EUROPEAN DATA PROTECTION SUPERVISOR

Contrôler et garantir le respect du règlement (CE) n° 45/2001

Document stratégique

Bruxelles, le 13 décembre 2010

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 63
Courriel: edps@edps.europa.eu – Site internet: www.edps.europa.eu
Tél.: 02-283 19 00 – Télécopie: 02-283 19 50

Table des matières

Contrôler et garantir le respect du règlement (CE) n° 45/2001

1. Introduction

Le présent document stratégique définit comment le Contrôleur européen de la protection des données (CEPD) contrôle, mesure et garantit le respect du règlement (CE) n° 45/2001 («le règlement»), et explique la nature des divers pouvoirs d'exécution , tout en précisant quand et comment le CEPD les utilisera. Ce document reflète bon nombre des activités et actions actuelles du CEPD dans le domaine du contrôle et de la garantie de la conformité, et fixe un cadre global pour tous les travaux à venir en la matière. Il est guidé par les principes de proportionnalité, de responsabilisation (en anglais "accountability") et de cohérence, et vise à rendre le traitement que le CEPD réserve aux informations obtenues grâce à nos activités (traitement des réclamations, contrôles préalables, suivi, etc.) transparent. Il reflète aussi les principes généraux grâce auxquels nous assimilerons et exploiterons ces informations ainsi que, le cas échéant, le poids ou la gravité que nous leur accorderons.

Cette stratégie vise à encourager le respect volontaire et les bonnes pratiques, à créer des incitations suffisantes en matière de conformité et à faciliter l'action ciblée, le cas échéant, en:

- soulignant à qui échoit la responsabilité;
- expliquant comment le CEPD soutient le respect des règles;
- expliquant ce que fera le CEPD en cas de non-conformité.

Afin d'optimiser l'efficacité du cadre existant, ce document stratégique vise à refléter l'approche par étape, prévue par le règlement, pour garantir la protection des données dans les institutions et les organes de l'Union européenne (UE): les institutions ou organes, les responsables du traitement, les délégués à la protection des données (DPD) et le CEPD contribuent tous à l'application et au respect du règlement. C'est pourquoi la stratégie vise à tirer parti de ces rôles et responsabilités et des synergies sous-jacentes, afin de veiller au respect effectif des principes de protection des données.

En conséquence de l'entrée en vigueur du traité de Lisbonne, l'ensemble des institutions et organes de l'Union sont liés par les droits fondamentaux à la vie privée et à la protection des données à caractère personnel (voir articles 7 et 8 de la Charte de l'UE et l'article 16 du TFUE). Le CEPD est chargé de contrôler et de garantir que ces droits sont respectés conformément au règlement (CE) n° 45/2001.

L'article premier, paragraphe 1, du règlement prévoit explicitement que les institutions et organes de l'Union européenne eux-mêmes assurent la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur droit à la vie privée, à l'égard du traitement des données à caractère personnel.

En outre, le CEPD tient à ce que les institutions et organes adoptent une approche proactive envers cette responsabilité en adhérant à la notion de «responsabilisation» (telle qu'élaborée récemment par le groupe de travail de l'article 29)[1] et, ce faisant, en encourageant la protection des données dans la pratique. La «responsabilisation» nécessite que les institutions et organes, de même que les responsables du traitement des données agissant en leur nom, mettent en place des mesures appropriées et efficaces afin de veiller à ce que les principes et obligations fixés dans le règlement soient respectés, et le prouvent au CEPD à sa demande. Le CEPD se concentrera ensuite sur ses responsabilités relatives au contrôle et, le cas échéant, à la garantie de la conformité.

Au sein des institutions et organes de l'Union, les DPD seront essentiels à la réussite de tout programme de «responsabilité», et dans ce contexte, le CEPD salue les «Normes professionnelles des Délégués à la protection des données des institutions et organes européens travaillant en application du règlement (CE) n° 45/2001» (octobre 2010) du réseau des DPD.[2] Le CEPD estime que ce document offre une base satisfaisante pour établir une nouvelle gouvernance plus efficace de la protection des données, composée de politiques saines, de mécanismes de mise en œuvre efficaces et de programmes d'assurance appropriés.

