Avis sur la notification d'un contrôle préalable relatif au système de coopération en matière de protection des consommateurs («SCPC») par la Commission européenne le 9 janvier 2009

Bruxelles, le 4 mai 2011 (dossier 2009-0019)

Table des matières

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

1. Introduction

1.1. Champ d'application de l'avis

Dans le présent avis, le Contrôleur européen de la protection des données (ci-après le «**CEPD**») évalue le respect de la protection des données par le système de coopération en matière de protection des consommateurs (ci-après le «**SCPC**») et recommande d'y apporter des améliorations supplémentaires, notamment des mesures techniques et organisationnelles devant être prises par la Commission.

Le SCPC est un système informatique conçu et exploité par la Commission conformément au règlement (CE) n° 2006/2004 relatif à la coopération en matière de protection des consommateurs (ci-après le «**règlement CPC**»). Le SCPC facilite la coopération entre les «**autorités compétentes**» des États membres de l'UE et la Commission dans le domaine de la protection des consommateurs. La coopération est limitée aux infractions à une série préétablie de directives et de règlements de l'UE. En outre, pour relever du champ d'application du règlement CPC, les infractions doivent être de nature transfrontalière et porter préjudice ou être susceptibles de porter préjudice aux «**intérêts collectifs des consommateurs**».

Dans le cadre de leur coopération, les autorités compétentes échangent des informations, y compris des données à caractère personnel (voir la section 1.3 ci-dessous)[1]. Le système est conçu comme un outil de communication sécurisé permettant aux autorités compétentes d'échanger des informations. En outre, le SCPC enregistre et stocke aussi les informations échangées, souvent pendant de longues périodes (voir la section 3.3). Par conséquent, il y a lieu de le considérer également comme une base de données.

Les recommandations du présent avis s'adressent à la Commission, qui joue un rôle central dans la conception et l'exploitation du SCPC et qui est soumise au contrôle du CEPD. Cela dit, bon nombre des recommandations formulées dans le présent avis – notamment celles relatives à la formation, aux lignes directrices en matière de protection des données, à l'information des personnes concernées et aux solutions de «respect de la vie privée dès la conception» intégrées à l'architecture du système – peuvent également faciliter le respect des règles en matière de protection des données par les autres utilisateurs du système, comme les autorités compétentes des États membres. Par conséquent, les recommandations adressées à la Commission devraient contribuer à assurer un niveau général plus élevé de protection des données dans le SCPC.

Parallèlement à l'adoption du présent avis sur une notification de contrôle préalable (rendu conformément à l'article 27 du règlement (CE) n° 45/2001 – ci-après le «**règlement**»)[2], le CEPD publie un autre avis (conformément à l'article 28, paragraphe 2, du règlement), qui commente le cadre juridique du SCPC en se concentrant essentiellement sur la modification du 1er mars 2011 de la décision 2007/76/CE de la Commission[3]. Dans cet avis, le CEPD fait

[1] En outre, la Commission collecte et traite également les données à caractère personnel des utilisateurs du SCPC (gestionnaires de dossiers), comme l'exploitation du système l'exige (par exemple, pour attribuer des identifiants et des mots de passe). Cette activité de traitement ne faisant pas l'objet d'un contrôle préalable (voir la section 2.2 ci-dessous), elle ne sera pas examinée plus avant dans le présent avis.

[2] 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 communautaires et à la libre circulation de ces données, JO 2001, L 8/1.

[3] Décision de la Commission du 1er mars 2011 modifiant la décision 2007/76/CE portant application du règlement (CE) n° 2006/2004 du Parlement européen et du Conseil relatif à la coopération entre les autorités

également le point sur les progrès réalisés à ce jour et met en exergue certaines autres préoccupations et considérations pour l'avenir. Les deux documents devraient être considérés conjointement.

1.2. Description du traitement

Les flux d'informations suivants sont prévus dans le SCPC pour faciliter la coopération:

- **Échange d'informations sur demande** (article 6 du règlement CPC). À la demande d'une autorité requérante, l'autorité requise fournit sans retard toute information pertinente requise pour établir si une infraction communautaire s'est produite ou s'il y a de bonnes raisons de soupçonner qu'une telle infraction est susceptible de se produire.
- **Échange d'informations sans demande préalable** (article 7). Toute autorité peut envoyer un message d'avertissement («**alerte**») à ses homologues du réseau dans les autres États membres ainsi qu'à la Commission pour les informer d'une infraction à la législation relative à la protection des consommateurs ou leur faire savoir qu'elle a de bonnes raisons de soupçonner une telle infraction. L'autorité qui émet l'alerte peut choisir les États membres auxquels elle souhaite adresser son message. Autrement dit, toutes les alertes ne parviennent pas nécessairement à tous les États membres.
- **Demande de mesures d'exécution** (article 8). Une autorité requérante peut demander à une autre autorité de prendre toutes les mesures d'exécution nécessaire pour faire cesser ou interdire sans retard une infraction[4].
- **«Notifications» (article 7, paragraphe 2, et article 8, paragraphe 6).** Lorsqu'à la suite d'une alerte, une autorité prend des mesures d'exécution ou reçoit une demande d'assistance mutuelle, elle doit notifier les mesures d'exécution ou la demande à ses homologues du réseau dans tous les autres États membres ainsi qu'à la Commission (article 7, paragraphe 2). Une autorité doit également informer ses homologues du réseau dans tous les États membres ainsi que la Commission de toute mesure d'exécution qu'elle a prise à la suite d'une demande de mesure d'exécution ainsi que de ses effets (et notamment indiquer si l'infraction a cessé) (article 8, paragraphe 6).
- **Coordination des activités de surveillance du marché et d'exécution de la législation** (article 9). Lorsqu'une infraction porte préjudice aux intérêts des consommateurs dans plus de deux États membres, les autorités compétentes concernées coordonnent leurs mesures d'exécution et leurs demandes d'assistance mutuelle. Elles peuvent en particulier mener des enquêtes et prendre des mesures d'exécution de façon simultanée.

En plus de ces échanges, des informations qui ne sont pas liées à des dossiers peuvent être échangées à travers un «**module de forum**». Ce forum ne vise pas à échanger des données à caractère personnel (bien qu'on ne puisse exclure cette éventualité; pour réduire le plus possible la divulgation par mégarde de données à caractère personnel sur le forum, voir les recommandations à la section 3.2).

nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, pour ce qui est de la coordination de la surveillance du marché et des activités d'exécution de la législation.

[4] Dans le présent avis, l'«échange d'informations sur demande» et la «demande de mesures d'exécution» seront parfois désignés l'un et l'autre comme des «**demandes d'assistance mutuelle**».

1.3. Données à caractère personnel traitées

Lorsqu'ils échangent des informations dans le SCPC, les utilisateurs peuvent compléter plusieurs champs de données structurés. Certains sont facultatifs, d'autres obligatoires. Ces champs de données décrivent le type d'infraction avérée ou présumée; le vendeur ou le fournisseur responsable de l'infraction (y compris ses données de contact, son adresse IP, sa société mère et ses directeurs); le préjudice potentiel pour les consommateurs; et d'autres informations importantes liées à l'affaire.

En ce qui concerne les champs de données structurés, un champ de données pour le(s) nom(s) des directeurs de la société permet de relier des informations à des individus (les directeurs mentionnés). Il implique dès lors un traitement de données à caractère personnel.

