



Rapport Annuel d'Activité

Exercice
2012

1. Introduction	3
2. Résultats opérationnels	4
3. Gestion des ressources	4
4. Systèmes de gestion et de contrôle interne	5
4.1 Caractéristiques et nature des activités et des risques	5
4.1.1 LA MISSION DU CEPD	5
4.1.2 LE RÔLE CROISSANT DU CEPD	6
4.2 Révision stratégique de l'institution	10
4.2.1 LA RÉVISION STRATÉGIQUE	10
4.2.2 VALEURS FONDAMENTALES ET PRINCIPES DIRECTEURS	12
4.2.3 PLAN D'ACTION	15
4.2.4 MESURES ET PERFORMANCES	18
4.3 Coopération interinstitutionnelle	19
4.4 Evènements de l'année ayant un impact sur la réputation	20
4.5 Système de gestion de contrôle interne	20
4.6 Evaluation interne du système de contrôle interne et indicateurs soutenant la déclaration d'assurance	21
4.7 Résultats d'audit indépendant pendant l'exercice	21
4.7.1 COUR DES COMPTES	21
4.7.2 SERVICE AUDIT INTERNE (IAS)	22
4.7.3 SUIVI DE LA RÉOLUTION DE DÉCHARGE DU PARLEMENT EUROPÉEN	23
4.8 Suivi des réserves des exercices précédents	27
4.9 Conclusions sur l'efficacité du contrôle interne	27
5. Réserves et impact sur la déclaration	28
5.1 Les critères de matérialité	28
5.1.1 OBJECTIFS DES CRITÈRES DE MATÉRIALITÉ	28
5.1.2 CRITÈRES QUALITATIFS	28
5.1.3 CRITÈRES QUANTITATIFS	29
5.1.4 CRITÈRES DU SERVICE D'AUDIT INTERNE	29
5.2 Réserves	29
5.3 Conclusion	29
6. Déclaration d'assurance de l'Ordonnateur Délégué	30
7. ANNEXES	31
Annexe 1 : résumé du rapport annuel d'activité	32
Annexe 2 : budget 2012	33
Annexe 3 : tableau final de gestion des risques	35

1. Introduction

Le règlement financier (article 60 paragraphe 7¹) prévoit que chaque **ordonnateur délégué** transmet à son institution un [rapport annuel d'activité](#), accompagné des informations financières et de gestion. Ce rapport présente les réalisations de son unité prenant en considération les ressources utilisées. C'est également un rapport de gestion portant sur la performance dans le cadre de ses fonctions en tant qu'ordonnateur délégué. Cette nécessité est la conséquence logique du paragraphe 4² de ce même article qui rend l'ordonnateur délégué responsable pour les contrôles internes.

Dans le rapport annuel d'activité de l'ordonnateur délégué, l'ordonnateur délégué doit inclure une déclaration sur la base de son propre jugement et sur les informations à sa disposition, dans laquelle il :

- Déclare que les informations contenues dans son rapport sont sincères et véritables ;
- Affirme avoir l'assurance raisonnable que les ressources allouées aux activités décrites dans son rapport ont été utilisées aux fins prévues et conformément aux principes de bonne gestion financière, et que les procédures de contrôle mises en place donnent les garanties nécessaires quant à la légalité et la régularité des transactions sous-jacentes ;
- Confirme qu'il n'a connaissance d'aucun fait non signalé pouvant nuire aux intérêts de l'institution.

¹ Le règlement financier, article 60 paragraphe 7: L'ordonnateur délégué rend compte à son institution de l'exercice de ses fonctions sous la forme d'un rapport annuel d'activité, accompagné des informations financières et de gestion. Ce rapport indique les résultats de ses opérations par rapport aux objectifs qui lui ont été assignés, les risques associés à ces opérations, l'utilisation des ressources mises à sa disposition et le fonctionnement du système de contrôle interne. L'auditeur interne prend connaissance du rapport annuel d'activité, ainsi que des autres éléments d'information identifiés. Le Contrôleur transmet au plus tard le 15 juin de chaque année à l'autorité budgétaire un résumé des rapports annuels d'activités de l'année précédente.

² Le règlement financier, article 60 paragraphe 4: L'ordonnateur délégué met en place, conformément aux normes minimales arrêtées par chaque institution et en tenant compte des risques associés à l'environnement de gestion et à la nature des actions financées, la structure organisationnelle ainsi que les systèmes et les procédures de gestion et de contrôle internes adaptés à l'exécution de ses tâches, y compris, le cas échéant, des vérifications ex post.

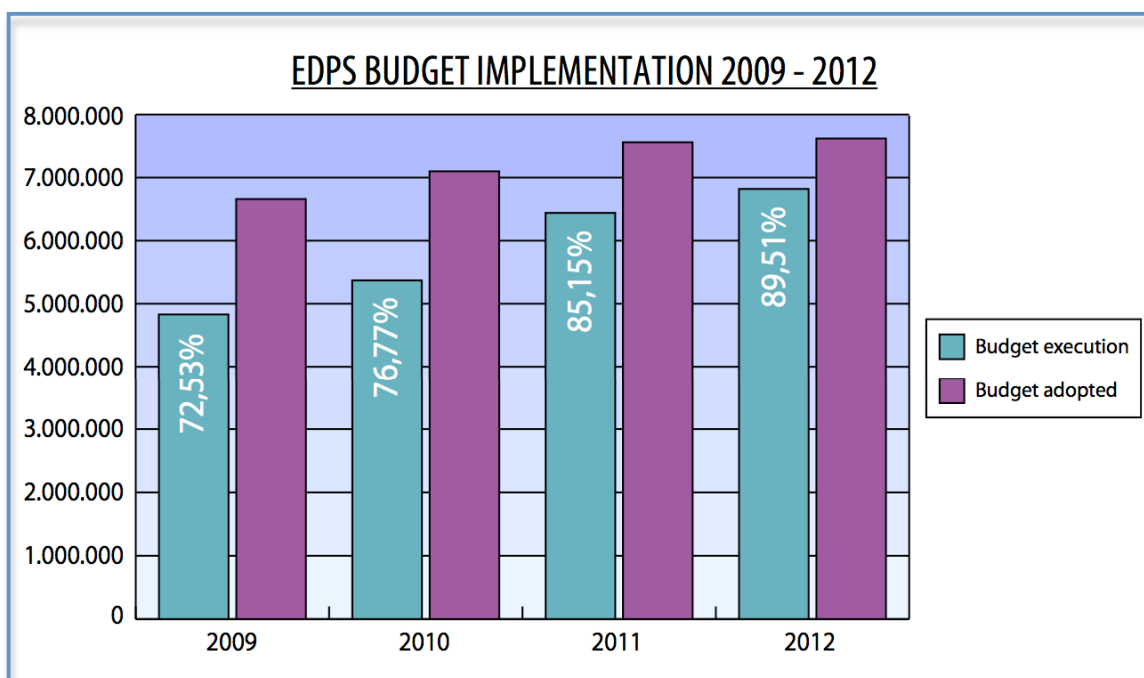
2. Résultats opérationnels

Chaque année, le CEPD publie un "rapport annuel" qui présente un aperçu des objectifs et des résultats du travail de l'institution. Les informations sur les résultats opérationnels se trouvent dans le rapport annuel³.

3. Gestion des ressources

Le budget pour l'année 2012 adopté par l'autorité budgétaire est de 7.624.090,00 € (voir Annexe 2).

Ceci représente une augmentation de 0.79 % par rapport au budget de l'année 2011. Le taux d'exécution estimé pour l'année 2012 serait de 89.51 % contre 85.15% pour l'année 2011.



Le CEPD applique les règles internes de la Commission européenne en ce qui concerne la mise en œuvre du budget, dans la mesure où ces règles sont applicables à la structure et à la taille de l'institution et dans la mesure où le CEPD n'a pas adopté de règles spécifiques.

Sur base de l'accord de coopération interinstitutionnelle, le Comptable de la Commission a été nommé Comptable du CEPD et l'Auditeur interne de la Commission a été nommé Auditeur du CEPD.

³ <http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/lang/fr/AR>

4. Systèmes de gestion et de contrôle interne

4.1. Caractéristiques et nature des activités et des risques

4.1.1. LA MISSION DU CEPD

4.1.1.1. Le CEPD est le gardien européen de la protection des données

Le CEPD est l'autorité indépendante de la protection des données de l'Union européenne (UE). Il contrôle et veille 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.