Selon le CEPD, cette nouvelle gouvernance permettra une approche sélective, ciblée et fondée sur le risque, tout en mettant l'accent sur les institutions ou organes faisant preuve d'un manque d'engagement manifeste ou de mauvaises performances en matière de respect. En retour, cette approche permettra une utilisation efficace de nos ressources limitées dans le cadre actuel de la protection des données de l'Union européenne.

2. Contrôle de la conformité

Le CEPD dispose de plusieurs outils et mécanismes lui permettant de remplir ses fonctions de contrôleur. Certains d'entre eux découlent directement des dispositions du règlement, tandis que d'autres résultent de dispositions législatives différentes ou reflètent simplement les bonnes pratiques. Les indices recueillis grâce à l'ensemble de ces outils et mécanismes serviront à établir des renseignements sur les différents organes ou institutions, ce qui, en retour, permettra d'étayer toute décision liée aux mesures d'exécution formelles.

1 Avis de mars 2010 concernant le principe de responsabilité (WP 173), adopté le 13 juillet 2010, disponible à l'adresse suivante: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_fr.pdf

2 Disponible à l'adresse suivante: http://www.edps.europa.eu/EDPSWEB/edps/Supervision/DPOnetwork

2.1. Outils à la disposition du CEPD

2.1.1. Sensibilisation

Conformément à l'article 46, point d), et à l'article 47, paragraphe 1, point b), du règlement, le CEPD continuera de consacrer du temps et des ressources pour fournir des conseils, des orientations et des formations (génériques comme personnalisés) sur les questions liées à la protection des données relevant de son domaine de compétence. Le cas échéant, il publiera et attirera l'attention sur ces orientations de façon appropriée. Le CEPD espère ainsi encourager non seulement le respect, mais aussi l'adoption de bonnes pratiques au sein des institutions et des organes de l'Union.

Dans le contexte de cette stratégie, le CEPD s'attend à ce que toute orientation ou formation fournie soit mise en œuvre par l'institution ou organe concerné, et à ce que les responsables du traitement, notamment les DPD, jouent un rôle significatif et approprié en ce sens, conformément à leurs responsabilités prévues par le règlement (voir article 24, paragraphe 1, points a) et c), concernant les DPD). Par conséquent, il tiendra compte de tous les résultats et indices pertinents rassemblés dans l'exercice de ses fonctions lorsqu'il envisagera de prendre une mesure éventuelle d'exécution. Il contrôlera également la demande et les résultats de la formation et des conseils ou orientations fournis afin d'étayer sa prise de décision à ce sujet.

Le CEPD élabore actuellement des orientations sur certains sujets sous la forme de documents thématiques, afin d'adopter des avis horizontaux pour établir des procédures administratives standard au sein des agences. Ces dernières constitueront ensuite un ensemble de normes du CEPD pour les institutions. Les travaux dans ce domaine peuvent être approfondis sous la forme d'ateliers et de séminaires interactifs lors desquels le CEPD présente notre position et notre expérience dans un domaine donné.

2.1.2 Contrôles préalables

En vertu de l'article 27 du règlement, le CEPD est habilité à effectuer des contrôles préalables des traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées. Au titre du même article, les DPD sont tenus de notifier ces contrôles préalables au CEPD. En retour, l'avis résultant d'un contrôle préalable doit être notifié au responsable du traitement, qui est tenu de modifier le traitement lorsque cela est nécessaire, sans quoi il risque de faire l'objet d'une mesure d'exécution.

Lorsque le CEPD a commencé ses activités, plusieurs opérations de traitement sujettes à contrôle préalable étaient déjà en cours. En 2004, le CEPD a demandé aux institutions ou organes d'effectuer un inventaire des cas susceptibles d'être soumis à un contrôle préalable. En ce qui concerne les contrôles préalables ex-post, le CEPD a adopté une approche thématique, en définissant des thèmes prioritaires (données médicales, évaluations du personnel, données disciplinaires, services sociaux) et en demandant une

notification pour ces derniers. À l'issue de cette phase initiale, le CEPD a invité les institutions à soumettre toutes les notifications relatives aux traitements déjà en place. Aujourd'hui, la situation est telle que la grande majorité des contrôles préalables ex-post dans les institutions européennes a été notifiée au CEPD.

