



**Évaluation du respect du règlement (CE) n° 45/2001
au sein des institutions et organes de l'UE («Enquête 2011»)**

Rapport général

Bruxelles, le 23 janvier 2012

Sommaire

Résumé

1. Introduction

2. Méthodologie

3. Résultats comparatifs de l'enquête

4. Suivi de l'enquête précédente: visites de contrôle

5. Fixation de valeurs de référence

6. Conclusions

Annexe (1) Groupes d'institutions et d'organes

Annexe (2) Limites de la méthodologie

Annexe (3) Liste des sigles des institutions

Annexe (4) Tableau comparatif des résultats

Résumé

Comme les administrations publiques, les institutions et organes de l'UE traitent des données à caractère personnel aussi bien dans leurs tâches administratives quotidiennes que dans le cadre de leurs activités fondamentales. Dans un cas comme dans l'autre, ils doivent respecter les principes et les obligations énoncés dans le règlement pertinent en matière de protection des données¹. Le Contrôleur européen de la protection des données (CEPD) contrôle et garantit le respect de ce règlement².

Dans ce contexte, le CEPD a effectué un **état général de la situation** en se concentrant sur les aspects qui donnent une bonne indication des progrès réalisés au regard de la mise en œuvre du règlement dans l'ensemble des **58 institutions et organes**. Un rapport général a été rédigé sur la base des réponses que les institutions et les organes ont apportées aux lettres du CEPD en date du 30 septembre 2011.

Ces réponses ont été présentées dans des tableaux comparatifs, par groupe³ d'institutions et d'organes. Des **valeurs de référence** ont été établies sur la base des résultats obtenus dans chaque groupe. Ces valeurs n'ont donc pas été définies de manière abstraite par le CEPD, mais résultent des niveaux de performance atteints par les institutions et les agences. Elles permettent une **comparaison entre pairs** et donnent une indication du niveau qu'une institution ou organe du groupe concerné doit normalement atteindre.

Le présent rapport sera publié dans le cadre de la politique du CEPD relative à l'application des règles⁴. Il souligne les progrès réalisés par les institutions et les organes, tout en relevant leurs manquements. Il vise à les responsabiliser davantage au respect des règles relatives à la protection des données.

Le CEPD tiendra compte des résultats de cette enquête au moment de planifier de nouvelles activités de supervision et d'application des règles. Ce programme associera du **conseil** donné aux institutions et aux organes, des **actions de mise en application des règles** et d'autres initiatives promouvant la **responsabilisation des acteurs**. Plus particulièrement, des visites de contrôle déclenchées par un manque manifeste d'engagement de la part d'une institution ou organe ont été planifiées sur la base des résultats de l'enquête 2011.

Les réponses reçues et les visites de contrôle précédentes réalisées par le CEPD ont révélé que la mise en œuvre du règlement n'est pas seulement une question de temps ou de ressources, mais aussi de **volonté de**

¹ Règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes de la Communauté et la libre circulation de ces données.

² Conformément à l'article 41, paragraphe 2, du règlement.

³ Voir l'annexe 1 du rapport.

⁴ Voir le document d'orientation du CEPD du 13 décembre 2010 intitulé «Contrôler et garantir le respect du règlement (CE) n° 45/2001», p. 8.

l'organisation. Le rapport ne vise pas à évaluer les performances du délégué à la protection des données, mais celles des institutions et organes chargés de la protection du droit à la vie privée des individus pour ce qui touche au traitement de données à caractère personnel. Le respect de la réglementation est en effet un processus qui nécessite l'**engagement** et le **soutien** de la hiérarchie dans toutes les institutions et organes.

1. Introduction

En tant qu'administrations publiques, les institutions et organes de l'UE traitent des données à caractère personnel aussi bien dans leurs tâches administratives quotidiennes que dans le cadre de leurs activités fondamentales.

Il incombe aux institutions et organes de protéger les libertés et les droits fondamentaux des personnes physiques pour ce qui est du traitement des données à caractère personnel et de mettre en place des mesures appropriées et effectives afin de garantir le respect des principes et des obligations énoncés dans le règlement (CE) n° 45/2001 (ci-après, le «règlement»), et d'en apporter la preuve.

C'est le devoir et la tâche du Contrôleur européen de la protection des données de contrôler et de garantir que les droits des individus sont respectés conformément au règlement⁵.

Dans son document d'orientation adopté en décembre 2010⁶, le CEPD annonce qu'il «continuera de mener ces “enquêtes” périodiques afin de garantir qu'il dispose d'un aperçu représentatif du respect de la protection des données au sein des institutions et organes de l'Union, et qu'il peut fixer des objectifs internes appropriés pour traiter ses constatations».

En avril 2011, le CEPD s'est attelé à son troisième état de la situation. Cet exercice s'inscrit dans la continuation des exercices de 2007 et de 2009.

L'exercice a une large portée, puisqu'il couvre toutes les institutions et organes pertinents, et s'est focalisé sur les aspects donnant une bonne indication des progrès réalisés dans la mise en œuvre du règlement.