Le CEPD conseille les institutions et organes de l'UE sur toutes les questions relatives au traitement des informations personnelles. Il est consulté par le législateur au sujet des propositions de textes législatifs et de l'élaboration de nouvelles politiques. Il suit également le développement des nouvelles technologies qui pourraient affecter la protection des informations personnelles. Il intervient devant la Cour de justice de l'UE pour fournir des avis d'experts sur l'interprétation des textes de loi concernant la protection des données. Enfin, il coopère avec les autorités de contrôle nationales et autres organes de même nature pour améliorer la cohérence en matière de protection des données à caractère personnel.

4.1.1.2. La protection des données est cruciale pour la société

La protection des données à caractère personnel est essentielle pour les citoyens de la société de l'information. Étant donné que les personnes sont de plus en plus dépendantes de l'utilisation des technologies de l'information (utilisation des paiements en ligne, des réseaux sociaux et des moteurs de recherche, par exemple) et qu'un nombre toujours plus élevé d'informations à caractère personnel est collecté ou généré, il importe plus que jamais que les libertés individuelles fassent l'objet d'une protection adéquate.

Les règles de protection des données ont été élaborées pour protéger les individus et faciliter le traitement licite de leurs informations personnelles. Ces règles énoncent le droit de toute personne de ne pas figurer dans des fichiers ou de ne pas être surveillée de manière abusive ou en l'absence de tout contrôle. L'objectif est de permettre aux individus d'exercer leurs droits et de protéger leurs intérêts légitimes.

Le droit fondamental à la protection des données et au respect de la vie privée ne peut être réalisé que si les règles de protection des données sont effectivement respectées dans la pratique.

4.1.1.3. Garantir la protection du droit fondamental au respect de la vie privée

Le CEPD est une autorité indépendante dotée d'une expertise dans le domaine de la protection des données à l'échelle de l'UE, qui intervient également, plus largement, aux niveaux national et international. Son objectif consiste à travailler de manière stratégique pour promouvoir une «culture de protection des données» au sein des institutions et organes de l'UE et contribuer ainsi à améliorer les principes de bonne administration et de gestion efficace des risques. Il œuvre en vue d'intégrer le respect des principes de protection des données à la législation et aux politiques de l'UE et cherche à améliorer la qualité des politiques de l'UE chaque fois que l'efficacité de la protection des données est une condition essentielle à leur succès.

L'intervention du CEPD s'avère efficace s'il parvient à communiquer le message relatif à la protection des données et à impliquer tous les acteurs concernés. Si nécessaire, il use également de ses pouvoirs d'investigation et de mise en application de la législation afin de garantir le respect des règles.

4.1.1.4. Communiquer sur la protection des données: une condition essentielle pour la rendre plus effective

Le CEPD entend sensibiliser l'opinion à la protection des données et informer les individus sur l'existence et le contenu de leurs droits. Pour gagner la confiance du public et s'assurer qu'il comprend et soutient sa démarche, il est essentiel d'améliorer la transparence du traitement des données à caractère personnel au niveau de l'UE et d'accéder à davantage d'informations sur la protection des données dans l'Union. C'est pourquoi le CEPD communique de façon à ce que le public comprenne facilement le message.

4.1.2. LE ROLE CROISSANT DU CEPD

En tant qu'**organe de contrôle, de supervision et de mise en application de la législation**, le CEPD exerce une pression plus forte sur l'administration de l'UE afin qu'elle respecte davantage les règles régissant la protection des données. Pour ce faire, il multiplie ses actions de supervision et de suivi en procédant à des contrôles préalables, des enquêtes, des visites et des inspections. Il a conçu des outils externes pour aider les responsables du traitement des données à respecter les règles établies en fournissant un meilleur support aux Délégués à la Protection des Données (DPD) et Coordinateurs à la Protection des données (CPD) par le biais notamment de formations, de lignes directrices et d'enquêtes de suivi. Après la déclaration politique formulée dans le document stratégique du CEPD sur le respect et l'application de la législation en décembre 2010, ce dernier a de plus en plus exercé ses pouvoirs lorsque cela s'avérait nécessaire.

En tant que **conseiller**, le CEPD reçoit désormais davantage de demandes d'avis formels et informels tant en ce qui concerne des mesures administratives que des initiatives législatives. La protection des données est en effet en pleine expansion dans tous les domaines de la politique de l'UE du fait du développement de nouveaux instruments reposant sur des outils informatiques destinés à faciliter les échanges d'informations. De même, il est désormais un partenaire à part entière des institutions de l'UE, qui le consultent régulièrement dans le cadre de l'élaboration des politiques et de la législation. En outre, il fournit de plus en plus fréquemment des avis d'experts sur l'interprétation de la législation en matière de protection des données dans le cadre des actions en justice, que ce soit de sa propre initiative ou à la demande des juridictions.

La **coopération** avec d'autres autorités de contrôle gagne également en importance du fait de la participation plus active du CEPD au travail des forums des autorités chargées de la protection des données au sein de l'UE (p. ex. groupe de travail «Article 29»), ainsi qu'au travers de la consolidation et de l'expansion de la méthode dite de **supervision coordonnée**. Il s'agit d'un modèle de supervision pour les systèmes informatiques européens à grande échelle impliquant à la fois le CEPD et les autorités nationales chargées de la protection des données (APD) au sein duquel il fait office de secrétariat.

Dans un monde hyper-connecté caractérisé par des technologies en constante évolution et un nombre croissant d'échanges d'informations personnelles, la protection des données à caractère personnel requiert des **approches globales, coordonnées et transfrontalières**. Par conséquent, des initiatives innovantes visant à promouvoir la protection des données ont également été présentées par le CEPD lors de la Conférence internationale des commissaires à la vie privée et à la protection des données, lors de la Conférence européenne sur la protection des données, dans le contexte de l'OCDE, du Conseil de l'Europe et du Groupe de Berlin (groupe d'experts internationaux sur la protection des données et les télécommunications), ainsi que dans le cadre d'une série d'ateliers sur la protection des données axés sur la «bonne gouvernance» dans les organisations internationales.

La sensibilisation aux questions relatives à la protection des données ayant été renforcée au sein de l'administration de l'UE au fil des ans, la **visibilité** du CEPD a, elle aussi, progressé. Cela a naturellement amélioré l'interaction avec l'Union européenne et les diverses institutions nationales, de même qu'avec les citoyens et les médias, et conduit les parties prenantes à consulter plus fréquemment le CEPD sur un ensemble de questions beaucoup plus vaste.

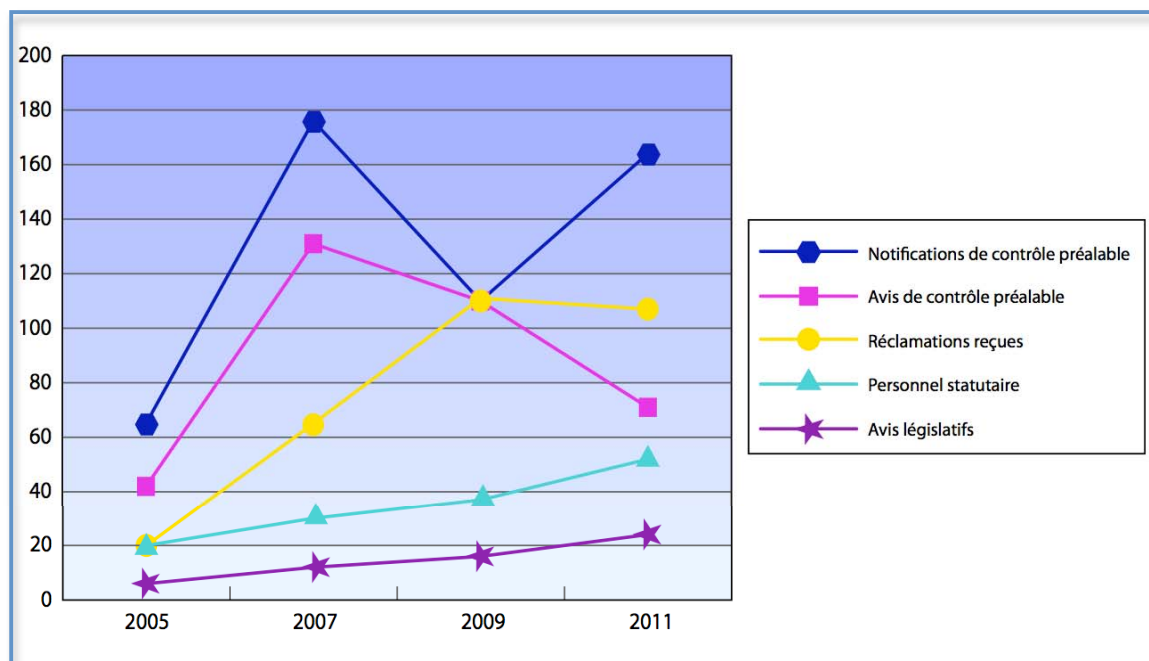
S'adapter aux nouveaux défis

Outre l'augmentation de ses activités, le CEPD doit faire face à plusieurs évolutions majeures :

- l'accélération de l'utilisation d'internet et des nouvelles technologies ;
- l'entrée en vigueur du traité de Lisbonne, qui met l'accent sur les droits fondamentaux ;
- l'adoption et la poursuite de la mise en œuvre d'un nouveau programme politique concernant l'espace de liberté, de sécurité et de justice (programme de Stockholm) et l'importance capitale de la protection des données dans cet espace ;
- l'adoption, la révision et la poursuite de la mise en œuvre de la stratégie de la Commission destinée à soutenir l'essor de l'internet et à susciter la confiance des utilisateurs (stratégie numérique) et son impact sur la protection des données, et
- le processus de révision en cours du cadre juridique de la protection des données de l'UE, notamment la question sensible de la gouvernance et de ses implications pour la coopération entre les autorités chargées de la protection des données.