Au moment de publier le présent avis, le champ relatif au nom du directeur dans l'architecture du SCPC n'était pas encore utilisé, bien que techniquement disponible. Une pratique provisoire a été mise en place au lieu de cela pour répondre aux problèmes de protection des données épinglés dans l'avis du groupe de travail sur la protection des données institué par l'article 29, avis évoqué à la section 2.3 ci-dessous. Ainsi, les noms des directeurs, lorsqu'ils sont téléchargés dans le SCPC, figurent actuellement dans des pièces jointes confidentielles plutôt que dans le champ de données structuré spécifique prévu à cet effet.

Sur le plan pratique, cela implique que i) par défaut, les «bureaux de liaison uniques» (ci-après les «**BLU**»)[5] n'ont pas accès à ces informations; ii) la Commission n'a pas accès à ces informations; et iii) ces informations ne sont pas interrogeables dans la base de données puisqu'elles ne sont pas incluses dans un champ de données structuré.

La pratique consistant à utiliser des pièces jointes au lieu de champs de données structurés est décrite à la page 15 du document intitulé «Consumer Protection Cooperation Network: Operating Guidelines» («Le réseau de coopération pour la protection des consommateurs: lignes directrices»), approuvé par le comité CPC le 8 juin 2010 (ci-après les «**lignes directrices du RCPC**»)[6]. La Commission attend actuellement la publication du présent avis sur la notification d'un contrôle préalable, et donc les nouvelles recommandations du CEPD, pour commencer à utiliser les champs de données structurés relatifs aux noms des directeurs.

D'autres informations traitées dans le SCPC peuvent également être considérées, en fonction des circonstances de l'affaire, comme des données à caractère personnel et donc exiger des garanties en matière de protection des données.

Ces informations peuvent notamment être les suivantes:

- Le vendeur ou fournisseur en infraction peut – dans certains cas – être un individu. Dans ce cas, toutes les données liées à son entreprise et traitées dans le SCPC (par exemple, le fait que l'entreprise soit soupçonnée d'infraction) constituent ses données à caractère personnel protégées par le règlement et, le cas échéant, la directive 95/46/CE (ci-après la «**directive**»).

[5] Comme exposé ci-dessous à la section 1.4, les BLU sont des autorités publiques spécifiques chargées dans chaque État membre de coordonner l'application du règlement CPC.

[6] Pour ce qui est des droits d'accès, des balises de sécurité et des possibilités de recherche, voir la section 1.5 ci-dessous.

- Le lien entre une raison sociale et un individu est parfois très fort et peut être reconstitué facilement (par exemple, la raison sociale d'une petite entreprise peut comprendre le nom de famille du propriétaire, et son adresse être la même que l'adresse privée du propriétaire). Dans ce cas aussi, les données liées à l'entreprise et traitées dans le SCPC présentent également un intérêt pour l'individu[7].

Par ailleurs, le SCPC contient aussi deux champs non structurés pour les échanges d'informations:

- un champ pour les «**résumés succincts**», qui doit être complété en tant que texte libre[8] et
- une fonction permettant de joindre des documents.

Ces champs peuvent contenir des données à caractère personnel, par exemple, les données de salariés, de plaignants ou de consommateurs.

Enfin, on ne peut exclure que des informations échangées dans le module de forum contiennent également des données à caractère personnel. Cela dit, les lignes directrices en matière de protection des données dans le cadre de la CPC (voir la section 3.1 ci-dessous) recommandent clairement aux agents des services répressifs de ne pas inclure de données à caractère personnel dans les résumés succincts et dans le forum de discussion.

1.4. Responsables du traitement des données: rôles et responsabilités

Dans le SCPC, plusieurs acteurs sont concernés de diverses manières par le traitement de données à caractère personnel. Il y a trois «types» de responsables du traitement dans le SCPC, chacun ayant son propre rôle et ses responsabilités spécifiques.

- Premièrement, chaque **autorité compétente** est responsable de sa propre utilisation du SCPC (par exemple, de la pertinence et de l'exactitude des informations qu'elle télécharge dans le système). En tant qu'utilisateur, elle fait donc office de responsable du traitement dans le SCPC en vertu de la législation nationale relative à la protection des données.
- Deuxièmement, l'architecture du SCPC repose notamment sur les «bureaux de liaison uniques» («**BLU**»). Il s'agit d'autorités publiques spécifiques chargées dans chaque État membre de coordonner l'application du règlement CPC[9]. Elles ont notamment pour tâche d'acheminer les demandes d'assistance mutuelle aux autorités compétentes adéquates. Les BLU font également office de responsables du traitement (chacun individuellement), pour ce qui est de leurs propres activités.
- Enfin, la **Commission** a elle aussi un rôle et des responsabilités spécifiques en tant que responsable du traitement. Elle joue en particulier un rôle central en définissant les fonctions du système, elle exploite le système, veille à la sécurité des données échangées, gère les utilisateurs du SCPC et traite les incidents techniques et de sécurité. C'est aussi la seule partie capable de poser certains actes (comme

[7] Dans certains États membres, les données relatives aux entités juridiques sont également considérées et traitées comme des données à caractère personnel protégées par la législation relative à la protection des données. Dans ces pays, les autorités compétentes échangeant des informations dans le SCPC doivent veiller à la protection des données à caractère personnel relatives aux sociétés, du moins dans une certaine mesure (par exemple, pour ce qui est de la qualité des données ou des droits d'information et d'accès).

[8] Les résumés succincts ne doivent pas contenir de données à caractère personnel (voir la section 3.2).

[9] Les tâches de coordination sont définies à l'article 3, point d), à l'article 9, paragraphe 2, et à l'article 12, paragraphes 2 et 5, du règlement CPC.

l'effacement d'affaires). En outre, la Commission a accès à certaines des données à caractère personnel échangées dans le système, puisqu'elle est destinataire des alertes ainsi que des notifications.

Le CEPD accueille favorablement le fait que:

- le règlement CPC (à l'article 10) précise clairement que chacune des parties susmentionnées ont leurs propres responsabilités en tant que responsables du traitement;
- les lignes directrices en matière de protection des données dans le cadre de la CPC (à la section 3) apportent des éléments supplémentaires concernant les rôles et les responsabilités.

1.5. Accès aux informations dans le SCPC

Les autorités compétentes, les BLU et la Commission ont accès à des catégories différentes d'informations échangées dans le cadre du SCPC:

- Les autorités compétentes ont accès aux demandes d'informations et aux demandes de mesures d'exécution qui leur sont spécialement adressées; elles ont aussi accès aux alertes (à condition d'avoir été sélectionnées comme destinataire par l'expéditeur) et aux notifications relevant de leur compétence.
- Les BLU ne peuvent lire que les informations essentielles sur une affaire afin de pouvoir déterminer l'autorité compétente à laquelle une demande doit être transférée. Ils ne peuvent accéder aux pièces jointes des demandes d'assistance mutuelle que si celles-ci n'ont pas été «**marquées**» comme confidentielles[10]. Ils n'ont pas du tout accès aux alertes et aux notifications.
- Les utilisateurs du SCPC issus de la Commission ont accès aux alertes[11] et aux notifications, en lecture seule. La Commission n'a pas accès aux demandes d'assistance mutuelle.

En outre, comme la Commission est chargée de la maintenance et de l'exploitation du système, ses techniciens peuvent lire et modifier toutes les données du SCPC, y compris les données à caractère personnel.