Le CEPD tiendra compte des résultats de cet exercice – y compris les valeurs de référence pour les différentes catégories d'institutions et d'organes – au moment de planifier les activités de supervision et d'application des règles. Comme indiqué dans le document d'orientation, après plusieurs années d'activités de contrôle, il est temps de signaler un changement d'approche⁷.

Le présent rapport général est basé sur les réponses que six institutions de l'UE et 52 organes (notamment ceux des deuxième et troisième piliers) ont apportées, en juin et en septembre 2011, aux lettres du CEPD soulevant des questions spécifiques. Le contenu des lettres du CEPD était légèrement différent selon le statut des institutions et des organes – récents ou moins récents, avec ou sans délégué à la protection des données (DPD) nommé. Le CEPD a reçu des réponses de toutes les institutions et organes concernés,

⁵ Conformément à l'article 41, paragraphe 2, du règlement.

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

⁷ Ibid, par. 3.1.

sauf de l'ECDC et de l'IESUE⁸. Le CEPD abordera cette question de manière spécifique.

⁸ Voir la liste des sigles des institutions à l'annexe 3.

2. Méthodologie

Les questions soulevées dans les lettres adressées aux institutions et aux organes étaient principalement orientées sur les aspects suivants de la mise en œuvre du règlement:

- l'existence d'un inventaire des traitements et la notification de ceux-ci au DPD conformément à l'article 25;
- la notification des traitements soumis à un contrôle préalable en vertu de l'article 27;
- le suivi réservé aux avis du CEPD dans les cas de contrôle préalable;
- l'adoption de dispositions d'application conformément à l'article 24, paragraphe 8;
- la désignation et le rôle du DPD.

Les réponses ont été évaluées et sont présentées dans un tableau comparatif (voir l'annexe 4). Les institutions et organes ont été répartis en quatre groupes selon l'année de leur établissement afin de permettre une comparaison valable. L'année de création du CEPD – 2004 – constitue un premier critère de répartition. La date de désignation d'un DPD a été retenue comme deuxième critère (voir l'annexe 1). Le CEPD a chiffré certaines données afin d'affiner son évaluation des résultats comparatifs et d'établir des valeurs de référence. Toutefois, comme le rapport le montrera, certains paramètres ne peuvent être aisément traduits en chiffres; par conséquent, l'exercice ne peut être mathématique à cent pour cent (voir les limites de la méthodologie à l'annexe 2). Quoi qu'il en soit, les facteurs ne sont jamais considérés isolément: ils forment une image globale qui sera évaluée minutieusement avant de déboucher sur de nouvelles initiatives éventuelles.

Le présent rapport sera publié dans le cadre de la politique du CEPD relative à l'application des règles. Il souligne les progrès réalisés par les institutions et les organes, tout en relevant leurs manquements sur le plan du respect de la réglementation. Ces signaux permettront tant au CEPD qu'aux institutions et organes européens eux-mêmes de cibler leurs actions de manière à mieux respecter leurs obligations dans le domaine de la protection des données.

Les valeurs de référence mentionnées dans le présent rapport seront particulièrement utiles pour orienter les progrès futurs afin de garantir le respect du règlement si nécessaire. Ce processus nécessitera une attention suffisante et permanente.

La seconde partie du rapport porte plus particulièrement sur les organes ayant reçu la visite du CEPD en 2010 ou au premier semestre 2011. Les résultats obtenus en matière de respect de la réglementation avant et après les visites ont été comparés afin d'analyser leur impact.

Le CEPD tiendra compte des conclusions du présent rapport lorsqu'il établira son programme de supervision et d'application des règles pour 2012. Ce

programme contiendra tout à la fois des orientations données aux institutions et organes, des actions de mise en application des règles et d'autres initiatives promouvant la responsabilisation des acteurs.

3. Résultats comparatifs de l'enquête

a) Inventaire et notifications au DPD

Le CEPD a demandé une mise à jour de l'inventaire de tous les traitements identifiés impliquant des données à caractère personnel, y compris le nombre de ces traitements déjà notifiés au DPD conformément à l'article 25 et consignés dans le registre (notifications au titre de l'article 25).

Ce troisième état de la situation montre, parallèlement aux exercices précédents, qu'un **inventaire des traitements** est un élément crucial pour assurer le respect du règlement. Cet instrument utile donne aux DPD et à leur hiérarchie une vue d'ensemble des traitements de l'organisation et facilite l'identification des risques. Pour fonctionner efficacement comme instrument de mesure, l'inventaire doit comprendre au moins les champs suivants: intitulé du traitement, brève description de celui-ci s'il n'est pas assez explicite, statut des notifications au titre des articles 25 et 27 et personne de contact responsable de la gestion interne du traitement. Le CEPD a constaté qu'un inventaire bien tenu s'accompagne en général d'un bon niveau de respect de la réglementation. Le CEPD rassemblera prochainement dans un modèle d'inventaire les traitements communs aux organes de l'UE afin de faciliter la mise en place de cet instrument dans les nouveaux organes⁹.