L'article 27 laisse peu de place à une approche sélective en ce qui concerne les travaux de contrôle préalable, mais le cas échéant, le CEPD a limité son champ d'application en invoquant l'article 27, paragraphe 3 (qui prévoit la consultation du CEPD en cas de doute quant à la nécessité d'un contrôle préalable). Par exemple, le CEPD a déterminé que le traitement des données à caractère personnel liées à l'utilisation de téléphones portables par le personnel de l'EACI en mission n'était pas soumis à un contrôle préalable, car la finalité du traitement était de contrôler des factures d'un montant supérieur à 50 EUR, et non d'évaluer les aspects de la personnalité des membres du personnel. Dans un autre cas, le CEPD a décrété que le traitement des données à caractère personnel visant à garantir que le personnel de l'OEDT perçoit des allocations scolaires n'était pas soumis à un contrôle préalable, car il ne visait pas en tant que tel à exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat.

Le suivi des avis résultant des contrôles préalables est un élément essentiel de la stratégie de mise en application du CEPD. Le CEPD conclut généralement ces derniers en déclarant que le traitement n'enfreint pas le règlement (CE) n° 45/2001, pour autant que certaines recommandations soient mises en œuvre. Si ces recommandations ne sont pas appliquées et mises en évidence, l'institution doit savoir qu'elle risque une mesure d'exécution formelle. Pour sa part, le CEPD définira des recommandations et des délais clairs et concis, et effectuera le suivi de façon cohérente et approfondie pour garantir le respect du règlement.

Les contrôles préalables permettent d'instaurer un dialogue préventif avec les institutions ou organes sous la forme de réunions ou de consultations publiques, l'objectif étant d'encourager une culture positive et proactive en matière de protection des données.

Les contrôles préalables permettent également au CEPD d'avoir un aperçu des activités des institutions et organes de l'Union, et l'aident à repérer les principales questions relatives à la protection des données et à établir sa propre jurisprudence. Grâce à l'expérience obtenue quant à l'application du règlement, le CEPD a pu acquérir une expertise et fournir des lignes directrices génériques thématiques aux institutions et organes.

Les lignes directrices du CEPD en matière de vidéosurveillance du 17 mars 2010[3] doivent être perçues comme un cas expérimental, tant en ce qui concerne la transmission d'orientations aux institutions et organes qu'au regard de leur mise à l'essai au moyen d'un recentrage des priorités sur la

3 Disponible à l'adresse suivante: http://www.edps.europa.eu/EDPSWEB/edps/Supervision/Guidelines

«responsabilisation». Si un organe respecte les recommandations formulées par le CEPD, un contrôle préalable est en principe inutile. Cependant, une fois encore, lorsqu'une institution ou un organe ne tient pas compte des lignes directrices, ne respecte pas les délais appropriés ou ne met pas en œuvre les recommandations y afférentes, le risque de mesure d'exécution formelle augmente.

2.1.3 Consultations

En vertu de l'article 28, paragraphe 1, et de l'article 46, point d), du règlement, les institutions et organes de l'Union sont tenus d'informer et de consulter le CEPD lorsqu'ils élaborent des règles internes et de mesures administratives relatives au traitement de données à caractère personnel.

L'article 28, paragraphe 1, dispose que les institutions et organes informent le CEPD lorsqu'ils élaborent des mesures administratives, telles que des règles de mise en œuvre relatives au règlement ou au DPD (article 24, paragraphe 8), ainsi que des règles internes administratives générales relatives au traitement de données à caractère personnel (par exemple l'utilisation du courriel, le contrôle électronique, l'archivage, etc.). Le cas échéant, le CEPD évaluera les mesures en projet et formulera des recommandations, que l'institution sera tenue d'appliquer. Le CEPD s'attend à être tenu informé des progrès en la matière et mènera des activités de suivi afin de garantir la conformité.

L'article 46, paragraphe d, décrit dans les grandes lignes le rôle consultatif du CEPD *«pour toutes les questions concernant le traitement de données à caractère personnel»*, et ajoute que le CEPD peut conseiller *«avant l'élaboration [par les institutions ou organes] de règles internes relatives à la protection des libertés et droits fondamentaux des personnes à l'égard du traitement des données à caractère personnel»*.

Bien que l'article 46, point d), se recouvre en partie avec l'article 28, paragraphe 1, il élargit le champ d'application à «toutes» les autres questions, et fournit dès lors une base pour conseiller sur les cas impliquant des activités de traitement spécifiques ou des questions abstraites relatives à l'interprétation du règlement (par exemple quant à la façon d'appliquer le droit d'accès dans des cas particuliers présentant des difficultés pratiques, à la manière d'interpréter et de mettre en œuvre l'article 9, etc.). Lorsque les consultations reçues reposent sur des cas hypothétiques ou traitent de questions d'interprétation, le suivi est limité, mais ne peut être exclu.