Le traité de Lisbonne a introduit une solide base juridique pour un cadre complet de protection des données dans tous les domaines de la politique européenne, qui exerce une pression considérable sur les ressources limitées du CEPD. La fin de la séparation traditionnelle des «piliers» politiques de l'UE (communautés européennes et coopération policière et judiciaire en matière pénale) a entraîné à ce qu'un plus grand nombre d'activités de traitement relatives à l'«application de la législation» tombent sous le champ d'application du droit de l'Union européenne et soient dès lors soumises à la supervision du CEPD.

Le graphique ci dessous montre une nette augmentation de l'ensemble des activités du CEPD au fil des ans, ce qui nécessite d'investir énormément de ressources. Or, les effectifs sont demeurés au même niveau. Les évolutions soulignées ci-dessus suggèrent également que l'augmentation de sa charge de travail risque de se poursuivre dans la plupart des domaines. Pour faire face à cette hausse avec efficacité et efficience, le CEPD devra «faire plus avec moins», dans la limite des ressources humaines dont il dispose actuellement.



Le CEPD ne dispose, pour mener l'ensemble de ses missions, que de crédits administratifs annuels, d'un montant relativement peu élevé. Le CEPD a adopté les procédures spécifiques de contrôle interne jugées les mieux adaptées à ses besoins en fonction de la taille de l'institution et de ses activités. L'objectif est de fournir à la direction une assurance raisonnable quant à la réalisation des objectifs de l'institution et à la gestion des risques liés à ses activités. Le CEPD a progressé dans l'identification des risques liés au développement de ses activités notamment par l'adoption d'une décision en matière de gestion des risques adoptée en juillet 2012. Cela permettra une approche plus structurée dans la gestion des risques comme a pu le démontrer l'adoption du tableau final des risques (*voir annexe 3*) à la suite des workshops qui sont tenus en septembre et octobre 2012 tels que prévus dans la décision. Une révision de la décision sur les contrôles internes ainsi qu'une décision en matière de gestion de qualité (CAF) seront adoptées en 2013.

Le CEPD n'a pas d'activité opérationnelle au sens Activity Based Budget, comme à la Commission, mais bien des dépenses administratives (limitées). Tout engagement financier et contractuel est soumis à l'accord de l'ordonnateur délégué ou subdélégué et vérifié au préalable par un membre de son équipe. L'introduction d'un nouveau système de vérification financière interne, la nomination d'un correspondant comptable et l'adoption d'un système de vérification ex-post a conduit à un renforcement notable des contrôles internes au sein du CEPD.

4.2. Révision stratégique de l'institution



EN RESUME

En Juillet 2011, face à une charge de travail accrue et un plus large champ d'activités, le CEPD a lancé un processus de révision stratégique. L'objectif de l'étude était d'identifier les priorités et élaborer une stratégie pour répondre efficacement à ces défis et la nécessité de «faire plus avec moins» dans les années à venir.

La révision stratégique a été réalisée grâce à un vaste processus de consultation de ses partenaires internes et externes et a abouti à l'élaboration d'une stratégie pour les deux années qui jette également les bases pour le long terme. Cette stratégie lui permettra de respecter ses engagements envers les citoyens et les institutions et organes communautaires dans un environnement difficile et en constante évolution. C'est aussi un moyen d'informer les parties prenantes sur la façon dont il mène ses activités.

La stratégie a été adoptée en Décembre 2012 sous la forme d'un rapport sur la stratégie pour 2013-2014 intitulé «Vers l'excellence en matière de protection des données»⁴.

La contribution pertinente de ses partenaires lui a permis de développer ses valeurs fondamentales et les principes directeurs sur lesquels élaborer un plan d'action détaillé pour la réalisation de ses objectifs stratégiques. Le rapport se termine par une liste d'indicateurs clés de performance permettant de mesurer la réussite.

Le CEPD a réévalué ses priorités et réaffecté ses ressources pour accroître son efficacité et efficacité afin de tenir compte des suggestions de ses partenaires.

Il continuera de développer et de renforcer sa stratégie afin de répondre efficacement au défi d'atteindre l'excellence en matière de protection des données au niveau européen au-delà de 2014

4.2.1. LA REVISION STRATEGIQUE

En juillet 2011, le conseil d'administration a lancé le processus de révision stratégique et créé un groupe de travail à cet effet. Les objectifs stratégiques définis amélioreront l'efficacité et l'impact des principales activités et optimiseront du même coup l'impact de la protection des données au niveau européen.

⁴

<http://www.edps.europa.eu/EDPSWEB/edps/lang/fr/EDPS/Publications/Strategy;jsessionid=1451994FE4657586276FC51B96B2D CAD>

4.2.1.1. Nos objectifs stratégiques

- 1. 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.**
- 2. 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.**
- 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'UE.**
- 4. Développer une stratégie de communication efficace.**
- 5. Améliorer l'utilisation des ressources humaines, financières, techniques et organisationnelles.**

4.2.1.2. Exploiter les points forts

Le processus de révision repose sur plusieurs modifications substantielles et organisationnelles déjà effectuées ou en cours :

- En 2005, le CEPD a publié sa politique sur les institutions de l'UE qui le consultent. Cette politique, qui est énoncée dans les priorités publiques annuelles (inventaire des politiques), a orienté ses activités jusqu'au processus de révision.
- En 2008, il a adopté ses orientations concernant les opérations de traitement des données en matière de recrutement de personnel et sa première session de formation destinée aux DPD a eu lieu en 2011.
- En 2010, il a adopté une nouvelle approche concernant le respect et la mise en application de la législation.
- Cette même année, le CEPD a entrepris de réorganiser le secrétariat en introduisant un nouveau cadre institutionnel constitué d'unités et de secteurs relevant d'un directeur. Ce processus a été achevé en 2012 avec la création d'un nouveau secteur dédié à la politique des technologies de l'information.

Les commentaires des parties prenantes à l'origine de certains de ces changements ont souligné la nécessité d'améliorer la communication sur les activités du CEPD déjà en place.

4.2.1.3. Le processus de consultation

La révision stratégique s'est déroulée en deux phases :

Consultation interne

L'objectif de la consultation interne était d'identifier les moyens disponibles pour améliorer l'efficacité de l'organisation afin d'être mieux à même de relever les défis et de saisir les opportunités à plus long terme. L'ensemble du personnel a été impliqué dans la définition de la stratégie. Les idées et propositions émises ont été analysées lors de la première conférence interne du CEPD organisée le 25 octobre 2011. Les conclusions des discussions internes ont posé les fondements de la consultation externe.

Consultation externe

Les acteurs externes ont été consultés afin de déterminer la manière dont ils perçoivent les activités de l'institution et d'identifier ce qui, selon eux, pourrait être amélioré dans la façon du CEPD de travailler avec eux et comment il pourrait y parvenir. La consultation externe a été lancée en mars 2012 par le biais d'une enquête en ligne.

4.2.2. VALEURS FONDAMENTALES ET PRINCIPES DIRECTEURS

Le CEPD a tenu compte des retours d'informations des diverses parties prenantes lors de la définition de ses valeurs fondamentales, de ses principes directeurs et de son plan d'action. Les principes suivants exposent la manière dont il aborde sa mission et indiquent comment il travaille avec les parties prenantes.

4.2.2.1. Les valeurs fondamentales

Toutes les activités du CEPD reposent sur les valeurs fondamentales suivantes :

- **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 qu'il fait et pourquoi il le fait dans un langage clair et accessible à tous ;
- **Pragmatisme** – comprendre les besoins des parties prenantes et rechercher des solutions qui fonctionnent dans la pratique.