Les institutions et organes du **groupe A** ont tous atteint un niveau élevé de notifications au titre de l'article 25. Le Comité des régions a notamment réalisé une avancée impressionnante à cet égard, puisque près de 100 % des traitements ont été notifiés au DPD. Pour les organes présentant un taux de conformité élevé (environ 95 % de l'inventaire), le défi est passé de la notification des traitements à l'actualisation de l'inventaire. La Commission européenne et le Parlement européen ont évoqué ce nouveau défi. D'autres institutions ou organes tels que le Conseil, la BEI, le Médiateur européen, le CdT ainsi que des organes du groupe B tels que l'OHMI pourraient être confrontés à un défi similaire au cours des prochains mois. Il est en effet nécessaire de tenir à jour l'inventaire pour maintenir et renforcer le niveau de respect de la réglementation.

La majorité des institutions et organes du groupe A ont atteint un score d'environ 95 % de notifications au titre de l'article 25. La valeur de référence établie pour ce groupe se situe autour de ce niveau. Au-dessous de 85 %, les institutions et organes font moins bien que leurs pairs.

⁹ Cela aidera également les organes présentant un (faible) niveau de procédures identifiées impliquant le traitement de données à caractère personnel qui ne correspond pas à la réalité de leurs activités (REA, EACI). D'autres organes peuvent l'utiliser pour identifier les notifications au titre de l'article 27 (Artemis).

Dans le **groupe B**, certains organes ont également un taux très élevé de notifications au titre de l'article 25: OHMI, EU-OSHA, EMA, EMSA, AEE et Eurofound. Toutefois, même par comparaison avec l'OEDT (71 %), l'EACI (73 %) ou l'OCVV (70 %), certains organes bien établis comme l'ETF (33 %) et l'AESA (22 %) présentaient toujours un faible niveau de notifications. Le Cedefop a désormais atteint un taux de 62 % de notifications au titre de l'article 25.

Il a également été constaté que certains organes se concentrent encore exclusivement sur les notifications au titre de l'article 27. Ainsi, l'ETF, qui a un bon niveau de notifications au titre de l'article 27 (75 %), a un faible taux de notifications au titre de l'article 25. La Fondation n'a progressé que de 3 % entre l'enquête de 2009 et l'enquête actuelle. L'AESA présente elle aussi un très faible niveau de notifications au titre de l'article 25, mais elle a bien progressé en ce qui concerne les traitements visés à l'article 27 et notifiés à la suite des lignes directrices du CEPD.

Le niveau de procédures identifiées de l'EACI impliquant le traitement de données à caractère personnel est plus faible que celui d'organes comparables (19 contre 30-39).

La moitié du groupe B a désormais atteint au moins 70 % de notifications exigées par l'article 25. Un quart se situe entre 55 et 70 %. Un niveau inférieur à 55 % dénote par conséquent un faible niveau de respect de la réglementation.

Quatre organes du **groupe C** ont envoyé une copie de leur *registre* au lieu de leur *inventaire* (Entreprises communes Artemis, Clean Sky, PCH et IMI). Le niveau de notifications au titre de l'article 25 est dès lors difficile à mesurer. Cela dit, de nombreuses procédures semblent avoir été identifiées et notifiées au titre de l'article 25, ce qui constitue un bon début qu'il convient d'encourager.

Dans ce groupe, l'ECHA a atteint près de 60 % de notifications au titre de l'article 25, tandis que la REA, le SESAR, F4E, la GSA, l'AFE et l'ERCEA conservent un niveau très faible de notifications, à savoir entre 0 et 20 %¹⁰. La REA n'a identifié que sept procédures impliquant le traitement de données à caractère personnel (7 contre 30 dans des agences comparables). L'Agence TEN-TEA, l'ACCP, l'EAHC et l'EACEA se situent aux environs de 45 % de notifications.

L'inventaire de l'ECHA est organisé par unité. En outre, il contient les niveaux de notifications prévues aux articles 25 et 27 exprimés en pourcentages et par unité. Par conséquent, chaque chef d'unité chargé en interne de gérer les traitements est responsabilisé à la protection des données. Le CEPD salue

¹⁰ Le faible niveau de notifications au titre de l'article 25 peut également s'expliquer par le fait que toutes les procédures n'ont pas été adoptées par les organes et que, dès lors, même si les traitements sont identifiés, ils n'ont pas encore lieu et la notification de la procédure au DPD n'est pas encore possible.

cette approche qui permet de faire des comparaisons et qui renforce donc la responsabilisation.

Certains inventaires des organes du groupe C sont trompeurs et pourraient être améliorés: l'agence Frontex a sans doute confondu le registre et l'inventaire des traitements. Cette approche ne donne pas une image claire du niveau de notifications au titre des articles 25 et 27. L'Agence semble néanmoins présenter un bon niveau de notifications.

Dans le groupe C, la valeur de référence est plus difficile à déterminer parce que quatre ou cinq des 17 organes ont envoyé leur registre au lieu de leur inventaire. Parmi les organes du Group C, ce compris ceux ayant communiqué leur registre, le groupe le plus avancé affiche un taux de 40 à 60 % de notifications au titre de l'article 25.