Le CEPD salue toute consultation proactive de la part d'une institution ou d'un organe, et considérera cette démarche comme une avancée positive vers le respect du règlement. Il escompte néanmoins que les institutions ou organes concernés endosseront les responsabilités appropriées pour effectuer toute modification, ou appliquer les conseils ou recommandations découlant de ces consultations, et ne peut exclure la possibilité de prendre des mesures d'exécution dans le cas contraire.

2.1.4. Traitement des réclamations

L'article 33 du règlement permet aux employés des institutions ou organes de l'Union de présenter une réclamation au CEPD pour une violation alléguée des dispositions du règlement régissant le traitement des données à caractère personnel. L'article 46, points a) et b), dispose que le CEPD examine les réclamations et effectue des enquêtes à leur sujet le cas échéant. L'examen des réclamations par le CEPD nécessite la coopération des DPD et des responsables du traitement, en particulier, mais peut très bien inclure d'autres membres du personnel de l'institution ou de l'organe concerné lorsque cela est nécessaire pour l'examen d'un cas donné.

Les réclamations et les examens qui en découlent constituent une source d'informations importante du point de vue du contrôle du respect du règlement. Le CEPD continuera d'analyser ces informations afin de décider, lors de ses activités de supervision au sens large, si elles témoignent de problèmes de respect supplémentaires ou étayent d'autres indices de mauvaise pratique ou de non respect déjà recueillis. Il déterminera alors s'il y a lieu de prendre des mesures complémentaires, telles qu'une inspection ou une mesure d'exécution formelle.

Le CEPD a adopté une politique en matière de réclamations qui permet un traitement sélectif de celles-ci. Des critères ont été fixés dans le manuel interne des réclamations afin de déterminer, dans un premier temps, si une réclamation nécessite d'être traitée, puis de choisir comment procéder. Si l'expérience permettra de mieux détailler ces critères, les principaux éléments de la politique ont été publiés[4] afin d'aider les requérants potentiels à comprendre l'approche du CEPD et de permettre à ce dernier de mieux répondre à leurs attentes.

Qui plus est, le CEPD envisage de fournir des orientations aux institutions comme au public, de sorte que si une réclamation peut être directement déposée auprès du CEPD, les bonnes pratiques impliqueront généralement que les deux parties tentent de résoudre l'affaire de façon bilatérale au moyen d'une procédure de réexamen interne. Il importe de noter que cette procédure nécessite de fournir les ressources nécessaires au DPD afin qu'il puisse traiter les réclamations. Les dispositions d'application adoptées en vertu de l'article 24, paragraphe 8, du règlement, confèrent ces pouvoirs à certains organes et institutions. De plus, le document relatif aux normes professionnelles du réseau des DPD soutient cette approche[5], et contribue ainsi aux objectifs consistant à accroître la «responsabilisation» du

4 Disponible à l'adresse suivante: http://www.edps.europa.eu/EDPSWEB/edps/Supervision/Complaints

5 Voir section 3.7 des «Normes professionnelles des Délégués à la protection des données des institutions et organes européens travaillant en application du règlement (CE) n° 45/2001»

responsable du traitement et à transférer la responsabilité de la conformité aux institutions ou agences elles-mêmes.

2.1.5. Exercices de contrôle et de reporting ciblés

Le CEPD effectuera un contrôle ciblé sur la base des connaissances et des indices obtenus de toutes ses activités de supervision, l'objectif étant de repérer les thèmes, les institutions ou les organes méritant une attention plus particulière. Ce contrôle consistera généralement à mener des enquêtes fondées sur la correspondance en ce qui concerne certains types de traitement des données, pour la totalité ou certains des organes et institutions. En cas de besoin, il pourra toutefois comprendre une visite de terrain - par exemple lorsqu'un organe ou une institution enfreint à plusieurs reprises les dispositions du règlement ou n'en tient pas suffisamment compte. Ces exercices aboutiront généralement à un ensemble approuvé de recommandations et de délais, souvent sous la forme d'une feuille de route.