4.2.2.2. Principes généraux

- A.** Le CEPD sert 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. Il contribue à l'élaboration des politiques au sens large dès lors qu'elles affectent la protection des données européenne.
- B.** En s'appuyant sur son expertise, son autorité et ses pouvoirs officiels, il entend 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.
- C.** Il centre son attention et ses 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. Il agit de manière sélective et proportionnée.

4.2.2.3. Principes spécifiques par activité

Les principes directeurs énoncés ci-dessous viennent compléter les principes fondamentaux de la protection des données, sans toutefois les remplacer.

- A)** Le CEPD use de son expertise et de son autorité pour exercer ses pouvoirs de supervision et de mise en application. Il cherche à garantir la protection des informations à caractère personnel, ainsi qu'un juste équilibre, tout en poursuivant des objectifs politiques plus larges.
- B)** Dans le cadre de ses activités de supervision et de mise en application :
 - a) il reconnaît que les institutions (responsables du traitement des données, DPD/CPD) endossent une responsabilité de premier plan ;
 - b) il s'efforce d'aider les institutions à assumer efficacement leurs responsabilités en veillant à mettre à leur disposition l'assistance, les formations et les conseils appropriés ;
 - c) il use de ses pouvoirs de supervision pour renforcer la responsabilité ;
 - d) il est prêt à user de ses pouvoirs d'exécution chaque fois que cela s'avère nécessaire.

- C)** Dans le cadre de son travail politique et consultatif :
 - a) il cherche à coopérer de manière constructive avec les responsables politiques à un stade précoce de l'élaboration des politiques ;
 - b) il cherche des solutions créatives qui soutiennent les objectifs politiques et les principes de protection de la vie privée en s'appuyant sur ses connaissances des législations et des technologies ;
 - c) il œuvre 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 ;
 - d) il cherche 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.

- D)** Dans le cadre de sa coopération avec d'autres autorités chargées de la protection des données et organes de contrôle :
 - a) il s'appuie sur son expertise et son expérience concernant la législation et les pratiques européennes en matière de protection des données ;
 - b) il cherche à améliorer la cohérence de la législation relative à la protection des données au sein de l'UE.

- E)** Le CEPD cherche à se positionner en tant qu'organe faisant autorité en développant l'expertise et l'assurance de son personnel pour pouvoir collaborer efficacement avec ses différentes parties prenantes.

4.2.3. PLAN D'ACTION

Pour atteindre ses objectifs, le CEPD a évalué et classé ses activités par ordre de priorité de manière à refléter les résultats internes et externes de la révision stratégique. Il a identifié les priorités suivantes pour chacun des objectifs stratégiques définis au point 4.2.1.1 supra.

OBJECTIF 1

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

- Mettre des orientations et des formations à la disposition des responsables du traitement des données, des DPD et des CPD.
- Multiplier les initiatives de sensibilisation au sein des institutions et organes de l'UE par le biais d'ateliers, de réunions, de séminaires, de formations et de conférences.
- Sensibiliser les acteurs à la protection des données à tous les niveaux d'encadrement et dans le cadre de divers forums.
- Encourager le dialogue avec les responsables du traitement des données, les DPD et les CPD.
- Augmenter le nombre de visites et d'inspections en tant qu'élément de notre politique relative au respect et à la mise en application des règles.
- Promouvoir et fournir des services d'orientation concernant l'application des principes de «respect de la vie privée dès la conception» et de «respect de la vie privée par défaut».

OBJECTIF 2

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

- Continuer à fournir en temps opportun des conseils avisés au législateur de l'UE sur toutes les questions liées au traitement des informations à caractère personnel durant toutes les phases de l'élaboration des législations et politiques.
- Accroître son utilisation de l'inventaire des initiatives politiques en étant plus sélectifs dans l'identification des initiatives pour lesquelles le respect de la protection des données est essentiel.
- Mettre à la disposition du législateur et des responsables politiques des lignes directrices incluant des conseils sur des questions horizontales.
- Renforcer les contacts avec les organes législatifs de l'UE à tous les niveaux. Il s'agit notamment d'entretenir des contacts informels réguliers pour contribuer à l'élaboration des politiques à un stade précoce et continuer à exercer une influence jusqu'au terme du processus législatif.
- Évaluer les risques liés à la vie privée induits par l'utilisation des nouvelles technologies en collectant et en analysant les informations appropriées.

OBJECTIF 3

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

- Contribuer activement aux réalisations du groupe de travail «Article 29» en participant à ses sous groupes, à la rédaction des avis et autres textes et en cherchant à améliorer les synergies au niveau de ses activités.
- Coopérer avec d'autres APD sur les questions concernant les politiques liées aux technologies et leur mise en œuvre et échanger l'expérience acquise et les meilleures pratiques avec leurs experts en la matière.
- Développer les méthodes de supervision coordonnée du nombre croissant de systèmes informatiques à grande échelle et publier des lignes directrices à ce sujet.

OBJECTIF 4

Développer une stratégie de communication efficace et créative.

- Mettre à jour et étoffer le site internet du CEPD.
- Développer de nouveaux outils de communication pour rendre les activités principales du CEPD plus visibles.
- Sensibiliser l'opinion à la protection des données par le biais d'ateliers, de réunions et de séminaires.
- Utiliser un langage clair pour rendre les questions techniques plus accessibles.

OBJECTIF 5

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

- Améliorer la planification et le suivi des activités.
- Mettre en œuvre une politique de formation efficace pour renforcer les compétences professionnelles.
- Améliorer la planification, la mise en œuvre et le suivi des ressources financières.
- Mettre en place une politique de gestion des ressources humaines plus stratégique.
- Renforcer la coopération administrative avec d'autres institutions de l'UE.
- Développer et mettre en œuvre un système exhaustif de gestion de la qualité.
- Moderniser la gestion des dossiers et des connaissances.
- Développer la stratégie interne du CEPD relative aux technologies de l'information.

4.2.4. MESURE DES PERFORMANCES

Pour mesurer les progrès accomplis dans le cadre de la réalisation de ses objectifs, le CEPD mesurera régulièrement les performances des activités répertoriées ci-dessus. Il a identifié les activités qui jouent un rôle clé dans la réalisation de ses objectifs et les a retenues pour constituer la base des indicateurs clés de performance (ICP) présentés ci-dessous. Ces indicateurs lui permettront d'évaluer l'impact de son travail, ainsi que son niveau d'efficacité quant à l'utilisation des ressources. Ils seront revus régulièrement et adaptés si nécessaire afin d'améliorer ses performances futures. Le CEPD présentera les premiers résultats à ce sujet dans son rapport d'activité annuel 2013.

- ICP 1** Nombre d'inspections ou de visites effectuées.
- ICP 2** Nombre d'initiatives de sensibilisation et de formations au sein des institutions et organes de l'UE que le CEPD a organisées ou co-organisées (ateliers, réunions, conférences, formations et séminaires).
- ICP 3** Niveau de satisfaction des DPD/CPD par rapport aux formations et aux orientations.
- ICP 4** Nombre d'avis formels et informels formulés à l'endroit du législateur.
- ICP 5** Taux d'exécution des dossiers identifiés dans son inventaire des politiques de l'UE comme devant faire l'objet d'une action.
- ICP 6** Nombre d'affaires traitées par le groupe de travail «Article 29» pour lesquelles le CEPD a apporté une contribution écrite substantielle.
- ICP 7** Nombre d'affaires pour lesquelles des orientations sur les développements technologiques sont fournies.
- ICP 8** Nombre de visites sur le site Internet du CEPD.
- ICP 9** Taux d'exécution du budget.
- ICP 10** Taux de mise en œuvre des formations destinées au personnel du CEPD.

4.3. Coopération interinstitutionnelle

Le CEPD bénéficie d'un accord de coopération interinstitutionnelle générale en vertu de l'accord conclu en 2004, avec les secrétaires généraux de la Commission, le Parlement et le Conseil, qui a été prolongé en 2006 (pour une période de trois ans) et en 2010 (pour une période de deux ans) sans autre participation du Conseil. Une nouvelle prolongation de l'accord a été signée par les secrétaires généraux de la Commission, le Parlement et le CEPD en Décembre 2011 pour une autre période de deux ans. Cette coopération est fondamentale pour le CEPD car elle lui permet d'accroître son efficacité mais également des économies d'échelle.

En raison du déménagement du CEPD en octobre 2012 dans un nouveau bâtiment du Parlement européen, les annexes de cet accord interinstitutionnel liées au Parlement européen ont été renégociées. Elles portent tout particulièrement sur les aspects IT, la sécurité et le courrier. Ces annexes devraient être signées en juin 2012.