Dans le **groupe D**, trois organes ont déjà soumis un inventaire. Trois autres se sont engagés à le faire d'ici la fin septembre 2011, bien qu'aucun inventaire ne soit parvenu au CEPD à cette date.

Parmi les organes des deuxième et troisième piliers, le CEPOL a soumis un inventaire pour consultation. L'AED et le CSUE ont indiqué que leur inventaire était en cours d'élaboration.

b) Notifications de traitements soumis à un contrôle préalable

Le CEPD a demandé des informations sur le statut des traitements soumis à son contrôle préalable (article 27). Afin de faciliter la notification de ces procédures comprenant des traitements à risque effectués par des organes de l'UE, le CEPD a publié des lignes directrices sur les procédures administratives communes à toutes les institutions et organes de l'UE (recrutement, données relatives à la santé, etc.).

Pour mesurer le niveau de respect de la réglementation des **notifications au titre de l'article 27**, le CEPD a comparé les notifications dans les domaines dans lesquels il a publié des lignes directrices. Il y a lieu de différencier les différentes procédures faisant l'objet de lignes directrices du CEPD: en effet, si certains traitements sont en place depuis l'existence d'un organe donné (recrutement du personnel), d'autres peuvent ne pas encore avoir été établis (par exemple, les enquêtes administratives). En évaluant le respect de l'article 27, nous avons tenu compte de cette situation, de même que de l'ancienneté de l'organe concerné. Il convient de noter que le respect des lignes directrices en matière de vidéosurveillance sera analysé dans un rapport distinct sur un exercice de contrôle spécifique en cours actuellement.

Les pourcentages de notifications au CEPD au titre de l'article 27 qui ont été identifiées (et qui font ou non l'objet de lignes directrices du CEPD) sont également considérés comme un indicateur du niveau de respect de la réglementation.

Dans leur inventaire, certains organes n'ont pas identifié correctement les procédures qui impliquent des traitements relevant de l'article 27. Artemis a plusieurs procédures qui doivent être considérées comme soumises à un contrôle préalable (promotions, marchés publics, sélection d'experts, etc.) et qui n'ont pas été identifiées en tant que telles.

Le groupe A a atteint un bon niveau de respect de l'article 27: la majorité des institutions et organes ont notifié leurs procédures couvertes par des lignes directrices du CEPD. Le CdT doit encore notifier certaines procédures dans le domaine disciplinaire, de même que la Cour des comptes dans le domaine des données relatives à la santé.

Dans le groupe B, l'OHMI n'a pas encore notifié les traitements «de base» tels que le recrutement, le traitement de données relatives à la santé et les procédures disciplinaires. Dans ce groupe, la majorité des procédures en place couvertes par des lignes directrices du CEPD ont été notifiées à ce dernier.

Dans le groupe C, la majorité des organes ont notifié des traitements ayant trait aux données relatives à la santé et aux procédures de recrutement. Dans ce groupe, l'indicateur d'un faible niveau du respect de la réglementation correspond par conséquent au fait que ces deux procédures n'ont pas été notifiées au CEPD.

c) Suivi des avis du CEPD

Le CEPD a demandé une copie des éventuelles procédures de suivi visant à garantir la mise en œuvre des recommandations qu'il a formulées à l'occasion des avis de contrôle préalable.

La réponse à la question concernant les éventuelles procédures mises en place pour garantir le **suivi des recommandations du CEPD** se limite en général à des informations sur les rappels que le DPD adresse à la personne chargée de gérer le traitement. Certains institutions ou organes ont adopté des rappels automatisés ou conservent la trace des réponses au moyen de tableaux spécifiques. Certaines (EFSA, AFE, FRA) élaborent actuellement une telle procédure de rappel. La FRA a suggéré d'inclure un article en ce sens dans ses dispositions d'application (DA) pour «formaliser» la procédure de suivi. D'autres organes possèdent déjà un article spécifique dans leurs DA pour régler la question du suivi. D'autres encore ont suggéré d'ajouter une colonne à leur inventaire.

Dans tous les cas, les institutions et organes ont déclaré qu'il appartenait au DPD de rappeler au responsable du traitement ou à la personne chargée de gérer le traitement l'obligation qui leur incombe. Le DPD est aujourd'hui considéré comme l'interlocuteur privilégié dans le cadre de la mise en œuvre des recommandations du CEPD. Il semble également qu'aucune institution ou organe n'ait jugé nécessaire d'instaurer des mesures spécifiques pour imposer à un responsable «réticent» de prendre des mesures appropriées

pour mettre en œuvre les recommandations du CEPD. En outre, les cadres supérieurs ne sont pas officiellement avertis d'une absence de réponse au CEPD.