En ce qui concerne les possibilités de recherche, la Commission a expliqué au CEPD que tous les champs de données structurés sont interrogeables. Les champs de données non structurés, comme les pièces jointes et les champs de texte libre pour les résumés succincts, ne sont pas interrogeables. Chaque utilisateur du SCPC ne peut effectuer une recherche que dans les données auxquelles il a accès (par exemple, le contenu d'une demande d'assistance mutuelle ne peut être interrogé que par les deux autorités compétentes ayant échangé l'information; le contenu d'une alerte peut seulement être interrogé par l'autorité compétente qui a téléchargé l'alerte et par celles qui l'ont reçue).

Le CEPD se félicite que:

[10] Toutes les pièces jointes sont marquées confidentielles par défaut. L'autorité compétente qui télécharge la pièce jointe doit «décliquer» la balise de confidentialité si elle souhaite que le contenu de la pièce jointe soit disponible au BLU.

[11] À l'exception des pièces jointes des alertes, auxquelles les utilisateurs du SCPC issus de la Commission n'ont pas accès.

- des domaines de compétence aient été attribués à chaque autorité compétente: l'information n'est partagée qu'avec les autorités responsables d'un domaine législatif donné (c'est-à-dire une ou plusieurs mesures spécifiques dans le domaine de la protection des consommateurs);
- les BLU acheminent les demandes aux autorités concernées, réduisant ainsi le risque d'erreur lors de la désignation des destinataires;
- les pièces jointes des demandes d'assistance mutuelle et des alertes soient marquées confidentielles par défaut;
- l'accès de la Commission soit limité à ce qui est exigé par le règlement CPC. Ainsi, la Commission n'a pas accès aux informations échangées entre les États membres dans le cadre des demandes d'assistance mutuelle;
- les BLU n'aient accès qu'aux informations essentielles sur une affaire afin de pouvoir déterminer l'autorité compétente à laquelle une demande doit être transférée; et
- les possibilités de recherche soient liées aux droits d'accès.

En ce qui concerne le champ de données structuré relatif aux noms des directeurs, le CEPD n'a aucune objection à ce qu'un champ de données structuré soit utilisé (au lieu que les noms des directeurs soient inclus dans des pièces jointes confidentielles, comme c'est la pratique actuellement).

Toutefois, à moins que la Commission n'explique au CEPD la raison pour laquelle l'accès à ce champ de données est nécessaire à l'exécution des missions de surveillance qui lui incombent en vertu du règlement CPC, le CEPD recommande que des mesures techniques soient mises en œuvre dans le système afin d'exclure cet accès.

En outre, afin de garantir que les données individuelles liées à un vendeur ou à un fournisseur soupçonné d'infraction ne seront pas conservées dans la base de données de manière à pouvoir y être recherchées pendant une période excessivement longue, les recommandations concernant la conservation des données doivent également être appliquées (voir la section 3.3.2 ci-dessous). Quoi qu'il en soit, en cas d'infractions présumées, les données concernant des directeurs diffusées dans une alerte ne doivent pas être interrogeables après la période recommandée à la section 3.3.2 ci-dessous (qui est en principe de six mois). Si nécessaire, d'autres restrictions des possibilités de recherche devront encore être envisagées.

2. Compétence du CEPD

2.1. Applicabilité du règlement (CE) n° 45/2001

Dans la mesure où les activités de la Commission sont concernées, le traitement notifié relève du champ d'application du règlement et du contrôle du CEPD (voir les articles premier et 3 du règlement)[12].

2.2. Motifs de contrôle préalable

Les échanges d'informations dans le SCPC comprennent des données à caractère personnel portant sur des infractions avérées ou présumées à la législation relative à la protection des consommateurs. Ces infractions peuvent être de nature administrative ou pénale. Par

[12] Pour chaque autorité compétente et chaque BLU, la législation applicable est sa propre législation nationale en matière de protection des données (conformément à la directive) et ses activités sont contrôlées par sa propre autorité nationale ou régionale chargée de la protection des données.

conséquent, le SCPC est soumis à l'article 27, paragraphe 2, point a), du règlement, qui prévoit le contrôle préalable du CEPD en cas, notamment, de «traitements de données relatives à des suspicions, infractions, condamnations pénales ou mesures de sûreté».

2.3. Procédure

Le 9 janvier 2009, la Commission a notifié le SCPC au CEPD en vue d'un contrôle préalable «*ex post*»[13]. Le CEPD a publié l'avis le 4 mai 2011, après avoir reçu les informations nécessaires demandées à la Commission[14].

Le CEPD note que le SCPC était déjà utilisé avant qu'il en soit informé et, par conséquent, ses recommandations doivent être appliquées *ex post*. Pour l'avenir, le CEPD attire l'attention de la Commission sur le fait que l'avis du CEPD doit être demandé et obtenu avant de commencer tout traitement de données à caractère personnel.

3. Analyse juridique et recommandations

3.1. Base juridique et licéité du traitement

Après avoir adopté le règlement CPC (voir la section 1.1), la Commission a encore renforcé la base juridique du SCPC en adoptant une décision de mise en œuvre et une recommandation:

- la décision 2007/76/CE de la Commission du 22 décembre 2006 mettant en œuvre le règlement CPC, telle que modifiée le 17 mars 2008 et le 1er mars 2011 (ci-après la «**décision mettant en œuvre la CPC**»)[15] et
- la recommandation de la Commission du 1er mars 2011 concernant les lignes directrices régissant l'application de règles relatives à la protection des données au SCPC (ci-après «**les lignes directrices en matière de protection des données dans le cadre de la CPC**»)[16].

Comme il a été observé dans l'avis sur les nouvelles mesures adoptées par la Commission en vue de l'application du règlement CPC, le CEPD note avec satisfaction que le traitement repose sur une base juridique solide dont le fondement est un règlement adopté par le Conseil et le Parlement. En outre, le CEPD accueille favorablement le fait que cet instrument juridique initial ait été complété au fil du temps pour apporter de plus amples précisions et remédier aux problèmes liés à la protection des données.

---

[13] Le SCPC avait été examiné précédemment par le groupe de travail sur la protection des données institué par l'article 29, qui a publié son avis 6/2007 (GT 139) le 21 septembre 2007. Les recommandations émises dans le présent avis sont conformes à l'avis 6/2007.

[14] Conformément à l'article 27, paragraphe 4, du règlement, le présent avis doit être rendu dans les deux mois, sans compter les éventuelles périodes de suspension autorisées pour la réception des informations complémentaires demandées par le CEPD. Le CEPD a demandé de plus amples renseignements à la Commission le 14 janvier 2009 et le 24 janvier 2011, renseignements fournis le 22 décembre 2010 et le 2 mars 2011, respectivement. Le CEPD a envoyé son projet d'avis pour commentaires le 18 mars 2011. Dans le même temps, en raison de la complexité de l'affaire, il a également prolongé de deux semaines le délai dont il disposait pour rendre son avis. La Commission a communiqué ses observations finales le 14 avril 2011. Le délai pour rendre l'avis du CEPD était donc le 4 mai 2011.

[15] Décision 2007/76/CE de la Commission portant application du règlement (CE) n° 2006/2004 du Parlement européen et du Conseil relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs en ce qui concerne l'assistance mutuelle.