Par ailleurs cette coopération interinstitutionnelle s'est poursuivie en 2012 essentiellement avec le service d'audit interne de la Commission européenne.

L'IAS et le CEPD ont un intérêt commun dans le domaine de l'audit. C'est pourquoi un protocole d'accord (Mémoire of Understanding - MoU) pour permettre aux deux organisations de s'acquitter de leurs rôles dans la manière la plus efficace a été conclu avec le plein respect de leurs droits respectifs, les obligations et l'indépendance comme prévu dans leurs documents constitutifs.

Un accord de niveau de service (SLA) entre l'IAS et le CEPD a été signé en même temps. Depuis Septembre 2004, date de la nomination de l'IAS en tant qu'auditeur interne du CEPD, ce Service a fourni des services d'audit dans le cadre de l'accord interinstitutionnel entre le Parlement européen, la Commission européenne et le CEPD. Alors que l'accord avec la Commission expirera en Décembre 2013 et ne sera probablement pas renouvelé, ce SLA agit comme un document autonome sur lequel peuvent se fonder les services d'audit futurs.

Enfin, une charte de mission IAS a également été signée. Cette charte énonce la mission, les objectifs, les rapports et les modalités de travail qui sont essentielles à la bonne exécution du rôle de l'IAS envers le CEPD.

Pour conclure, l'institution est membre de divers comités interinstitutionnels et groupes de travail dont notamment le Collège des Chefs d'administration, le Comité de Gestion Assurance maladie, le Comité de Préparation des Questions Statutaires, le Comité du Statut, le groupe de travail interinstitutionnel de l'EUSA, le conseil d'administration d'EPSO/EUSA, le groupe de travail d'EPSO, la Commission paritaire commune et le Comité de préparation pour les Affaires sociales.

4.4. Evènements de l'année ayant un impact sur la réputation

Pendant l'année 2012, aucun évènement n'a eu ou pu avoir un impact négatif sur la réputation de l'institution.

4.5. Système de gestion de contrôle interne

Le système de contrôle interne, en vigueur depuis 2006, gère le risque d'échec à atteindre les objectifs de l'institution. En 2012, la liste des actions de mise en œuvre a été étendue afin d'assurer l'efficacité du contrôle interne des processus en place. A titre d'exemple, une version révisée de toutes les descriptions de poste, les règles internes de procédure (article 46.k du règlement (CE) 45/2001), la présentation des activités des unités à tout le personnel, un manuel sur l'accès aux documents et un registre des risques nouveaux sont des actions qui ont été adoptées pour mettre en œuvre les standards de contrôle interne (SCI).

Une décision révisée sur les SCI sera adoptée en Janvier 2013 afin de simplifier l'approche, accroître l'appropriation et renforcer leur efficacité.

Afin d'acquérir une plus grande autonomie dans le domaine des marchés publics, le CEPD a adopté en juin 2012 ses lignes directrices pour les marchés publics de faible valeur.

Le système à trois niveaux de planification des activités (stratégique, annuel et hebdomadaire) est le fondement de la gestion de la charge de travail du CEPD. Cette planification a été mise en œuvre en 2012 de façon détaillée.

Un plan annuel de gestion a été élaboré décrivant les activités qui seront menées par objectif spécifique. En raison de la nature du travail de réglementation et de conseil du CEPD, tout ne peut être prévu. Lié par des ressources fixes, il doit être capable d'adapter son planning en conséquence. A ceci s'ajoutent des indicateurs clés de performance définis et mesurés régulièrement pour suivre les progrès accomplis au cours des années à venir.

Suite à l'adoption d'un plan de gestion annuel au début de l'année 2012, une décision relative à la gestion des risques a été adoptée en Juillet 2012 - outils contemporains qui aident à identifier les risques et les plans d'action possibles. La gestion des risques va au-delà de l'évaluation des risques, elle implique également une mise en place des contrôles et des mesures qui doivent ensuite être suivis. Ainsi la CEPD a-t-il inclus la gestion du risque comme un élément essentiel de sa stratégie globale de gestion de qualité totale (TQM pour Total Quality Management).

Ces contrôles mis en place par le CEPD ainsi que ces circuits et procédures ont pour objet de corriger toute erreur tant de nature financière que de procédure pouvant survenir. Ils sont intégrés, tout comme les corrections éventuelles qu'ils engendrent, dans la gestion du CEPD. Les corrections sont de ce fait connues par l'ordonnateur délégué. Ni leur nature ni leur fréquence n'ont revêtu une importance significative.

4.6. Évaluation interne du système de contrôle interne et indicateurs soutenant la déclaration d'assurance

En 2011, le CEPD a poursuivi la mise en œuvre des recommandations découlant de l'évaluation de son système de contrôle interne effectuée en 2008. Il ne reste plus à ce jour que trois recommandations à terminer de mettre en œuvre. Il s'agit du système électronique d'enregistrement et archivage du courrier (dernière étape de mise en œuvre pour fin 2013), de la gestion des dossiers de mission et enfin de la supervision des dossiers du personnel.

Ces deux dernières recommandations ont été mises en œuvre par le CEPD. Un effort substantiel a été accompli en matière de missions avec la mise en œuvre de MIPS. Les dossiers personnels ont été intégralement revus afin de procéder à leur numérisation (NDP) par l'intermédiaire la Commission européenne suite à la mise en œuvre de Sysper 2 au sein du CEPD. Lors de la prochaine visite de l'IAS (juin 2013) ces deux recommandations pourraient être clôturées par l'auditeur interne.

A ce stade, l'ordonnateur délégué estime le niveau de la gestion et du contrôle mis en place approprié, même s'il continue de l'améliorer. De telles améliorations ne sont pas de nature à avoir un impact "matériel" au sens du paragraphe 5.1. Aucune réserve n'est nécessaire par rapport à ces améliorations en cours.

Au moment de la rédaction de ce rapport annuel d'activité, on peut constater qu'aucune erreur significative ne s'est produite et qu'aucune réserve quant aux contrôles préventifs n'est nécessaire.

Pour ces raisons, aucune des recommandations pour lesquelles la mise en œuvre est encore en cours n'est susceptible d'avoir un impact matériel⁵.

4.7. Résultats d'audit indépendant pendant l'exercice

Il existe deux types d'audit indépendant applicables au CEPD. Un premier est le travail de la Cour des comptes européenne, un deuxième est le travail de l'Auditeur Interne de l'institution.

4.7.1. COUR DES COMPTES

Le rapport de la Cour des comptes européenne concernant l'exercice 2012, est parvenu mais reste encore de nature confidentielle et provisoire. Le contenu ne concerne que le suivi d'une recommandation précédente qui ne semble revêtir aucun caractère substantiel et la réponse du CEPD semble donner toute satisfaction à la Cour des Comptes.

⁵ Les critères de matérialité utilisés pour ce jugement sont expliqués dans le chapitre 5.1 de ce rapport.

4.7.2. SERVICE AUDIT INTERNE (IAS)

L'Auditeur Interne de la Commission est l'auditeur interne du CEPD. Afin de garantir une gestion efficace des ressources du CEPD, l'auditeur interne effectue des contrôles réguliers sur les systèmes de contrôles internes du CEPD ainsi que sur ses opérations financières.

Enfin, en novembre 2011, l'IAS est venu auditer l'activité opérationnelle "Contrôle et mise en application" au sein du CEPD. Le rapport final a été émis en avril 2012 suite aux discussions et échanges approfondis entre le CEPD et l'IAS et, comprend 19 recommandations.

En Juin 2012, à la suite de cette vérification spécifique, l'IAS a émis un rapport consultatif sur le processus d'inspection du CEPD. L'objectif de cette mission de conseil a été de fournir des recommandations pour améliorer plus encore le processus d'inspection du CEPD. Les domaines d'amélioration concernent les points suivants :

- l'approche stratégique,
- les processus d'inspection,
- la gestion des ressources et des mesures de surveillance mises en place par les soins du CEPD afin de lancer le processus de manière efficace et efficiente.

En mai 2012, l'IAS a émis le rapport annuel de vérification interne (ARIA - l'article 86 (3) du règlement financier) pour 2011, qui résume l'activité d'audit interne en 2011 du CEPD.

Du suivi des six recommandations en suspens ouvertes des audits précédents, deux ont été clôturées par l'IAS (registre des exceptions et accords de travail - liste des accords de niveau de service - SLA), une a été clôturée en janvier 2013 (décision en matière de gestion des risques). Sur les 3 autres restantes, deux sont susceptibles d'être clôturées au cours de l'année 2013 (voir supra 4.6).