Le CEPD estime que des mécanismes de responsabilisation des institutions et organes doivent être développés, notamment en ce qui concerne la mise en œuvre de ses recommandations. Le DPD ne doit pas être considéré comme la personne chargée de la mise en œuvre des recommandations. À cet égard, le CEPD a l'intention de développer sa pratique dans le sens d'une communication directe avec la personne chargée du traitement¹¹. Dans un proche avenir, le CEPD adressera directement à la hiérarchie – au besoin, au plus haut niveau – les questions de suivi qui restent en souffrance depuis longtemps. Ce changement dans la communication devrait favoriser encore plus la culture de la protection des données au sein des institutions et des organes.

En l'absence de différences significatives entre institutions et organes, la procédure de suivi n'a pas été prise en compte dans l'analyse comparative. Cette question s'est cependant avérée utile pour améliorer la communication du CEPD en ce qui concerne le suivi des avis rendus dans le cadre d'un contrôle préalable.

d) Adoption de dispositions d'application («DA»)

Le CEPD a demandé aux institutions et organes une copie de leurs dispositions d'application (DA) sur les tâches, fonctions et compétences du DPD conformément à l'article 24, paragraphe 8, du règlement.

La plupart des institutions et organes ont **adopté des DA** ou consulté le CEPD sur leur projet de décision. Il s'agit là d'un domaine dans lequel des progrès très significatifs ont été réalisés. Il est désormais de pratique courante, pour les organes européens récemment créés (SEAE, AEMF) de commencer l'application du règlement (CE) n° 45/2001 en consultant le CEPD, en vertu de l'article 28, paragraphe 1, sur l'adoption de DA. Dans certains organismes, celle-ci constitue une condition préalable à la désignation du DPD (SEAE).

Un petit nombre d'organes ont négligé de consulter le CEPD (Artemis, Clean Sky, IMI) avant d'adopter leurs DA.

L'ensemble des institutions et organes des groupes A et B ont désormais adopté leurs DA. Dans le groupe C, F4E et la REA doivent encore consulter le CEPD avant d'adopter leur décision, conformément à l'article 24, paragraphe 8.

Dans le groupe D, les résultats sont encourageants: 7 organes sur 12 ont adopté (ou soumis pour consultation) leur décision sur les DA.

¹¹ Pour garantir la continuité et la cohérence des opérations, le DPD sera toujours mis en copie.

Les DA visés à l'article 24, paragraphe 8, du règlement sont en général adoptées ou soumises pour consultation au CEPD au cours de l'année d'établissement d'un nouvel organe de l'UE ou au plus tard l'année qui suit. Si les DA ne sont pas adoptées au cours de l'année suivant l'établissement de l'organe, cela peut être considéré comme un mauvais signal par le CEPD.

e) Désignation et rôle du DPD

Le CEPD a demandé à être informé de la désignation d'un DPD dans les nouveaux organes (groupe D) et rappelé à toutes les institutions et organes l'existence de l'article sur les normes professionnelles pour les DPD (groupe A, B et C).

Les nouveaux organes ont été invités à **désigner un DPD** conformément à l'article 24, paragraphe 1, du règlement. Dans le groupe D, parmi les nouveaux organes (huit) et ceux des deuxième et troisième piliers (quatre), huit ont désigné un DPD, trois sont sur le point de le faire, tandis qu'un organe n'a pas encore répondu à la lettre du CEPD (IESUE).

Le DPD joue un rôle crucial dans le respect du règlement, comme le prouve clairement l'ECDC, qui n'a pas remplacé son DPD depuis mars 2011: le mécanisme de contrôle du respect de la réglementation est bloqué depuis lors et le CEPD n'a jusqu'à présent reçu aucune réponse à l'enquête. Cette situation appellera de nouvelles mesures d'application de la réglementation à très court terme.

Le document établi par réseau des DPDs sur les normes professionnelles pour les DPD¹² a été porté à la connaissance des chefs d'institution ou d'organe pour la deuxième fois. Il s'agit là d'un excellent document de référence qui vise à les aider à définir les normes nécessaires pour garantir l'indépendance des DPD et à définir les meilleures pratiques en relation avec les fonctions de ces derniers.

Le Conseil a indiqué qu'il avait dûment tenu compte du document dans la procédure de sélection en vue de la désignation de son nouveau DPD. Le CdT a également indiqué que le document lui avait été utile pour sélectionner le DPD. Le CEPD salue le fait que les institutions et organes font bon usage de cet outil de référence..

Le CEPD tient à souligner les progrès notables effectués, sur le plan du respect de la réglementation, par les institutions et organes de l'UE du groupe A, qui avaient désigné un DPD avant même l'établissement du CEPD, ce qui prouve clairement l'importance du rôle du DPD.

¹² Ainsi que le document de référence du CEPD sur le «*Rôle joué par les délégués à la protection des données pour garantir le respect effectif du règlement (CE) n° 45/2001*», 28 novembre 2005.

4. Suivi de l'enquête précédente: visites de contrôle

À la suite de l'enquête précédente – hormis le suivi général et certains cas spécifiques –, le CEPD a rendu visite à six organes épinglés lors de l'exercice de 2009. Ces visites ont été déclenchées par un manque manifeste d'engagement de la part de ces organes ainsi que par d'autres éléments de preuves recueillis lors de l'exercice précédent.