[16] Recommandation de la Commission du 1er mars 2011 concernant les lignes directrices régissant l'application de règles relatives à la protection des données au système de coopération en matière de protection des consommateurs (SCPC) (2011/136/UE).

3.2. Qualité des données

L'article 13, paragraphe 1, du règlement CPC prévoit que «*les informations fournies peuvent uniquement être utilisées pour assurer le respect des lois protégeant les intérêts des consommateurs*». L'article 13, paragraphe 2, ajoute que «*les autorités compétentes peuvent invoquer comme moyen de preuve des informations, des documents, des constatations, des déclarations, des copies certifiées conformes ou des renseignements transmis, au même titre que des documents analogues obtenus dans leur propre pays*».

Vu le large champ d'application de ces dispositions, il est essentiel que les échanges de données dans le cadre du SCPC répondent, sur le plan pratique, aux normes de qualité des données fixées par l'article 4, paragraphe 1, points a), b), c) et d), du règlement. Ainsi, il est impératif que toute donnée à caractère personnel échangée soit adéquate, pertinente, proportionnée et exacte; qu'elle soit traitée loyalement et licitement; et qu'elle ne soit pas traitée ultérieurement à des fins incompatibles.

Chaque cas est différent. Par conséquent, le respect des principes de qualité des données doit être évalué de manière concrète, pour chaque cas particulier, que l'information soit téléchargée, retirée ou traitée par les utilisateurs du SCPC. Vu les difficultés d'une évaluation au cas par cas et étant donné que la plupart des utilisateurs du SCPC ne sont pas des experts de la protection des données, il est extrêmement important que:

- l'architecture du SCPC soit conçue et configurée de telle manière à favoriser le plus possible le respect de la législation relative à la protection des données; et que
- les utilisateurs du système soient dûment formés, conseillés et habilités à prendre des décisions concernant la protection des données.

Le CEPD se félicite que la décision mettant en œuvre la CPC prévoie des séries spécifiques de champs obligatoires et facultatifs pour chaque échange d'informations et que celles-ci soient proportionnées, compte tenu des finalités des échanges d'informations[17].

En outre, le CEPD accueille favorablement les recommandations figurant dans les lignes directrices en matière de protection des données dans le cadre de la CPC, qui visent à limiter les données à caractère personnel incluses dans les échanges d'informations, et plus particulièrement:

- que les agents des services répressifs doivent évaluer si l'inclusion du nom des directeurs est vraiment nécessaire;
- qu'ils ne doivent pas inclure de données à caractère personnel dans le champ de texte libre pour les «résumés succincts»;
- qu'ils doivent évaluer si des données à caractère personnel doivent être incluses dans les pièces jointes; que si cette inclusion n'est pas strictement nécessaire, les données à caractère personnel doivent être censurées ou retirées[18]; et
- que le forum de discussion ne puisse pas servir à l'échange de données liées aux affaires ni contenir de données à caractère personnel.

[17] Pour ce qui est du champ «directeurs», voir nos recommandations spécifiques à la section 1.5 ci-dessus.

[18] S'il s'avère ultérieurement que cette information est cruciale pour les finalités de l'enquête ou de la mesure d'exécution (par exemple, si elle peut servir de preuve), elle peut être demandée dans une communication ultérieure.

3.2.1. Effacement de données erronées

La décision mettant en œuvre la CPC[19] impose aux autorités compétentes de demander à la Commission de supprimer les données erronées qui ne peuvent être corrigées d'une autre manière.

La Commission a expliqué au CEPD que cette disposition constitue une solution «de repli» pour un faible nombre d'affaires pour lesquelles il n'existe pas d'autres mécanismes plus adéquats permettant la correction ou l'effacement des données. C'est parfois le cas des «doublons», lorsqu'une autorité compétente télécharge deux fois la même information par erreur, ou lorsque cette autorité se trompe en indiquant le domaine législatif concerné (par exemple, une directive). Dans la plupart des autres situations, les autorités compétentes sont en mesure de corriger elles-mêmes les données téléchargées. Par exemple, elles peuvent modifier les informations relatives au vendeur ou au fournisseur concerné, ou corriger ou supprimer les données dans une pièce jointe.

Le CEPD n'a aucune objection à la solution «de repli» décrite ci-dessus. Toutefois, il insiste sur le fait que le système et ses interfaces doivent être conçus de telle manière à réduire la nécessité de recourir à cette solution de repli.

Par ailleurs, l'effacement doit toujours être effectué de telle manière qu'une piste d'audit appropriée soit disponible pour attester l'opération réalisée (voir aussi la section 3.6).

3.2.2. Vers un module de protection des données (respect de la vie privée dès la conception)

Comme il a été observé précédemment, pour faciliter la mise en œuvre de ces recommandations dans la pratique, le CEPD préconise que l'architecture du SCPC soit conçue et configurée de telle manière à favoriser le plus possible le respect de la législation relative à la protection des données.

Le CEPD note avec satisfaction que l'architecture du système contient déjà certaines fonctions respectueuses de la protection des données afin de renforcer le respect des exigences en la matière, comme des messages contextuels informant le gestionnaire de dossiers qui télécharge une pièce jointe qu'aucune donnée à caractère personnel ne peut être incluse dans celle-ci si elle n'est pas strictement nécessaire, ou le message contextuel général incitant les autorités compétentes à évaluer les aspects liés à la protection des données avant d'«envoyer» formellement une demande d'assistance mutuelle ou une alerte par le SCPC.

Si l'expérience montre que des orientations supplémentaires sont nécessaires pour les gestionnaires de dossiers, d'autres solutions que les messages contextuels actuels ou des mesures techniques supplémentaires pourraient être élaborées et constituer un **«module de protection des données**» spécifique dans l'architecture du SCPC. Celles-ci pourraient comprendre les garanties «cliquables» suivantes:

- lorsqu'une autorité compétente complète le champ relatif au nom des directeurs, le système pourrait afficher automatiquement un message d'avertissement demandant si l'inclusion de ces informations est absolument nécessaire pour les besoins de l'affaire, et demander également une justification spécifique pour cette inclusion;

[19] Voir l'annexe, point 2.1.5, tel que modifié.

- avant de télécharger un résumé succinct, un avertissement pourrait apparaître, qui demanderait à l'utilisateur de confirmer qu'aucune donnée à caractère personnel n'a été incluse dans le résumé succinct (si ce n'est la dénomination commerciale du vendeur ou du fournisseur, s'il s'agit d'une personne physique);
- avant de décliquer une balise de confidentialité, un avertissement pourrait apparaître, qui décrirait clairement les implications de cette décision, en particulier les personnes qui auraient alors accès à quel type d'informations téléchargées.

Le système devrait également inclure des directives sur les questions de protection des données, comme celles mentionnées ci-dessus, dans le «menu d'aide» accessible depuis l'application du SCPC.

Une fonction permettant le retour d'information et la communication entre les autorités compétentes et la Commission en ce qui concerne les problèmes de respect de la protection des données peut également être envisagée, si le besoin s'en fait sentir. En utilisant cette fonction, tout destinataire de l'information aurait la possibilité, à travers le SCPC, de signaler à l'autorité compétente qui télécharge l'information que celle-ci a posé un problème au regard du respect de la protection des données. Par exemple, des données à caractère personnel ont été incluses dans les résumés succincts, ou des données à caractère personnel sans rapport avec l'affaire ont été incluses dans une pièce jointe. Une telle fonction pourrait contribuer à réduire le plus possible les échanges de données à caractère personnel et faciliter la correction d'informations inexactes ou dépassées[20].