Les relations avec l'auditeur interne du CEPD ont été également soutenues par l'adoption de trois documents clés : un accord de niveau de service (SLA), une charte de mission de l'IAS et un protocole d'accord (Mémoire of Understanding). Voir supra point 4.3 coopération interinstitutionnelle.

4.7.3. SUIVI DE LA RESOLUTION DE DECHARGE DU PARLEMENT EUROPEEN

Dans la cadre de l'exercice de décharge budgétaire effectué par le Parlement européen, ce dernier a demandé au CEPD de mentionner dans le présent rapport le suivi accordé aux recommandations incluses dans la résolution de décharge.

Ces dernières recouvrent les 3 points suivants :

1. Est-ce que les manuels détaillés internes adoptés en 2011 et portant sur le recrutement de plusieurs catégories de personnel comprenaient la coopération avec EPSO ?

Oui, les manuels comprennent la coopération avec EPSO et mentionnent spécifiquement l'utilisation de listes de réserve des concours EPSO et CAST pour la sélection des candidats correspondant aux profils recherchés. Suite à la demande du CEPD, EPSO a organisé en 2009 trois concours pour des spécialistes en matière de protection des données et le CEPD a largement recrutés dans les listes de réserve correspondantes au cours des trois dernières années.

Les autres institutions européennes ont également bénéficié de l'organisation de ces concours, puisque certains d'entre eux ont ajouté leurs besoins de spécialistes en matière de protection des données lors la planification (et ont également fourni des membres des jurys). Ils ont demandé ultérieurement au CEPD de pouvoir recruter des lauréats sur les listes.

De la même manière, la recherche du CEPD en matière de personnel ne se limite pas aux concours de spécialistes : le CEPD peut également recruter sur les listes de réserve des concours organisés par EPSO à la demande d'une autre institution, mais ouvert à toutes les institutions. Les listes principalement utilisées sont celles pour les juristes et pour les profils dans les activités de soutien (administration, finances, ressources humaines, communication, informatique, secrétaires, etc.) Quand il s'agit de ces listes, l'aide d'EPSO dans la gestion des quotas est cruciale.

Mais la coopération avec EPSO va au-delà ce qui est mentionné dans les manuels limités aux phases de sélection et de recrutement. Le CEPD coopère avec EPSO dans d'autres domaines, tels que la planification des besoins futurs de l'organisation des concours EPSO. Cette coopération se déroule lors de deux groupements interinstitutionnels : le groupe de travail EPSO et le conseil d'administration d'EPSO : le CEPD est membre des deux puisque le premier prépare les travaux du second. En plus des discussions multilatérales, EPSO se réunit avec le CEPD une fois par an afin de discuter bilatéralement des besoins du CEPD.

**2. Pourquoi le CEPD a-t-il établi deux postes spécifiques
se rapportant au harcèlement sexuel?
Quelle a été la raison de créer une "personne de confiance" en 2011,
à la disposition de tout le personnel pour discuter
des cas possibles de harcèlement ?
Avez-vous enregistré une augmentation des cas de harcèlement ?
Comment sont-ils résolus ?**

Il n'y a eu aucun cas signalé de harcèlement dans la courte histoire du CEPD (neuf ans). Néanmoins, l'institution était consciente de l'importance de cette question (le harcèlement sous toutes ses formes et non uniquement le harcèlement sexuel) et c'est pour cette raison que le Comité du personnel et l'unité HRBA (Ressources Humaines, budget et administration) ont contacté les spécialistes de ces questions au sein de la Commission européenne. Deux personnes de confiance ont été désignées dans cette petite institution : un membre du comité du personnel et un membre de l'unité HRBA. Cela ne veut pas dire que nous avons deux postes spécifiques alloués à cette tâche, mais seulement que ces deux collègues sont à la disposition du personnel dans la mesure où ils souhaiteraient discuter de cette problématique et d'éventuels cas de harcèlement.

Même si aucun cas n'a été rapporté à ce jour, nous allons explorer en 2013 la signature éventuelle d'un accord de niveau de service (SLA) avec la Commission ainsi que la présentation d'une décision spécifique à l'examen du comité du personnel et le conseil d'administration de l'institution. L'objectif de cette décision serait de construire sur la prévention et la sensibilisation et d'établir des mesures de protection pour les deux parties dans une affaire de harcèlement potentiel : la présumée victime et l'auteur présumé.

**3. Pourriez-vous expliquer le but du logiciel
qui est développé pour le Contrôleur européen de la protection des données
que vous inscrivez à la rubrique des immobilisations incorporelles
(comptes annuels définitifs 2011 page 15 Point 2.2) ?**

a. Finalité du logiciel

Le CEPD a un pourcentage important de ses données stockées sous format électronique.

Actuellement, la gestion des cas au CEPD est fondée sur une structure de dossiers reposant sur un système de fichiers partagé, accessible par le logiciel Microsoft Office, incluant Excel, Word, Access et Microsoft Outlook. Les principaux documents auxquels le personnel du CEPD a besoin d'accéder, sont les suivants :

- une table des cas contenant des données pour chaque cas tels que le nom (s) des gestionnaires ainsi que des références aux dossiers sur le lecteur partagé ;
- un système de dossiers représentant des cas. Ces dossiers servent de référentiels pour les documents (documents internes) et les enregistrements (courrier entrant et sortant) ;
- divers fichiers de rapports - Feuilles généralement répartis et applications de base de donnée.

Les lacunes des outils actuels limitent l'efficacité de l'organisation, en particulier en ce qui concerne l'accès, la cohérence de stockage, les capacités de recherche, la sécurité, les pistes d'audit et l'archivage. Ils permettent un stockage de base, mais les flux de travail ne sont pas pris en charge.

Ces observations ont été confirmées par un audit interne qui a signalé ce qui suit :

Extrait du rapport des auditeurs internes (24/01/2008).

- "pas de base de données adéquate pour les dossiers"
 - risque : utilisation inefficace des ressources : un temps excessif peut être nécessaire afin d'obtenir des avis relatifs à un cas donné.
 - risque : manque d'harmonisation des opinions : possibilité de produire des opinions différentes pour des cas similaires.
 - risque: piste de vérification inadéquate et de rupture de continuité des opérations si le seul fichier dans le lecteur partagé est endommagé.
 - risque : risque juridique si les informations nécessaires ne sont pas facilement disponibles.
 - recommandation: Le CEPD devrait mettre en place un système de classement des cas qui permette des recherches par contenu.

- "sécurité insuffisante sur les fichiers archivés"
 - risque : le personnel et même des parties externes peuvent accéder aux cas enregistrés ainsi qu'à leur contenu.
 - risque : risque de moindre transparence et de traitement inégal du personnel.
 - recommandation : le CEPD devrait assurer le contrôle de l'intégrité et de la disponibilité de toutes les informations relatives à ses dossiers.

Afin de remédier aux problèmes observés, le CEPD a décidé de mettre en œuvre un système de gestion de dossiers plus sophistiqué (CMS) qui incorpore le document électronique et le système de gestion des dossiers (EDRMS). Ce système est capable de stocker des documents et des dossiers regroupés dans des dossiers pour toutes les activités du CEPD. Les dossiers sont classés selon un plan de classement. Le système inclut des fonctionnalités telles qu'un contrôle d'accès sophistiqué, l'inscription électronique, les calendriers de conservation, la capacité de mettre des blocages juridiques, la gestion des versions de documents, le marquage des objets, le texte intégral et la fonctionnalité de recherche de base de données, des pistes d'audit, des rapports et des workflows. Le résultat sera, entre autres, une meilleure sécurité, une meilleure productivité et une collaboration interne plus efficace.

b. Protection des informations sensibles

Aucune information classifiée de l'UE (EUCI) n'est produite ou stockée électroniquement par le CEPD et ne sera donc pas stockée dans le CMS.

D'un point de vue opérationnel, les informations sensibles peuvent être considérées comme toutes les informations qui justifient un traitement particulier dans le domaine de la sécurité, ce qui en soi inclut la confidentialité, l'intégrité et la disponibilité de ses composantes. La confidentialité doit être comprise comme la faculté d'empêcher la divulgation d'informations à des personnes non autorisées ou des systèmes. L'intégrité doit être comprise comme la faculté de s'assurer que ces données ne peuvent être modifiées sans détection. La disponibilité signifie que l'information doit être disponible en cas de besoin.