La non-application de ces recommandations et/ou le non-respect des délais y afférents pourront entraîner une augmentation des mesures d'exécution. Dans ce contexte, le CEPD comptera sur l'assistance et la collaboration nécessaires des dirigeants des institutions, des responsables du traitement et bien sûr des DPD, conformément à l'article article 47, paragraphe 2, point a), et à l'article 24, paragraphe 1, point b), du règlement.

2.1.6. Exercices de contrôle et de reporting généraux

À ce jour, le CEPD a tenté à deux reprises de mesurer le respect général du règlement en écrivant à la direction des institutions et des agences et en demandant un retour d'information écrite sur certains sujets. Le CEPD continuera de mener ces «enquêtes» périodiques afin de garantir qu'il dispose d'un aperçu représentatif du respect de la protection des données au sein des institutions ou organes de l'Union, et qu'il peut fixer des objectifs internes appropriés pour traiter ses constatations.

Qui plus est, sur la base des réponses et des indices qu'il reçoit, le CEPD fournira des commentaires individuels à chaque institution ou agence, et définira des objectifs normatifs pertinents en cas de non-respect. Le retour d'information pourra également servir à sélectionner les institutions ou organes à contrôler, le cas échéant. En cas de non-réalisation des objectifs, des décisions contraignantes seront généralement adoptées, y compris une obligation de notification. Le non-respect répétitif du règlement est alors susceptible d'entraîner des mesures d'exécution (voir plus bas).

Il convient en outre de noter que les dispositions d'application de certaines institutions obligent leurs DPD à rédiger des rapports d'activité. Ces rapports indiquent souvent le niveau de respect du règlement au sein de l'institution, et

présentent dès lors un intérêt manifeste pour le CEPD. Aussi le CEPD apprécierait-il de recevoir des copies de ces rapports[6], mais aborderait évidemment toute question soulignée de façon collaborative et informelle pour ne pas décourager la pratique en général. Cependant, si l'institution n'applique aucun des conseils ou recommandations du CEPD qui en découlent, l'adoption de mesures d'exécution formelles ne peut être exclue.

2.1.7. Inspections

L'article 41, paragraphe 2, l'article 46, point c), et l'article 47, paragraphe 2, du règlement accordent au CEPD de larges pouvoirs qui lui permettent d'exercer ses fonctions d'autorité de supervision.

Une stratégie spécifique d'inspection est en cours d'élaboration. Néanmoins, étant donné l'importance du temps et des ressources nécessaires pour effectuer les inspections, le CEPD tient à garantir une approche sélective de leur utilisation, qui se limite à deux types généraux (standard et thématique), et est suscités par les indices et faits rassemblés grâce aux autres outils présentés dans la présente section.

Les inspections standard sont conçues pour examiner et garantir le respect des décisions du CEPD dans le cadre des avis résultant des contrôles préalables ou des réclamations, et de façon plus générale, pour garantir le respect du règlement lorsque les exercices de contrôle réguliers ont signalé de façon préoccupante un blocage du mécanisme de respect. Ces inspections doivent dès lors être considérées comme la dernière étape avant l'adoption de mesures d'exécution formelles.

Le CEPD effectuera également des inspections thématiques, dont l'approche consistera à fournir des orientations pour un domaine ou un thème particulier, ainsi qu'à fixer des délais dans lesquels les institutions et agences doivent respecter les normes de protection des données et les recommandations définies dans ces orientations. Le non-respect de ces délais ou la non-application des normes ou recommandations requises augmentera la probabilité de mesures d'exécution formelles.

Par leur nature, les inspections seront conçues sur mesure et structurées autour d'exigences et d'objectifs spécifiques. Il est toutefois probable que le CEPD souhaite faire participer et coopérer à cette procédure les directeurs et les responsables de l'institution ou de l'organe, les responsables du traitement des données concernés, le DPD[7] et tout autre membre du personnel approprié.

6 La section 4, paragraphe 1, des «Normes professionnelles des Délégués à la protection des données des institutions et organes européens travaillant en application du règlement (CE) n° 45/2001» est favorable à la transmission d'une copie de ces rapports au CEPD.
7 Le rôle du DPD dans les inspections effectuées par le CEPD sera élaboré dans la stratégie d'inspection du CEPD.