Comme on le signalera plus loin à la section 3.5, le module de protection des données pourrait aussi comprendre un mécanisme de coordination pour traiter les demandes d'accès formulées par les personnes concernées et prendre des décisions à leur sujet.

3.2.3. Formation et sensibilisation à la protection des données

Comme indiqué ci-dessus, un niveau élevé de protection des données dans le SCPC impose que les utilisateurs du système reçoivent des orientations adéquates quant à la manière d'appliquer la protection des données dans la pratique lorsqu'ils traitent des données dans le SCPC.

À cet égard, le CEPD salue les efforts que la Commission a faits, dans les lignes directrices en matière de protection des données dans le cadre de la CPC, en organisant des ateliers, en contactant des BLU et par d'autres moyens, afin de sensibiliser les gestionnaires de dossiers aux questions suivantes de protection des données, entre autres:

- les gestionnaires de dossiers doivent réduire le plus possible l'inclusion de données à caractère personnel (c'est-à-dire qu'ils ne doivent les inclure que lorsqu'elles sont essentielles aux finalités de l'échange d'informations);
- ils doivent avoir conscience du fait que le champ relatif au directeur de la société est facultatif et qu'ils doivent évaluer soigneusement si l'inclusion de cette information dans le SCPC est strictement nécessaire[21];

[20] Tant que la fonction (de discussion) «Questions et réponses» dans le SCPC permet aux autorités compétentes concernées par un échange d'informations donné de discuter de ces questions dans le cadre de l'architecture du SCPC, un canal de communication spécifique peut ne pas être strictement nécessaire à ce stade.

[21] Le CEPD accueille favorablement le fait que l'interface du SCPC indique clairement au moyen d'un astérisque tous les champs de données qui sont obligatoires et que le champ relatif au directeur n'en fait pas partie.

- ils doivent soigneusement passer en revue les destinataires de leurs messages et ne diffuser des données à caractère personnel que si ceux-ci doivent en prendre connaissance. Ce principe s'applique tant à la communication avec d'autres autorités compétentes qu'au sein d'une autorité compétente donnée;
- ils doivent classer les affaires en temps opportun et demander l'effacement des affaires tout de suite après;
- ils doivent avoir conscience des droits d'information et d'accès des personnes concernées et être bien au fait de la procédure de traitement des demandes d'accès;
- ils doivent se conformer aux mesures de confidentialité et de sécurité. À cet égard, chaque autorité compétente doit également veiller à ce que seuls des agents dûment accrédités aient accès au SCPC et que dès qu'un agent quitte sa fonction, les autorités informent immédiatement la Commission de manière à ce que l'accès accordé à cet utilisateur puisse être immédiatement retiré.

En outre, le CEPD accueille favorablement le fait que les lignes directrices en matière de protection des données dans le cadre de la CPC mettent en exergue l'importance de la formation.

Le CEPD souligne que, pour devenir réalité, les recommandations figurant dans les lignes directrices précitées doivent aller de pair avec des programmes de formation adéquats. Les utilisateurs du SCPC doivent avoir une bonne connaissance des problèmes de protection des données qu'ils sont susceptibles de rencontrer en échangeant des données dans le SCPC. Les activités de sensibilisation menées par la Commission jouent un rôle important.

3.3. Période de conservation

L'article 6, point e), de la directive dispose que «*les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées ou pour lesquelles elles sont traitées ultérieurement*». L'article 4, paragraphe 1, point e), du règlement contient une disposition équivalente.

3.3.1. Faits, cadre juridique et état de la situation

Trois périodes doivent être prises en considération dans le flux de travail des affaires du SCPC:

- période de conservation jusqu'au classement de l'affaire: la période qui prend cours au moment où une affaire est ouverte et qui se termine lorsque celle-ci est classée dans le système;
- période de conservation du classement à l'effacement: la période qui commence lorsqu'une affaire est classée et qui se termine lorsque les informations sont finalement effacées dans le système;
- période de conservation totale: la somme des deux autres périodes de conservation.

Le règlement CPC ne prévoit de règles spécifiques que i) pour les alertes non fondées (qui doivent être effacées sans délai) et ii) pour les affaires ayant donné lieu à une mesure d'exécution efficace (qui doivent être effacées dans les cinq ans suivant le classement de l'affaire).

Il ne prévoit aucune autre règle spécifique quant au moment où les affaires doivent être classées ou les informations effacées de la base de données. Toutefois, l'absence de clarté est

susceptible de conduire à une situation où certaines affaires ne seraient jamais classées ni effacées, ou resteraient dans la base de données plus longtemps que nécessaire. Aussi la Commission a-t-elle remédié à ce problème en apportant de plus amples précisions de diverses manières.

Précisions apportées par la décision mettant en œuvre la CPC

i) La décision mettant en œuvre la CPC a fourni des règles supplémentaires en ce qui concerne les différents flux d'informations:

- si une **demande d'information** est «classée» parce que les informations échangées n'ont pas donné lieu à des mesures de suivi (comme une demande de mesures d'exécution ou une alerte), ou qu'il a été établi qu'aucune infraction intracommunautaire n'a eu lieu, et l'autorité compétente concernée déclare que tel est le cas, l'autorité compétente doit dans les sept jours en informer la Commission (qui, pour sa part, doit supprimer toutes les données concernées dans la base de données dans les sept jours suivant la notification). Dans tous les autres cas[22], les demandes d'information sont effacées cinq ans après le classement de l'affaire;

- si une **alerte** est fondée, elle est effacée cinq ans après la date à laquelle elle a été lancée. Si une alerte s'avère non fondée, l'autorité compétente doit la retirer dans les sept jours (pour sa part, la Commission doit supprimer toutes les données concernées dans la base de données dans les sept jours suivant le retrait);

- lorsqu'une **demande de mesures d'exécution** est classée (à la suite de la notification de la cessation de l'infraction), les données liées à l'affaire sont effacées cinq ans après le classement de l'affaire;

- lorsqu'une demande d'information, une alerte ou une demande de mesures d'exécution contient des **données erronées** qui ne peuvent être corrigées d'une autre manière, elle doit être effacée dans les 14 jours (2 x 7 jours, calculé comme décrit ci-dessus).

ii) Sensibilisation prévue par les lignes directrices en matière de protection des données dans le cadre de la CPC

En plus des règles décrites dans la décision mettant en œuvre la CPC, les lignes directrices en matière de protection des données dans le cadre de la CPC sensibilisent à l'importance du classement des affaires en temps opportun.

iii) Repères dans les lignes directrices du RCPC

Au point 2.7 intitulé «*phases and time-lines in a CPC case*» («phases et délais d'une affaire de CPC»), les lignes directrices du RCPC passent en revue les flux d'affaires typiques et recommandent que les demandes d'information soient traitées dans un délai moyen de un à trois mois, et les demandes de mesures d'exécution dans un délai moyen de six à neuf mois (à l'exception des affaires pour lesquelles la procédure nationale prévoit une plus longue période, par exemple en cas de recours contre une décision administrative, où un délai de un an ou plus est davantage réaliste).