À l'époque, une inspection en tant que telle n'était pas envisagée pour ces organes parce que le niveau de respect du règlement (CE) n° 45/2001 était extrêmement faible. Il était impossible de «contrôler la réalité» de traitements qui n'avaient pas encore été notifiés ou d'outils de contrôle du respect de la réglementation (inventaire, registre) qui n'existaient pas.

Pour améliorer le respect de la réglementation, le CEPD a profité de ces visites pour établir des feuilles de route précises en accord avec la hiérarchie des organes concernés. Ces feuilles de route comprennent des objectifs et des délais spécifiques: établissement d'un inventaire, progrès à accomplir quant au niveau de notifications au titre des articles 25 et 27, notification de procédures ciblées pour lesquelles le CEPD a publié des lignes directrices et autres questions propres à l'organe visité (pérenniser la fonction de DPD, former le personnel à la protection des données, etc.).

Deux visites ont eu lieu en 2010 et quatre en 2011¹³. Une comparaison du niveau du respect de la réglementation entre l'enquête de 2009 et les résultats actuels a été effectuée pour souligner les effets de ces visites.

En général, des efforts satisfaisants ont été déployés dans tous les cas. Les organes qui avaient un taux de notifications au titre de l'article 25 proche de zéro atteignent maintenant des niveaux de 60, 70 et 80 %, et même de 100 % pour l'un d'entre eux. Chaque organe s'est désormais doté d'un inventaire intelligible et de bonne qualité.

Un rapport de clôture est envoyé à l'organe à l'expiration des délais convenus. Si les objectifs ne sont pas atteints, et en l'absence de progrès notables, le CEPD envisagera de nouvelles mesures afin de garantir le respect du règlement (CE) n° 45/2001¹⁴.

¹³ La quatrième a eu lieu en septembre 2011 et n'a pas été prise en compte dans le présent rapport.

¹⁴ Voir la partie 3 du document d'orientation du CEPD intitulé «Contrôler et garantir le respect du règlement (CE) n° 45/2001».

5. Fixation de valeurs de référence

Cette troisième analyse au cas par cas dans l'exercice de 2011 a permis au CEPD de définir des valeurs de référence au regard du respect du règlement. Les valeurs de référence sont établies par groupe d'institutions et organes comparables et indiquent le seuil qu'une institution ou un organe du groupe concerné doit normalement atteindre dans tous les cas. Ces valeurs de référence n'ont pas été fixées par le CEPD de manière abstraite, mais sont déduites des résultats atteints dans chaque groupe.

Les valeurs de référence concernant les procédures qui présentent des risques spécifiques au sens de l'article 27 sont établies sans préjudice du fait que les traitements liés aux activités fondamentales doivent toujours être notifiés avant leur commencement.

Groupe A:

- inventaire intelligible et notification d'au moins 85 % des traitements prévus par l'article 25;
- les procédures présentant des risques spécifiques au sens de l'article 27 doivent toutes avoir été notifiées au CEPD;
- un DPD est en fonction;
- des dispositions d'application ont été adoptées.

Groupe B:

- inventaire intelligible et notification d'au moins 55 % des traitements prévus par l'article 25;
- les procédures présentant des risques spécifiques au sens de l'article 27 et pour lesquelles le CEPD a publié des lignes directrices doivent toutes avoir été notifiées au CEPD, sauf si elles n'ont pas encore été adoptées en interne;
- un DPD est en fonction;
- des dispositions d'application ont été adoptées.

Groupe C:

- inventaire intelligible et notification d'au moins 40 % des traitements prévus par l'article 25;
- les procédures présentant des risques spécifiques au sens de l'article 27 et pour lesquelles le CEPD a publié des lignes directrices doivent toutes avoir été notifiées au CEPD, sauf si elles n'ont pas encore été adoptées en interne;
- un DPD est en fonction;
- des dispositions d'application ont été adoptées ou soumises au CEPD pour consultation.

Groupe D:

- un DPD est en fonction;
- des dispositions d'application ont été adoptées ou soumises au CEPD pour consultation.

6. Conclusions

Dans l'ensemble, le CEPD est satisfait des résultats atteints par de nombreux institutions et organes en ce qui concerne la mise en œuvre du règlement. Chez la plupart d'entre eux, le niveau de respect de la réglementation a augmenté depuis 2009, mais dans certains cas, des efforts supplémentaires sont nécessaires. Les organes du groupe D, qui participaient pour la première fois à cet état de la situation, affichent des débuts prometteurs.

La présence d'un DPD et son action déterminée constituent un facteur clé dans la mise en œuvre du règlement. Dans le même temps, et sans préjudice de la responsabilité du DPD, il conviendrait de renforcer la responsabilisation de l'institution ou de l'organe en matière de respect adéquat des règles en matière de protection des données. Le CEPD a un rôle à jouer pour souligner et, au besoin, faire appliquer cette responsabilisation.