2.2. Outils à la disposition des Institutions et agences de l'Union européenne

Les évaluations de l'incidence sur la vie privée, les notifications des brèches à la sécurité et les rapports internes de conformité sont des mécanismes que les institutions et organes de l'Union peuvent eux-mêmes utiliser afin d'encourager la conformité avec les responsabilités en matière de protection des données, et bien sûr pour contribuer à faire preuve d'un esprit ou d'une pratique «responsable». S'ils ne s'appuient pas encore tous sur des obligations légales, ils doivent néanmoins être perçus comme des outils importants au sein de l'environnement dans lequel le CEPD agit, et comme des indicateurs culturels importants et des sources de preuve du respect du règlement. Aussi le CEPD les encouragera-t-il lorsqu'ils seront pertinents et appropriés, par exemple en publiant des orientations.

En conséquence, lorsque ces initiatives auront été mises en œuvre sur une base volontaire, le CEPD adoptera une approche constructive et favorable à toute question concernant le respect repérée grâce à ces mécanismes, et recourra à des mesures plus sérieuses et formelles uniquement en l'absence d'une telle coopération.

Les audits et les évaluations des risques pour la vie privée constituent deux outils supplémentaires susceptibles d'accroître l'efficacité des activités de contrôle du respect du CEPD, mais doivent encore être mis au point à ce jour.

2.2.1. Évaluations des incidences sur la vie privée

Le CEPD devrait encourager les institutions et agences à réaliser des évaluations des incidences sur la vie privée (EIVP) pour chaque nouveau traitement mettant en jeu des données à caractère personnel. Le CEPD envisage dès lors de formuler des orientations en la matière afin d'indiquer que nous escomptons une réalisation par défaut des EIVP ou de préciser le type de données ou de traitement pour lesquels nous souhaiterions une EIVP. Une autre approche qui permettrait de soutenir cet outil de respect consisterait à ce que le CEPD effectue une évaluation initiale déterminant si une EIVP est nécessaire et, le cas échéant, charge l'institution d'y procéder.

Les EIVP sont importantes car elles permettent aux institutions et organes d'obtenir un meilleur aperçu des risques pour la vie privée et des moyens de les aborder. Elles peuvent également aboutir à des notifications, à des contrôles préalables, à des recommandations et à un suivi.

2.2.2 Notifications des brèches à la sécurité

Le CEPD devrait également encourager les institutions à adopter des procédures internes concernant les atteintes à la sécurité (conformément à la directive «Vie privée et communication électronique» et aux pratiques

nationales) comprenant la notification des brèches au DPD ou au CEPD par le responsable du traitement. Les règles d'application de la Commission en matière de sécurité (notification au DPD) doivent être considérées comme un premier pas en ce sens.

La réaction du CEPD à ces notifications dépendra bien sûr de plusieurs facteurs, dont la gravité de l'atteinte à la sécurité, le type et le volume des données concernées, le nombre de personnes concernées, la localisation des bénéficiaires, etc. La réaction du CEPD reflètera également la différence entre les brèches signalées par leur auteur et celles portées à son attention par l'intermédiaire de réclamations, de la presse ou autre.

2.2.3 Rapports internes sur la conformité

Le CEPD devrait envisager de formuler des orientations visant à encourager les institutions et organes de l'Union à élaborer des rapports internes sur le respect de la protection des données. Non seulement ces derniers constituent de précieux outils de contrôle, mais ils permettent également de transférer la responsabilité du respect vers les institutions elles-mêmes, encourageant par là même la "responsabilisation». Le CEPD pourrait inciter les institutions et organes à participer à ces notifications de façon proactive, par exemple en autorisant des dérogations appropriées de nos enquêtes générales de contrôle.

2.2.4 Audits

Le CEPD pourrait examiner les possibilités de coopérer avec les services d'audit, de façon à pouvoir suivre de façon appropriée les problèmes liés au respect découverts dans le cadre de leur travail. Cette coopération nécessitera presque à coup sûr un protocole d'accord afin de définir clairement les rôles, les responsabilités et les procédures. Le cas échéant, il conviendra également d'informer les institutions et les organes de la réalisation de ces échanges d'informations.

2.2.5. Évaluations des risques pour la vie privée

En vue de faciliter une approche sélective fondée sur le risque et de soutenir un programme de travail plus efficace et ciblé, le CEPD pourrait tenter de définir des critères et des bilans réguliers (par exemple bisannuels) afin de déterminer quels domaines et sujets méritent une attention particulière.