[22] Sauf pour les données erronées, voir ci-dessous.

iv) Évaluation annuelle de la situation

La Commission procède aussi à une évaluation annuelle de la situation afin d'encourager le classement des affaires en temps opportun. Elle prépare en particulier une liste d'affaires, qui met aussi en évidence les affaires qui sont restées ouvertes pendant une période considérablement plus longue que la période moyenne de traitement des affaires (la comparaison est effectuée par rapport aux délais fixés dans les lignes directrices du RCPC, comme indiqué ci-dessus). Celles-ci sont ensuite communiquées aux BLU qui, pour leur part, sont invités à contacter les autorités compétentes concernées[23].

v) Actualisation périodique de la situation entre les autorités compétentes concernées par une demande d'assistance mutuelle

Enfin, le point 2.1.3 de la décision mettant en œuvre la CPC exige que, le cas échéant, l'autorité compétente requise transmette régulièrement à l'autorité compétente requérante des données actualisées concernant les mesures d'enquête ou d'exécution qu'elle a prises afin de répondre à sa demande, au moins sur une base trimestrielle.

3.3.2. Évaluation et recommandations du CEPD

Comme indiqué ci-dessus, la Commission a réalisé d'importants progrès en précisant les règles de conservation des données dans le SCPC. Elle a aussi pris des mesures pour faire en sorte que les affaires soient classées en temps opportun.

i) Classement des affaires en temps opportun

En ce qui concerne les classements d'affaires, vu le nombre relativement faible d'informations actuellement échangées dans le SCPC (depuis 2007, 300 nouvelles affaires ont été ouvertes en moyenne chaque année, en ce compris les alertes), le CEPD note que les mesures décrites ci-dessus peuvent être considérées comme suffisantes pour réduire le plus possible les problèmes de protection des données susceptibles de découler du risque qu'un nombre significatif de données à caractère personnel dépassées ou inutilisées restent longtemps dans la base de données.

Au cas où les mesures décrites ci-dessus devaient s'avérer insuffisantes pour garantir à l'avenir le classement des affaires en temps opportun (que ce soit à cause d'une augmentation des informations échangées à travers le SCPC ou pour une autre raison), le CEPD recommande à la Commission d'envisager des mesures supplémentaires, qui pourraient comprendre, entre autres, l'effacement automatique des affaires restées inactives en dépit de messages d'avertissement répétés.

ii) Alertes

Pour ce qui est des alertes, le CEPD est préoccupé par le fait que les alertes resteront dans le système pendant cinq ans, sauf si elles sont explicitement déclarées «non fondées» et retirées par l'autorité compétente qui les a émises.

[23] La Commission projette également d'inclure une fonction de «timbre horodateur» dans la base de données pour certifier, lors de l'évaluation annuelle, que les données à caractère personnel téléchargées dans la base de données sont toujours exactes. Le CEPD accueille favorablement ce projet.

Comme le montrera plus avant l'avis du CEPD sur les nouvelles mesures adoptées par la Commission aux fins de l'application du règlement CPC, vu les risques qu'il y a de conserver pendant une longue période des données concernant des soupçons non confirmés, le CEPD recommande que toutes les alertes soient effacées dans des délais plus courts. Cela devrait être le cas à tout le moins des affaires qui ne donnent pas lieu à des mesures de suivi ultérieures, que ce soit à travers le SCPC ou d'une autre manière. Dans son avis sur les nouvelles mesures adoptées par la Commission, le CEPD recommande que les alertes soient effacées au plus tard dans un délai de six mois après avoir été téléchargées (sauf si une autre période de conservation plus appropriée peut être justifiée).

iii) Période de conservation pour les demandes d'assistance mutuelle classées

La durée de conservation «standard» appliquée dans le SCPC après le classement d'une affaire (qui peut faire l'objet d'exceptions particulières) est de cinq ans, tant pour les demandes d'information que pour les demandes de mesures d'exécution.

Ni le règlement CPC, ni la décision mettant en œuvre la CPC n'explique la raison ou la nécessité de conserver les données pendant une aussi longue période. En guise d'explication, les lignes directrices en matière de protection des données dans le cadre de la CPC énoncent que «*[p]endant la période de conservation, les agents de l'autorité compétente qui sont chargés de veiller au respect de la législation et à qui une affaire donnée avait initialement été confiée peuvent consulter le dossier en question afin d'établir des liens avec des infractions éventuellement répétées. Une telle démarche contribue à améliorer le contrôle de l'application de la réglementation, notamment du point de vue de son efficacité*»[24].

À cet égard, le CEPD recommande à la Commission:

- de préciser plus avant la finalité de la période de conservation de cinq ans;
- d'évaluer si une période de conservation plus courte atteindrait les mêmes objectifs; et
- d'évaluer si toutes les informations actuellement prévues doivent être conservées ou si une partie d'entre elles suffirait (par exemple, il convient d'examiner si la conservation des seules notifications introduites au titre de l'article 8, paragraphe 6, serait suffisante; il y a lieu également d'évaluer spécifiquement si la conservation des noms des directeurs ou des pièces jointes pouvant contenir des données supplémentaires à caractère personnel est nécessaire; une distinction doit en outre être établie entre les données liées à des infractions présumées et celles liées à des infractions «avérées»).

Des recommandations et des éléments d'appréciation supplémentaires concernant la période de conservation figurent dans l'avis du CEPD sur les nouvelles mesures adoptées par la Commission aux fins de l'application du règlement CPC. Comme mentionné ci-dessus, les deux séries d'observations sont complémentaires et doivent donc être considérées conjointement.

[24] Ces lignes directrices ajoutent en outre que «*[l]a période de conservation vise à faciliter la coopération entre les autorités publiques responsables de l'application des lois protégeant les intérêts des consommateurs, lorsqu'elles traitent de cas d'infractions intracommunautaires et à contribuer au fonctionnement harmonieux du marché intérieur, à favoriser la qualité et la cohérence dans l'application des lois qui protègent les intérêts des consommateurs, à contrôler la protection des intérêts économiques des consommateurs et à permettre d'améliorer la qualité et la cohérence de l'application*».

3.4. Informations à fournir à la personne concernée

Aux termes des articles 10 et 11 de la directive, les autorités compétentes sont tenues de fournir aux personnes concernées certaines informations sur le traitement, sans que celles-ci ne leur en aient fait spécifiquement la demande[25]. Les dispositions correspondantes du règlement (articles 11 et 12) établissent des exigences similaires pour la Commission en ce qui concerne les données à caractère personnel qu'elle traite. Les lignes directrices en matière de protection des données dans le cadre de la CPC recommandent une approche «à plusieurs niveaux» en matière d'information. D'après cette approche:

- la Commission doit fournir, sur sa page web EUROPA consacrée au SCPC, un avis détaillé concernant la vie privée qui explique dans un langage clair et simple le fonctionnement du SCPC ainsi que les garanties en matière de protection des données qui y sont appliquées; cet avis doit également comprendre, sans s'y limiter, un avis concernant la protection des données, tel que prévu par le règlement, portant sur les propres responsabilités de la Commission;
- les autorités compétentes (individuellement ou par l'entremise de leurs BLU) doivent également fournir des avis concernant la protection des données, par exemple sur leurs pages web, avis dont le contenu est déterminé par leurs législations nationales respectives en matière de protection des données. Ces informations doivent comprendre un lien vers la page web de la Commission contenant son avis concernant la protection des données, mais aussi fournir de plus amples informations, notamment les coordonnées de l'autorité compétente concernée ainsi que toute restriction nationale au droit d'accès ou d'information.

