agents/index_en.htm).

QT-AA-14-001-FR-N

Le Contrôleur Européen
de la protection des données

Le gardien européen de la protection des données

www.edps.europa.eu

Office des publications

@EU_EDPS