3. Mesures d'exécution

3.1. Introduction et contexte

Les pouvoirs d'exécution du CEPD sont énoncés à l'article 47 du règlement. Leur spectre est relativement large, allant du conseil à l'avertissement et à l'interdiction du traitement. Cette stratégie vise à conférer clarté et cohérence à l'application de ces pouvoirs.

Au vu du cadre interinstituonnel au sein duquel agit le CEPD, ce dernier n'a pas encore adopté d'approche punitive, préférant formuler des recommandations et encourager le respect plutôt que de mettre en garde ou de réprimander le responsable du contrôle ou de rendre des décisions juridiquement contraignantes. Néanmoins, après cinq ans d'activité sur ce modèle, il est temps de signaler un changement d'approche.

Si le CEPD continuera d'encourager le respect et les bonnes pratique selon des méthodes informelles et collaboratives, il adoptera désormais une approche globale et proactive envers l'action formelle pour les infractions graves, délibérées ou répétées, ou lorsque ses conseils ont été ignorés. Nous gardons à l'esprit que l'inaction en cas de non-respect avéré va à l'encontre de nos objectifs de responsabilité et de cohérence et risque de nuire à l'autorité du CEPD.

Comme énoncé précédemment dans le présent document, lorsqu'il décidera de prendre ou non des mesures d'exécution formelles, le CEPD examinera minutieusement la totalité des preuves et des faits obtenus grâce à toutes ses activités de supervision. Ces renseignements étayeront non seulement sa décision de recourir aux mesures d'exécution, mais l'aideront également à déterminer le type de mesures à prendre.

3.2. Types et définition des mesures d'exécution

Le CEPD dispose de différents types de mesures d'exécution. La mesure la plus efficace sera choisie en tenant compte des résultats qu'elle peut permettre d'atteindre et de son effet négatif ou éducatif possible pour l'institution ou organe en question et les autres institutions et organes. Dans le contexte du présent document stratégique, les mesures d'exécution formelles sont définies telles que prévues à l'article 47, paragraphe 1, points c) à h) du règlement, en vertu duquel le CEPD peut:

- ordonner que les demandes d'exercice de certains droits à l'égard des données soient satisfaites lorsque de telles demandes ont été rejetées en violation des articles 13 à 19;

- adresser un avertissement ou une admonestation au responsable du traitement;

- ordonner la rectification, le verrouillage, l'effacement ou la destruction de toutes les données lorsqu'elles ont été traitées en violation des dispositions régissant le traitement de données à caractère personnel, et la notification de ces mesures aux tiers auxquels les données ont été divulguées;

- interdire temporairement ou définitivement un traitement;

- saisir l'institution ou l'organe concerné et, si nécessaire, le Parlement européen, le Conseil et la Commission;

- saisir la Cour de justice de l'Union européenne (conformément aux conditions pertinentes).

Même si l'utilisation de ces pouvoirs sera probablement rare dans la pratique, le CEPD entend adopter une approche plus proactive et résolue quant à leur emploi à l'avenir. À titre d'illustration, des exemples de scénarios sont présentés à la section 3.4.

3.3. Déclencheurs des mesures d'exécution

Le CEPD adoptera une approche sélective et proportionnée envers l'introduction et la poursuite de mesures d'exécution, en adéquation avec ses ressources limitées. Comme mentionné plus haut, le cadre interinstitutionnel préconise une approche coopérative optant pour des mesures fondées sur l'article 47, paragraphe 1, point b) (saisir le responsable du traitement et formuler des propositions tendant à remédier à une violation). Par conséquent, dans la plupart des cas, toute mesure formelle sera prise en fonction de préoccupations sur les préjudices significatifs réels ou potentiels provoqués par le non-respect des principes de protection des données ou d'infractions répétées, graves ou délibérées aux recommandations du CEPD.

Les déclencheurs initiaux des mesures d'exécution seront en général:

- des préoccupations soulevées dans les réclamations que nous recevons;

- des préoccupations révélées par nos activités de supervision ou de contrôle

- des préoccupations révélées par nos activités consultatives.

En déterminant la nécessité de prendre des mesures, la forme de celles-ci et les proportions dans lesquelles nous les appliquerons, nous tiendrons compte des critères suivants:

- des mesures sont-elles nécessaires pour clarifier un point de loi ou un principe important?

- o des mesures sont-elles justifiées par la probabilité que les conséquences négatives d'une violation aient des effets durables, ou qu'une violation se répète si aucune mesure n'est prise?