La Commission a également élaboré et fourni au CEPD un projet d'avis concernant la protection des données.

Le CEPD accueille favorablement les dispositions contenues dans les lignes directrices en matière de protection des données dans le cadre de la CPC, de même que l'élaboration d'un projet d'avis concernant la protection des données, facile à utiliser et informatif. Dans le même temps, il appelle à de nouvelles mesures de nature à garantir que les personnes concernées soient effectivement informées du traitement de leurs données à caractère personnel.

Premièrement, pour ce qui est du projet d'avis concernant la protection des données, le CEPD recommande ce qui suit:

- la section 3.1 du projet (données traitées par les autorités du réseau) doit être modifiée à la lumière de la section 1.3 du présent avis, afin de décrire de manière plus complète les types de données à caractère personnel traitées, qui ne se limitent pas aux noms des directeurs et aux informations dans les pièces jointes;
- la section 5.2 (responsable du traitement compétent pour les données stockées et traitées par la Commission) doit être modifiée à la lumière de la section 1.4 du présent avis, afin de décrire de manière plus précise les rôles et les responsabilités de la Commission, qui vont au-delà du traitement des coordonnées des gestionnaires de dossiers et comprend, par exemple, la responsabilité de la Commission en tant qu'opérateur du système;
- la section 9.2 (recours), deuxième puce, doit être modifiée de manière à ne pas suggérer que les plaintes à l'encontre des activités menées par les autorités

[25] Sauf si certaines des exceptions visées à l'article 13 de la directive s'appliquent.

compétentes et les BLU doivent également être soumises au CEPD. Ces plaintes doivent être traitées par les autorités compétentes chargées de la protection des données dans les États membres;

- il se peut que d'autres modifications doivent encore être apportées au projet pour refléter les garanties supplémentaires fournies par ailleurs dans le présent avis (par exemple, en ce qui concerne les périodes de conservation et la procédure relative aux droits d'accès des personnes concernées);
- dès qu'un projet révisé aura été élaboré, la Commission devra publier son avis concernant la protection des données sur son site web à un endroit bien en vue et de telle manière qu'il puisse être trouvé facilement par les personnes concernées (normalement, en haut de la page d'accueil).

Deuxièmement, le CEPD recommande que la Commission joue, dans la mesure du possible, un rôle préventif, en sa qualité d'opérateur du SCPC, en sensibilisant les autorités compétentes (ou les BLU) à l'importance de fournir un tel avis, afin d'encourager cette pratique au niveau national.

Le CEPD salue et encourage en particulier les ateliers et les initiatives similaires, qui ont eu lieu par le passé. Il est de bonne pratique de renvoyer aux avis nationaux et locaux concernant la protection des données par des liens sur le site web de la Commission consacré au SCPC (et inversement, de renvoyer à l'avis de la Commission depuis les avis locaux). À cet égard, le CEPD souligne aussi l'importance du rôle de coordination que les BLU peuvent jouer en fournissant ces avis dans chaque État membre.

Enfin, le CEPD insiste sur le fait que si l'information sur l'internet est essentielle, cette information, sauf si elle directement portée à l'attention des personnes concernées, ne peut se substituer entièrement à un avis fourni directement à ces dernières.

Par conséquent, la Commission doit sensibiliser, dans la mesure du possible, les autorités compétentes aux meilleures pratiques en matière de communication directe d'avis. Par exemple, une occasion de communiquer l'avis peut se présenter au stade de l'enquête au cours duquel l'autorité chargée de l'enquête informe les représentants d'une entreprise soupçonnée qu'ils font l'objet d'une enquête. À cette occasion, la personne soupçonnée pourrait également être informée que des données à caractère personnel sont susceptibles d'être échangées à travers le SCPC, et un lien vers un avis en ligne concernant la protection des données (ou une copie de cet avis) pourrait lui être fourni.

3.5. Droits de la personne concernée

L'article 12 de la directive et l'article 13 correspondant du règlement imposent aux responsables du traitement d'accorder aux personnes concernées qui en font la demande l'accès à leurs données à caractère personnel afin de rectifier les erreurs et de supprimer des données dans certaines circonstances. Certaines exceptions peuvent s'appliquer en vertu de l'article 13 de la directive et de l'article 20 du règlement.

3.5.1. Restrictions des droits d'accès

L'existence de ce droit – et toute exception potentielle – est susceptible d'avoir d'importantes implications. Il importe de rappeler que, d'après les règles générales, la personne concernée a le droit de savoir si son activité commerciale a été signalée comme une infraction présumée. L'exercice de ce droit peut toutefois – selon les circonstances – interférer avec une enquête en cours.

En vertu de l'article 13, paragraphe 4, du règlement CPC, les États membres adoptent des mesures législatives qui, dans l'attente d'une enquête, peuvent restreindre les droits d'accès des personnes concernées (conformément à la directive). La Commission peut également appliquer certaines restrictions (conformément au règlement).

Eu égard à ce qui précède, lorsqu'elle statue sur une demande d'accès, une autorité compétente appliquera sa propre législation nationale (qui doit être en conformité avec la directive). Compte tenu du fait que chaque échange d'informations dans le SCPC implique au moins deux participants, et en l'absence d'une harmonisation complète des législations et procédures nationales relatives à la protection des données et des consommateurs ainsi que de leur exécution, il se peut qu'une autorité permette à la personne concernée d'accéder à ses données à caractère personnel, tandis que l'autre restreigne l'accès à ces mêmes données.

Afin de réduire le plus possible les conflits et incohérences potentiels susceptibles de surgir dans une telle situation, une approche coordonnée est souhaitable: la coordination devrait veiller à ce que, d'une part, les droits des personnes concernées soient pleinement respectés, et, d'autre part, que les exceptions appropriées découlant de la législation nationale soient prises en compte lorsqu'une nécessité pertinente et légitime de restreindre l'accès doit être satisfaite. Cette approche est non seulement importante pour la protection des données, mais elle contribue aussi à garantir que les autorités compétentes des différents États membres auront confiance dans le fait que leurs besoins légitimes de restreindre l'information seront respectés lors du transfert vers un autre État membre des données fournies par elles.

En l'absence (ou dans l'attente) d'une harmonisation plus poussée, le CEPD salue le fait que les lignes directrices en matière de protection des données dans le cadre de la CPC cherchent à apporter des clarifications et à encourager une approche coordonnée.

Le CEPD apprécie en particulier que les lignes directrices recommandent que la demande d'une personne concernée ne soit honorée qu'après la consultation des autorités dont les enquêtes pourraient être compromises par l'octroi d'un accès.

Le CEPD recommande également d'adopter une approche nuancée. Ainsi, au lieu de solliciter l'approbation formelle des autres autorités concernées, l'autorité compétente qui statue sur la demande d'accès doit tenir compte, au moment où elle prend sa décision (dans la mesure où cela s'avère approprié en vertu de sa propre législation nationale), du fait qu'elle pourrait, en octroyant l'accès, compromettre l'enquête menée par une autre autorité compétente dans un autre État membre.

Dans le même temps, le CEPD souhaite souligner qu'un examen attentif des incidences sur les enquêtes menées dans d'autres États membres (le principe de «prudence» suggéré par la Commission) ne doit pas donner lieu à un «nivellement par le bas» dans le domaine de la protection des données, ni avoir pour objectif de satisfaire la législation de l'État membre ayant le système le plus restrictif en matière de droits d'accès.