L'application offre une fonctionnalité complète qui permettra de gérer les droits d'accès des utilisateurs aux ressources du système. Le CEPD a mis au point un système complet de rôles et autorisations qui veillera à ce que cet accès ne soit accordé que sur la base du strict besoin d'en connaître. Ce système sera mis en œuvre par les membres du personnel spécialement formés qui exécuteront le rôle d'administrateur central.

En outre, l'application offre la possibilité de générer des traces d'audit pour chaque action dans le système. Les rapports d'audit seront générés par l'agent de sécurité de l'information, qui est un membre du personnel d'une autre unité. Toutes les exceptions trouvées devront être signalées à la hiérarchie.

Alors que le contrôle d'accès et des pistes d'audit sont des mesures garantissant notamment la confidentialité et l'intégrité du système et des données, ils contribuent également à la disponibilité des données et du système car ils empêchent toute intervention non autorisée avec l'exploitation du système.

D'autres mesures de sécurité techniques et organisationnelles garantissent des niveaux de sécurité appropriés à atteindre pour le fonctionnement du système. Celles-ci seront définies dans les instructions de fonctionnement pour le système. Lorsque le fonctionnement du système CEPD nécessite des services supplémentaires provenant de tiers, les obligations nécessaires seront fixées dans un accord astreignant approprié avec le fournisseur de service correspondant. Avant de conclure de tels accords avec un fournisseur de services, le CEPD effectue une évaluation des risques de l'organisation concernée. L'accord comprendra entre autres des garanties de disponibilité, exprimée en pourcentage de temps pendant lequel l'application doit être accessible; l'obligation de sauvegardes régulières du système, afin d'être protégé contre la perte involontaire d'informations, et la nécessité d'être prêt pour la reprise en cas de sinistre. Ceci fera l'objet d'un suivi régulier par le CEPD.

4.8. Suivi des réserves des exercices précédents

Le CEPD n'a émis aucune réserve particulière au terme des exercices précédents.

4.9. Conclusions sur l'efficacité du contrôle interne

En prenant en compte les informations décrites ci-dessus, l'ordonnateur délégué estime que le fonctionnement du système de contrôle interne est approprié vu l'importance des dépenses et du budget gérés par l'institution et donne ainsi l'assurance nécessaire à sa déclaration annuelle.

5. Réserves et impact sur la déclaration

5.1. Les critères de matérialité

Il est difficile pour le CEPD de prévoir une quelconque matérialité, même si l'impact de ses actions peut s'avérer extrêmement important pour l'institution, tant financièrement qu'en terme d'image.

5.1.1. OBJECTIFS DES CRITERES DE MATERIALITE

Le concept de matérialité donne à l'ordonnateur délégué une base pour déterminer les insuffisances significatives qui devraient nécessiter une réserve⁶ formelle à sa déclaration. L'appréciation de l'insuffisance relève du jugement tant qualitatif que quantitatif de l'ordonnateur délégué, qui reste responsable de la déclaration de l'assurance, y compris des réserves formulées.

Le but de ce chapitre, est de définir des critères qualitatifs et quantitatifs pour déterminer le niveau de matérialité.

5.1.2. CRITERES QUALITATIFS

Les paramètres suivants ont été utilisés pour déterminer les faiblesses significatives :

- Erreurs significatives/répétitives sans atténuation
- Faiblesse dans le système du contrôle interne
- Insuffisance de documents de support
- Problèmes matériels identifiés par la Cour des Comptes ou le Service d'Audit Interne
- Problème de réputation

⁶ La Commission (COM(2003)28 du 21 janvier 2003) estime que seulement des réserves 'matérielles' peuvent être utilisées pour qualifier la déclaration annuelle.

5.1.3. CRITERES QUANTITATIFS

Une fois qu'une faiblesse significative à été identifiée, des critères quantitatifs doivent être appliqués pour déterminer le niveau de matérialité. Ce niveau sera utilisé pour déterminer si la faiblesse "mérite" d'être rapportée.

- marge d'erreur
- montant maximum du risque

La Cour des comptes utilise un seuil de 2% de matérialité. Au cas où le risque résiduel d'une erreur est plus élevé, l'institution doit en expliquer les raisons.

En ce sens, le CEPD a retenu comme seuil de matérialité celui correspondant à 2% des crédits annuels, à savoir : 152.481,80 €.

5.1.4. CRITERES DU SERVICE D'AUDIT INTERNE

Dans le rapport des auditeurs internes "un tableau de signifiante" est ajouté.

Dans ce tableau, une distinction est faite entre recommandations et observations d'une part et d'autre part, des niveaux d'importance : critique, très important, important et souhaitable.

D'après les auditeurs internes, seules les observations du niveau "critique" peuvent aboutir à une réserve dans la déclaration figurant au rapport annuel d'activité. Pour le CEPD, il n'y a pas d'observations à ce niveau.

5.2. Réserves

Pas de réserve.

5.3. Conclusion

Sur la base de ce qui précède, le Directeur du Secrétariat du CEPD a établi, sans réserve, la déclaration annuelle.

6. Déclaration d'assurance de l'Ordonnateur Délégué

Je soussigné Christopher DOCKSEY,

Directeur du secrétariat du CEPD,

En ma qualité d'ordonnateur délégué

Déclare par la présente que les informations contenues dans le présent rapport sont sincères et véritables.

Affirme avoir une assurance raisonnable que les ressources allouées aux activités décrites dans le présent rapport ont été utilisées aux fins prévues et conformément au principe de bonne gestion financière et que les procédures de contrôle mises en place donnent les garanties nécessaires quant à la légalité et la régularité des opérations sous-jacentes.

Cette assurance raisonnable se fonde sur mon propre jugement et sur les éléments d'information à ma disposition, comme, par exemple, les résultats de l'auto-évaluation ainsi que le rapport du Service d'Audit Interne.

Confirme, en outre, n'avoir connaissance d'aucun fait non signalé pouvant nuire aux intérêts de l'institution.

Fait à Bruxelles, le 30 avril 2013.





Annexes

Annexe 1 :

résumé du rapport annuel d'activité

Le règlement financier (article 60 paragraphe 7⁷) prévoit que ***l'institution*** transmette au plus tard le 15 juin de chaque année à l'Autorité budgétaire (le Parlement européen et le Conseil) un résumé du rapport annuel d'activité de l'année précédente.

Parallèlement, l'article 48 du règlement 45/2001, prévoit que le CEPD présente au Parlement européen, au Conseil et à la Commission un rapport annuel sur ses activités.

Il est proposé de résumer le Rapport Annuel d'activité de l'ordonnateur délégué et d'insérer ce résumé dans le rapport d'activité comme prévu par l'article 48 du règlement 45/2001:

Globalement, le Contrôleur européen de la protection des données estime que les systèmes de contrôle interne qui sont en place apportent une assurance raisonnable quant à la légalité et à la régularité des opérations dont l'institution est responsable.

Le Contrôleur européen de la protection des données veillera à ce que son ordonnateur délégué poursuive ses efforts, afin de garantir que l'assurance raisonnable donnée dans la déclaration jointe à son rapport annuel d'activité est effectivement appuyée par des systèmes de contrôle interne appropriés

⁷ Le règlement financier, article 60 paragraphe 7: L'ordonnateur délégué rend compte à son institution de l'exercice de ses fonctions sous la forme d'un rapport annuel d'activité, accompagné des informations financières et de gestion. Ce rapport indique les résultats de ses opérations par rapport aux objectifs qui lui ont été assignés, les risques associés à ces opérations, l'utilisation des ressources mises à sa disposition et le fonctionnement du système de contrôle interne. L'auditeur interne prend connaissance du rapport annuel d'activité, ainsi que des autres éléments d'information identifiés.