- o la pratique d'une activité particulière par le représentant de l'institution ou de l'organe prend-elle des proportions nécessitant de donner un exemple?

- o le fait qu'une institution ou un organe ne suive pas les orientations du CEPD (document de position, lignes directrices, recommandations, etc.) appuie-t-il la prise de mesures?

- o l'attitude et la conduite de l'institution, de l'organe ou du DPD, en ce qui concerne aussi bien le cas d'espèce que les questions relatives au respect, de façon plus générale, suggèrent-elles une approche délibérément peu serviable ou peu coopérative?

- o le niveau d'intérêt public sur le sujet est-il suffisant pour soutenir la prise de mesures?

- o la prise de mesures d'exécution spécifiques peut-elle être justifiée au vu des ressources nécessaires et des exigences divergentes pesant sur celles-ci?

- o quels sont les risques encourus pour la réputation et la crédibilité du CEPD en cas d'action ou d'inaction?

- o serait-il plus opportun ou efficace que les mesures soient prises par d'autres moyens ou organes (par exemple par le Médiateur européen ou devant la Cour)?

3.4. Exemples de mesures d'exécution

Ci-dessous figurent plusieurs exemples de types de conduites susceptibles ou non d'inciter le CEPD à employer ses pouvoirs de d'exécution formelle. Lorsqu'une action est plausible, les exemples indiquent également les résultats potentiels. Ces exemples se veulent illustratifs plutôt qu'exhaustifs ou contraignants.

3.4.1. Action probable (notamment à la suite d'un avertissement)

- o le refus d'accorder l'accès à la personne concernée, lorsqu'il y a lieu de supposer que des informations importantes sont détenues, peut donner lieu à un ordre d'accorder l'accès;

- o l'absence répétée de réponse au CEPD ou de mise en œuvre de ses recommandations relatives à un traitement peut entraîner l'envoi d'un

avertissement au responsable du traitement. Cette mesure peut comprendre la transmission d'une lettre au directeur (ou haut fonctionnaire) concerné ou la publication de cette lacune et sa mention dans le rapport annuel du CEPD;

- la collecte et la détention de données à caractère personnel détaillées ou sensibles pour une période considérablement plus longue que nécessaire ou à des fins non précisées (notamment lorsque cela influe sur les perspectives de carrière) peut entraîner un ordre d'effacement ou de destruction;

- les préoccupations ou doutes restant sans réponse en ce qui concerne la légalité du traitement peuvent conduire le CEPD à imposer une interdiction temporaire ou définitive sur ce dernier;

- une divulgation non autorisée délibérée de données à caractère personnel ou l'accès non autorisé à ces dernières peut entraîner la saisie du Parlement européen, du Conseil ou de la Commission, voire, dans certaines circonstances, de la Cour de justice, ainsi qu'une publication ultérieure.

3.4.2. Action improbable

- le non-respect «accidentel» des dispositions du règlement est reconnu et suivi par une mesure correctrice prompte et efficace;

- le non-respect n'est pas particulièrement gênant et n'a pas porté de préjudice significatif, à moins qu'il ne soulève des questions plus larges;

- d'autres moyens de pression, tels que la publicité négative et la nuisance à la réputation, peuvent être plus rapides et plus efficaces que les mesures d'exécution formelles du CEPD en vue de remédier au non-respect.

4 Transparence et publicité

Le CEPD estime que la transparence sur ses activités est importante tant pour ses parties prenantes que pour sa bonne gouvernance. Il publie dès lors les informations pertinentes sur son site internet et dans son rapport annuel. Il recourt également à des communiqués de presse afin de souligner des actions, décisions et avis importants et d'attirer l'attention sur des questions d'actualité significatives dans le domaine de la protection des données.

En ce qui concerne ses activités de mise en application, le CEPD diffusera généralement des informations relatives à tout renvoi officiel devant le Parlement, le Conseil, la Commission ou la Cour de justice de l'UE. Qui plus est, il évaluera au cas par cas s'il est opportun ou avantageux de diffuser des

informations, par l’intermédiaire de médias appropriés, au sujet d'autres mesures d'exécution exposées dans la section 3.2 ci-dessus.

Lorsque le CEPD entendra diffuser les détails ou les résumés de ses mesures d'exécution formelles, il le signalera au préalable à l’institution ou à l’organe concerné pour lui permettre d’examiner et de préparer une réponse publique s’ils le jugent approprié.