Eu égard à ce qui précède, le CEPD recommande à la Commission:

- d'adopter ses propres règles sur la manière dont elle applique toute restriction aux demandes d'accès qui lui sont adressées;
- de se concerter avec les États membres afin de recueillir des informations sur la manière dont les restrictions sont appliquées dans les États membres;

- de contribuer à garantir, dans la mesure du possible, une approche coordonnée suivant les principes décrits ci-dessus; et
- de contribuer à la communication des résultats de cet exercice entre les autorités compétentes et aux personnes concernées.

3.5.2. Procédure autorisant les personnes concernées à exercer leurs droits

En plus des précisions concernant les éventuelles exceptions, il est également crucial de garantir que les personnes concernées puissent exercer leurs droits d'une manière simple et facilement accessible.

Vu le nombre de responsables du traitement (Commission, BLU, diverses autorités compétentes), le fait que chacun d'entre eux puisse avoir accès à différentes catégories de données à caractère personnel stockées dans le SCPC et la multiplicité des législations nationales en matière de protection des données, l'attribution du pouvoir de permettre aux personnes concernées d'exercer leurs droits d'accès est particulièrement complexe. Cela est d'autant plus vrai que la fourniture de l'accès par un utilisateur du SCPC dans un État membre peut affecter la confidentialité des enquêtes dans un autre État membre, comme on l'a montré ci-dessus. Par conséquent, la fourniture de l'accès peut rendre nécessaire la collaboration entre différentes parties.

Dans la pratique, une personne concernée est susceptible de demander à plusieurs sources différentes l'accès, la rectification et l'effacement de ses données à caractère personnel:

- à l'autorité compétente qui a téléchargé les données;
- à une autre autorité compétente ayant accès aux informations;
- à la Commission.

Il est également possible qu'une personne concernée demande l'accès à un responsable du traitement qui n'a aucun accès aux informations demandées (par exemple, parce qu'une alerte ne lui a pas été envoyée, ou parce qu'il n'a pas été associé à une enquête coordonnée).

Les lignes directrices en matière de protection des données dans le cadre de la CPC précisent que la Commission ne peut accorder l'accès à des données que si elle-même (c'est-à-dire, les utilisateurs du SCPC à la Commission) a accès à celles-ci (dans la plupart des cas, cet accès se limite aux alertes et aux notifications; voir la section 1.4).

Le CEPD accueille favorablement les précisions apportées dans les lignes directrices. De nouvelles précisions sont toutefois nécessaires. Ainsi, la procédure de mise en œuvre de l'exercice des droits d'accès doit être mieux définie sur le plan pratique afin de garantir que les demandes des personnes concernées seront effectivement honorées, d'une manière simple et prévisible et en temps opportun, avec le moins de charge administrative et de difficultés possibles pour les responsables du traitement impliqués ou les personnes concernées.

La procédure doit également être décrite de manière transparente dans un avis sur la protection des données qui soit facilement accessible aux personnes concernées. Celui-ci doit indiquer très clairement à qui les personnes concernées doivent soumettre leurs demandes, qui statuera sur celles-ci et sur la base de quelle législation applicable.

Enfin, dans un souci de commodité, la coordination doit également garantir, lorsque cela est possible, que les personnes concernées n'aient pas à soumettre une demande distincte à toutes les autorités compétentes qui utilisent le SCPC et qui sont susceptibles d'avoir accès à leurs

données à caractère personnel. Étant donné qu'à l'heure actuelle, il existe plus de trois cents autorités compétentes enregistrées dans le SCPC, cela pourrait faire peser une charge excessive sur l'exercice d'un droit fondamental.

Afin de réduire le plus possible la charge administrative et assurer une bonne coopération, le CEPD recommande que la coordination soit soutenue par un outil informatique, qui pourrait faire partie du module de protection des données mentionné à la section 3.2.2. Cette fonction pourrait notamment être utilisée pour gérer et acheminer les demandes d'accès dans les cas où l'octroi d'un accès aux données pourrait affecter les enquêtes de deux autorités compétentes ou plus. En outre, elle peut également contribuer à acheminer les demandes à d'autres autorités compétentes concernées au cas où l'autorité compétente contactée par la personne concernée n'aurait pas accès à toutes les données qui la concernent dans le SCPC. Cette fonction pourrait s'avérer particulièrement utile si le SCPC est de plus en plus utilisé et que le nombre de demandes d'accès augmente.

Cela dit, le CEPD n'exclut pas d'autres méthodes de coordination (sans recours à un outil informatique), pour autant que la procédure fixée fournisse une solution efficace permettant aux personnes concernées d'exercer leurs droits. L'intégration de cette fonction dans l'application du SCPC pourrait alors être considérée comme une deuxième étape si le besoin d'une coordination plus efficace se fait sentir. Pour garantir que de nouveaux développements seront réalisés si nécessaire, le CEPD recommande à la Commission de tenir des statistiques sur le nombre de demandes d'accès soumises aux autorités compétentes en ce qui concerne les données échangées à travers le SCPC. Ces statistiques devraient également porter sur la durée nécessaire pour honorer les demandes.

3.6. Confidentialité et sécurité du traitement

[...]

4. Conclusions

Le CEPD accueille favorablement le fait que le SCPC repose sur une base juridique telle que le règlement CPC et que ce texte législatif ait été complété au fil du temps par la décision mettant en œuvre la CPC et par les lignes directrices en matière de protection des données dans le cadre de la CPC, qui apportent de plus amples précisions sur le traitement ainsi que des garanties spécifiques en matière de protection des données. Le CEPD reconnaît en outre les progrès réalisés sur le plan pratique en ce qui concerne la sécurité et les fonctions du SCPC.

Dans l'ensemble, le CEPD n'a aucune raison de conclure à une quelconque violation du règlement, pour autant que les recommandations formulées dans le présent avis soient mises en œuvre, à savoir:

- en ce qui concerne la qualité des données, i) l'architecture du SCPC doit continuer à être configurée de telle manière à favoriser le plus possible le respect de la législation en matière de protection des données, et ii) la Commission doit poursuivre ses activités pour faire en sorte que les utilisateurs du système soient dûment formés, conseillés et habilités à prendre des décisions en matière de protection des données;
- pour ce qui est de la période de conservation, i) à moins qu'une enquête ou une mesure d'exécution ne soit en cours, les alertes doivent être retirées et effacées dans un délai approprié à compter de leur publication (le CEPD recommande une

période de six mois, sauf si une période de conservation plus appropriée peut être justifiée); la Commission doit ii) préciser plus avant la finalité de la période de cinq ans pour la conservation des données, iii) évaluer si une période de conservation plus courte ne permettrait pas d'atteindre les mêmes objectifs et iv) évaluer si toutes les informations actuellement prévues doivent être conservées ou si une partie d'entre elles pourrait suffire;

- la Commission doit revoir son projet d'avis concernant la vie privée et le placer en évidence sur son site web et sensibiliser les autorités compétentes (ou les BLU) à l'importance de fournir un avis afin d'encourager cette pratique au niveau national;
- des mesures supplémentaires doivent être prises pour faciliter l'exercice des droits d'accès, de rectification et d'effacement des données par les personnes concernées. Pour faciliter la coordination, un module de protection des données dans le SCPC doit être envisagé;
- *[...]*.

Fait à Bruxelles, le 4 mai 2011

(**signé**)

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données