La valeur de cet exercice de comparaison ressort de l'analyse et des valeurs de références qui en résultent. L'analyse a tenu compte du fait que les éléments comparés ne sont pas purement mathématiques et que des différences existent au sein de groupes d'institutions ou organes comparables (date d'établissement, ressources du DPD, taille de l'organe). En outre, l'analyse et les visites effectuées par le CEPD ont révélé que la mise en œuvre du règlement n'est pas seulement une question de temps et de ressources, mais aussi de volonté organisationnelle. Le respect de la réglementation est un processus qui nécessite une attention suffisante de la part de toutes les parties concernées ainsi que l'engagement et le soutien de la hiérarchie dans toutes les institutions et organes.

À l'image des exercices précédents, l'enquête de 2011 est une étape supplémentaire de l'action permanente du CEPD visant à contrôler et à garantir l'application du règlement. En identifiant les manquements et en présentant des valeurs de référence, le rapport vise aussi à responsabiliser davantage les institutions et organes de l'UE au respect des règles en matière de protection des données.

Annexe 1 Groupes d'institutions et organes

Groupe A (12): Institutions et organes fondés avant 2004 et ayant désigné un DPD avant l'établissement du CEPD:

Commission, Comité des régions, Conseil, Cour des comptes, Banque centrale européenne, Cour de justice européenne, Comité économique et social européen, Banque européenne d'investissement, Parlement européen, OLAF, Médiateur européen et Centre de traduction.

Groupe B (17): Organes établis (ou ayant commencé leurs activités) en 2004 ou antérieurement, mais ayant désigné un DPD ultérieurement:

Cedefop, OCVV, EACI, AESA, CEPD, AEE, EFSA, FEI, OEDT, EMA, EMSA, ENISA, ETF, Eurofound, FRA, OHMI et EU-OSHA.

Groupe C (17): Organes établis (ou ayant commencé leurs activités après 2004:

ACCP, EACEA, EAHC, ECDC, AFE, Frontex, GSA, TEN-T EA, Artemis, Clean Sky, ECHA, ERCEA, F4E, PCH, IMI, REA et SESAR.

Groupe D (12): Organes établis en 2011 et anciens organes des deuxième et troisième piliers:

ACRE, ABE, AEAPP, EIGE, EIT, AEMF, CERS, SEAE, CEPOL, AED, IESUE, CSUE.

Annexe 2 Limites de la méthodologie

i) Les inventaires contiennent parfois des procédures impliquant des traitements identifiés par l'organe mais non encore adoptés (en général, la procédure relative au harcèlement). D'évidence, la procédure ne peut être notifiée avant d'avoir été adoptée. Le calcul la fait toutefois apparaître comme traitement non notifié et met donc en évidence un niveau plus faible de respect de la réglementation.

ii) Un organe qui n'identifie pas convenablement toutes les procédures impliquant des traitements peut avoir un taux faussement élevé de respect de la réglementation.

iii) Seuls les traitements effectivement notifiés au DPD ou au CEPD sont pris en considération. Les projets de notifications au titre des articles 25 ou 27 ne sont pas inclus dans les pourcentages.

iv) Une institution peut identifier dans son inventaire un futur traitement à risque, mais comme la procédure liée à ce traitement n'est pas suffisamment développée, il ne peut être notifié conformément à l'article 27. Le calcul le fait toutefois apparaître comme traitement non notifié et met donc en évidence un niveau plus faible de respect de la réglementation.

v) Le CEPD peut suspendre l'analyse d'une notification si des lignes directrices sont en cours d'élaboration sur la même procédure. Le calcul peut toutefois la faire apparaître comme traitement non notifié et donc mettre en évidence un niveau plus faible de respect de la réglementation.

Annexe 3 Liste de sigles des institutions

ABE	Autorité bancaire européenne
ACCP	Agence communautaire de contrôle des pêches
ACRE	Agence de coopération des régulateurs d'énergie
AEAPP	Autorité européenne des assurances et des pensions professionnelles
AED	Agence européenne de défense
AEE	Agence européenne pour l'environnement
AEMF	Autorité européenne des marchés financiers
AESA	Agence européenne de la sécurité aérienne
AFE	Agence ferroviaire européenne
Artemis	Entreprise commune Artemis
BCE	Banque centrale européenne
BEI	Banque européenne d'investissement
CC	Cour des comptes européenne
CdR	Comité des régions
CdT	Centre de traduction
Cedefop	Centre européen pour le développement de la formation professionnelle
CEPD	Contrôleur européen de la protection des données
CEPOL	Collège européen de police
CERS	Comité européen du risque systémique
CESE	Comité économique et social européen
CJUE	Cour de justice de l'Union européenne
Clean Sky	Entreprise commune Clean Sky
COM	Commission européenne
Conseil	Conseil de l'Union européenne
CSUE	Centre satellitaire de l'Union européenne
EACEA	Agence exécutive «Éducation, audiovisuel et culture»
EACI	Agence exécutive pour la compétitivité et l'innovation
EAHC	Agence exécutive pour la santé et les consommateurs
ECDC	Centre européen de prévention et de contrôle des maladies
ECHA	Agence européenne des produits chimiques
EFSA	Autorité européenne de sécurité des aliments
EIGE	Institut européen pour l'égalité entre les hommes et les femmes
EIT	Institut européen d'innovation et de technologie
EMA	Agence européenne des médicaments
EMSA	Agence européenne pour la sécurité maritime
ENISA	Agence européenne chargée de la sécurité des réseaux et de l'information
ERCEA	Agence exécutive du Conseil européen de la recherche
ETF	Fondation européenne pour la formation
EU-OSHA	Agence européenne pour la sécurité et la santé au travail
Eurofound	Fondation européenne pour l'amélioration des conditions de vie et de travail
FEI	Fonds européen d'investissement
FRA	Agence des droits fondamentaux de l'Union européenne
Frontex	Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des États membres de l'Union européenne
F4E	Fusion for Energy
GSA	Autorité de surveillance du GNSS européen