Annexe 2 : budget 2012

TITLE 1 - EXPENDITURE RELATING TO PERSONS WORKING WITH THE INSTITUTION		2010	2011	2011 vs 2010 (%)	2012	2012 vs 2011 (%)
CHAPTER 10	MEMBERS OF THE INSTITUTION					
Article 100	Remuneration, allowances and other entitlements of Members					
	Item 1000 Remuneration and allowances	675.917,00	659.635,00	-2,41%	659.635,00	0,00%
	Item 1001 Entitlements on entering and leaving the service					
	Item 1002 Temporary allowances	127.000,00	130.357,00	2,64%	12.122,00	-90,70%
	Item 1003 Pensions					
	Item 1004 Provisional appropriation	16.451,00	16.885,00	2,64%	16.885,00	0,00%
	TOTAL Article 100	819.368,00	806.877,00	-1,52%	688.642,00	-14,65%
Article 101	Other expenditure in connection with Members					
	Item 1010 Further training	4.667,00	4.732,00	1,39%	4.732,00	0,00%
	Item 1011 Mission expenses, travel expenses and other ancillary expenditure	82.929,00	84.090,00	1,40%	59.394,00	-29,37%
	TOTAL Article 101	87.596,00	88.822,00	1,40%	64.126,00	-27,80%
	TOTAL CHAPTER 10	906.964,00	895.699,00	-1,24%	752.768,00	-15,96%
CHAPTER 11	STAFF OF THE INSTITUTION					
Article 110	Remuneration, allowances and other entitlements of officials and temporary staff					
	Item 1100 Remuneration and allowances	3.246.037,00	3.705.939,00	14,17%	3.755.970,00	1,35%
	Item 1101 Entitlements on entering, leaving the service and on transfer	198.924,00	204.613,00	2,86%	70.564,00	-65,51%
	Item 1102 Overtime					
	Item 1103 Special assistance grants	5.000,00	5.070,00	1,40%	5.070,00	0,00%
	Item 1104 Allowances and miscellaneous contributions in connection with early termination of service					
	Item 1105 Provisional appropriation	85.746,00	88.198,00	2,86%	88.198,00	0,00%
	TOTAL Article 110	3.535.707,00	4.003.820,00	13,24%	3.919.802,00	-2,10%
Article 111	Other staff					
	Item 1110 Contract staff	50.719,00	50.856,00	0,27%	147.186,00	189,42%
	Item 1111 Cost of traineeships and staff exchanges	164.064,00	165.212,00	0,70%	179.428,00	8,60%
	Item 1112 Services and work to be contracted out	38.110,00	44.096,00	15,71%	51.202,00	16,11%
	TOTAL Article 111	252.893,00	260.164,00	2,88%	377.816,00	45,22%
Article 112	Other expenditure in connection with staff					
	Item 1120 Mission expenses, travel expenses and other ancillary expenditure	105.628,00	103.346,00	-2,16%	112.686,00	9,04%
	Item 1121 Recruitment costs	9.895,00	10.034,00	1,40%	6.789,00	-32,34%
	Item 1122 Further training	71.498,00	72.499,00	1,40%	84.874,00	17,07%
	Item 1123 Social service					
	Item 1124 Medical service	14.639,00	14.844,00	1,40%	14.844,00	0,00%
	Item 1125 Union nursery centre and other day nurseries and after-school centres	121.639,00	117.356,00	-3,52%	87.938,00	-25,07%
	Item 1126 Relations between staff and other welfare expenditure	3.570,00	3.620,00	1,40%	3.865,00	6,77%
	TOTAL Article 112	326.869,00	321.699,00	-1,58%	310.996,00	-3,33%
	TOTAL CHAPTER 11	4.115.469,00	4.585.683,00	11,43%	4.608.614,00	0,50%
	TOTAL TITLE 1	5.022.433,00	5.481.382,00	9,14%	5.361.382,00	-2,19%

TITLE 2 - BUILDINGS, EQUIPMENT AND EXPENDITURE IN CONNECTION WITH THE OPERATION OF THE INSTITUTION		2010	2011	2011 vs 2010 (%)	2012	2012 vs 2011 (%)
CHAPTER 20	BUILDINGS, EQUIPMENT AND EXPENDITURE IN CONNECTION WITH THE OPERATION OF THE INSTITUTION					
Article 200	Rents, charges and buildings expenditure	578.340,00	586.437,00	1,40%	728.067,00	24,15%
TOTAL Article 200		578.340,00	586.437,00	1,40%	728.067,00	24,15%
Article 201	Expenditure in connection with the operation and activities of the institution					
	Item 2010 Equipment	89.789,00	101.046,00	12,54%	155.497,00	53,89%
	Item 2011 Supplies	19.254,00	19.524,00	1,40%	19.524,00	0,00%
	Item 2012 Other operating expenditure	40.054,00	40.615,00	1,40%	98.368,00	142,20%
	Item 2013 Translation and interpretation costs	1.039.330,00	1.053.881,00	1,40%	980.000,00	-7,01%
	Item 2014 Expenditure on publishing and information	164.024,00	166.320,00	1,40%	166.320,00	0,00%
	Item 2015 Expenditure in connection with the activities of the institution	151.127,00	114.932,00	-23,95%	114.932,00	0,00%
TOTAL Article 201		1.503.578,00	1.496.318,00	-0,48%	1.534.641,00	2,56%
TOTAL CHAPTER 20		2.081.918,00	2.082.755,00	0,04%	2.262.708,00	8,64%
TOTAL TITLE 2		2.081.918,00	2.082.755,00	0,04%	2.262.708,00	8,64%
TOTAL BUDGET		7.104.351,00	7.564.137,00	6,47%	7.624.090,00	0,79%

Annexe 3 : Tableau final de gestion des risques

Risk title & description (cause and effect)	Policy area & Activity / objective affected	Gross risk score			Controls	Person responsible & supervisor	Net (residual) risk score			Risk response	Monitoring		Control effectiveness	Further action		
		Likelihood	Impact	Overall score (L x I)			Likelihood	Impact	Overall score (L x I)		Frequency	Monitor		Action	Owner	Deadline
Ineffective implementation of training policy	HRBA Action point affected: Ensure good management of human resources	Likelihood	4	3	Development of a new policy Follow up +++ new training impetus more time to the COFO		Likelihood	3	3	Accept	Frequency	Monitor	Good = 1 Ok but so/so = 2 Pretty dreadful = 3	Review the training policy	AFR	11/2013
		Impact	3	3			9									
Failure to capture external request in system	OPS Objective affected: to implement best practice in records management incorporating principles of data protection and transparency (access to documents)	Likelihood	5	5	4 eyes system of checking EDPS box Mechanical SPAM filter re-checked		Likelihood	2	5	Accept	Frequency	Monitor		4 eyes system of checking EDPS box Mechanical SPAM filter re-checked	AB / MC MK	Done Done
		Impact	5	5			10									
Service provider does not provide services as agreed or do not respond on time (or not at all) to demands.	IT POLICY Action point 5 Improve the use of the EDPS human, financial, technical and organisational resources	Likelihood	4	3	Establish clear agreement with the service provider and proper monitoring at the EDPS		Likelihood	3	3	Accept	Frequency	Monitor		Establish clear agreement with the service provider and proper monitoring at the EDPS	AK	End of July
		Impact	4	3			9									

Risk title & description (cause and effect)	Policy area & Activity / objective affected	Gross risk score			Person responsible & supervisor	Net (residual) risk score			Risk response	Monitoring		Control effectiveness	Further action		
		Likelihood	Impact	Overall score (L x I)		Likelihood	Impact	Overall score (L x I)		Frequency	Monitor		Action	Owner	Deadline
Ineffective cooperation with DPAs	POLICY Action point 2 Cooperation with WP29, the institutions and other Stakeholders 2.b cooperation with WP 29	3	5	15		2	4	8	Accept	Frequency	Monitor	Good = 1 Ok but so/so = 2 Pretty dreadful = 3	Action	Owner	Deadline
Ineffective cooperation with EU institutions	POLICY Action point 2 Cooperation with WP29, the institutions and other Stakeholders 2.b cooperation with Commission, Council & EP	3	5	15		2	4	8	Accept	Frequency	Monitor		Id controls	AB	In the course of the year

Risk title & description (cause and effect)	Policy area & Activity / objective affected	Gross risk score			Controls	Person responsible & supervisor	Net (residual) risk score			Risk response	Monitoring		Control effectiveness	Further action		
		Likelihood	Impact	Overall score (L x I)			Likelihood	Impact	Overall score (L x I)		Frequency	Monitor		Action	Owner	Deadline
Lack of accountability	Supervision Action point affected: Increase enforcement	Likelihood	4		Establishing mechanisms (visits) Clear set of steps (escalation) Use of our enforcement powers		Likelihood	3	3	Accept	Frequency		Good = 1 Ok but so/so = 2 Pretty dreadful = 3	Visits to EU agencies Clear set of steps (escalation) Use of our enforcement powers	PH/GB Super-visors	Next year
		Impact	5	20			Overall score (L x I)	9	Monitor							
Lack of supervision visibility	Supervision General aspect	Likelihood	4		Presence in key meetings of the institutions (Heads of agencies, DGs...) Reference to S&E work in presentations (e.g experience relating to supervision when speaking of new regulation) Increase communic° tools: press releases - twitter. Communication team to think about tools improving our visibility Inspections - visits		Likelihood	3	4	Accept				Attendance of key meetings Reference to S&E work in presentations (e.g experience relating to supervision when speaking of new regulation) Communication team	MB MB + staff	All year In process
		Impact	4	16			Overall score (L x I)	12								