IESUE	Institut d'études de sécurité de l'Union européenne
IMI	Initiative en matière de médicaments innovants
ME	Médiateur européen
OCVV	Office communautaire des variétés végétales
OEDT	Observatoire européen des drogues et des toxicomanies
OHMI	Office de l'harmonisation dans le marché intérieur
OLAF	Office européen de lutte antifraude
PCH	Entreprise commune Piles à combustible et hydrogène
PE	Parlement européen
REA	Agence exécutive pour la recherche
SEAE	Service européen pour l'action extérieure
SESAR	Système européen de nouvelle génération pour la gestion du trafic aérien
TEN-T EA	Agence exécutive du réseau transeuropéen de transport

**Annexe 4 Tableau comparatif des résultats reçus au 30 septembre 2011
(par groupe dans l'ordre alphabétique)**

Institution ou organe	Inventaire	Notification au titre de l'article 25	Notification au titre de l'article 27	Procédures de recrutement notifiées	Procédures notifiées concernant des données de santé	Procédures disciplinaires notifiées	Procédures notifiées concernant le harcèlement	DA	DPD
CdT		82 %	70 %			N			
COM		98 %	97 %						
CdR		100 %	84 %						
Conseil		80 %	89 %						
CJUE		84 %	87 %						
CC		89 %	72 %		NA				
BCE		96 %	73 %						
BEI		99 %	88 %						
PE		98 %	98 %	NA					
CESE		89 %	92 %						
OLAF		100 %	100 %						
ME		100 %	100 %				NA		
Cedefop		62 %	65 %						
OCVV		70 %	80 %			N	N		
EACI		73 %	100 %			NA			
AESA		18 %	26 %						
CEPD		55 %	90 %		N	NA	NA		
AEE		80 %	60 %				N		
EFSA		57 %	75 %						
FEI		99 %	88 %						
EMA		100 %	87 %		N				
OEDT		71 %	81 %						
EMSA		100 %	70 %			NA	NA		
ENISA		73 %	66 %			NA	NA		
ETF		33 %	75 %			NA			
Eurofound		100 %	100 %						
FRA		100 %	68 %			NA			
OHMI		90 %	89 %	N	N	N			
EU-OSHA		100 %	43 %			NA	NA		
Artemis	R	R	R		NA	NA	NA		
Clean Sky	R	R	R		NA	NA	NA		
ACCP		40 %	31 %			NA	NA		
EACEA		45 %	66 %		N	NA			
EAHC		50 %	50 %			NA			
ECDC									N
ECHA		57 %	42 %						
AFE		19 %	53 %			N	NA		
ERCEA		10 %	20 %			NA			
F4E		10 %	18 %		N	NA	NA	N	
PCH	R	R	57 %		NA	NA	NA		
Frontex	R	R	R						
GSA (GNSS)	N	N	N	N	N	NA	NA	N	
IMI	R	R	R		NA	NA	NA		
REA		20 %	28 %	N		NA		N	
SESAR		16 %	28 %	N	NA	NA	NA		
TEN-T EA		48 %	55 %			NA			

ACRE	N	N	NA	NA	NA	NA	NA	EC
CEPOL		N	NA	NA	NA	NA	NA	
ABE	N	N	NA	NA	NA	NA	NA	
AED	N	N	NA	NA	NA	NA	NA	
SEAE	N	N	NA	NA	NA	NA	NA	EC
EIGE		N	NA	NA	NA	NA	NA	N
AEAPP	N	N	NA	NA	NA	NA	NA	
EIT		N	NA	NA	NA	NA	NA	N
AEMF	N	N	NA	NA	NA	NA	NA	EC
CERS		14 %	100 %					N
IESUE			NA	NA	NA	NA	NA	
CSUE	N	N	NA	NA	NA	NA	NA	N

	Groupe A
	Groupe B
	Groupe C
	Groupe D
	pas de réponse
	Oui
N	Non
R	Registre
NA	Non Applicable*
DA	Dispositions d'application
DPD	Délégué à la protection des données
EC	En cours

* Procédure non encore adoptée