Avis sur une notification en vue d'un contrôle préalable reçue de la déléguée à la protection des données de l'Office européen de lutte antifraude concernant le service de notification des fraudes

Bruxelles, le 18 décembre 2007 (dossier 2007-481)

1. Procédure

Le 23 juillet 2007, le contrôleur européen de la protection des données (ci-après le "CEPD") a reçu de la déléguée à la protection des données de l'Office européen de lutte antifraude ("OLAF") une notification en vue d'un contrôle préalable concernant la mise en place d'un service de notification des fraudes ("la Notification").

Le CEPD a demandé un complément d'information au sujet du service de notification des fraudes ("SNF") le 31 juillet 2007. Les réponses ont été reçues le 19 octobre 2007. Le 26 novembre 2007, le CEPD a envoyé le projet d'avis à l'OLAF afin de recueillir ses remarques, lesquelles ont été reçues le 11 décembre 2007.

2. Examen du dossier

Le service de notification des fraudes est un système d'information en ligne que l'OLAF a mis à la disposition du public afin de recueillir plus facilement les informations requises dans le cadre de la lutte contre la fraude, la corruption et autres activités illégales ayant une incidence sur les intérêts financiers de la Communauté. Dans l'ensemble, les fonctions de ce système sont les mêmes que celles du service d'appel gratuit de l'OLAF qui a été soumis à un contrôle préalable du CEPD en juin 2007[1]. Étant donné que les finalités ainsi que les fonctions de traitement de données des deux systèmes présentent des similitudes, le raisonnement juridique utilisé dans le cadre de ce contrôle préalable est fondamentalement le même que celui utilisé dans le cadre de l'avis relatif au contrôle préalable concernant le service d'appel gratuit de l'OLAF.

Le traitement de données à l'étude fait partie intégrante des activités d'enquête globales de l'OLAF et des procédures de lutte contre la fraude, la corruption et autres activités illégales ayant une incidence sur les intérêts financiers de la Communauté. En particulier, la collecte d'informations dans le cadre du SNF constitue la première phase d'une procédure qui peut continuer avec l'ouverture d'une enquête complète, si cela est jugé nécessaire et pertinent. Cependant, l'analyse juridique dans cet avis abordera uniquement les aspects exclusivement liés au traitement de données résultant de l'exploitation du SNF; elle ne portera pas sur les traitements de données effectués lors d'autres phases des procédures d'enquête de l'OLAF ayant pu être examinées dans le cadre d'autres contrôles préalables[2].

[1] Avis du CEPD du 6 juin 2007 sur une notification en vue d'un contrôle préalable concernant un service d'appel gratuit (dossier 2007-74).
[2] Cf. notes de bas de page 3 et 7.

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

On trouvera ci-après une synthèse des procédures d'enquête de l'OLAF destinée à montrer dans quelle mesure le SNF s'intègre dans le cadre du processus d'enquête global de l'OLAF, suivie par une description des fonctions de traitement de données du SNF.

2.1 Les faits

La durée d'une enquête de l'OLAF peut être résumée comme suit: au cours de la *première phase*, les responsables du dossier de l'OLAF évaluent les informations initiales qui ont pu être recueillies directement par l'OLAF ou fournies à l'OLAF par des tiers (témoins, dénonciateurs, informateurs, etc.). Cette phase est appelée la "phase d'évaluation". Si les informations initiales n'ont aucun lien avec un quelconque point relevant de la compétence de l'OLAF, l'affaire est considérée comme classée à première vue[3] ou comme classée[4]. Si l'OLAF estime que les informations sont pertinentes, la *seconde phase* intervient, au cours de laquelle se dérouleront les activités d'enquête comme telles. Il existe deux catégories d'enquêtes: internes et externes, ainsi que plusieurs autres catégories de dossiers: suivi, coordination et assistance pénale[5]. Si une enquête a été ouverte, l'OLAF décide, lorsqu'elle se termine, si elle doit être clôturée avec ou sans mesures de suivi. Dans la première hypothèse, la *troisième phase* est lancée, au cours de laquelle l'équipe de l'OLAF responsable du suivi met en œuvre différentes activités destinées à garantir que les autorités communautaires et nationales compétentes ont dûment exécuté les mesures recommandées par l'OLAF[6]. Si un dossier a été ouvert (plutôt qu'une enquête), il n'y a pas de troisième phase.

Les traitements au sein de la direction du service de notification des fraudes se déroulent généralement *avant* le début de la première phase. Comme décrit ci-après, les traitements effectués dans le cadre du SNF constituent une sorte de "phase d'évaluation préalable". En particulier, dans l'organisation du SNF, les enquêteurs et les responsables de l'OLAF analysent les informations conservées dans le cadre du SNF et entament une analyse préliminaire de leur pertinence afin que l'OLAF puisse décider si une phase d'évaluation doit être ouverte. Le traitement ultérieur qui peut avoir lieu une fois une phase d'évaluation ouverte ne fera pas l'objet d'une étude dans le cadre du présent avis qui, comme mentionné ci-dessus, se limitera à l'analyse qui a lieu exclusivement dans le cadre de l'exploitation et de la gestion du SNF[7].

Le service de notification des fraudes est mis à la disposition du public en tant que système d'information en ligne pouvant être utilisé par le public pour soumettre des informations à l'OLAF au sujet d'une fraude ou d'une corruption suspectée portant atteinte aux intérêts de la Communauté.

L'***objectif du traitement*** est d'obtenir du public des informations susceptibles de révéler l'existence d'une fraude ou d'une corruption portant atteinte aux intérêts financiers de la Communauté.

---

3 *Affaires classées à première vue*: lorsque les informations ne relèvent clairement et manifestement pas de la compétence de l'OLAF.

4 *Affaires classées:* lorsque les intérêts de l'UE ne semblent pas être menacés par une activité irrégulière ou lorsqu'un État membre traite déjà une question de façon satisfaisante.

5 *Dossiers de suivi:* dossiers pour lesquels l'OLAF aurait la compétence pour ouvrir une enquête externe mais où un État membre ou toute autre autorité est plus apte à mener l'enquête. Dans ces cas, il n'y a pas d'enquête de l'OLAF; l'OLAF assure toutefois le suivi avec l'équipe compétente.
Dossiers de coordination: dossiers qui pourraient faire l'objet d'une enquête externe, mais pour lesquels le rôle de l'OLAF est de contribuer aux enquêtes menées par d'autres services nationaux ou communautaires, en facilitant notamment la collecte et l'échange d'informations. Il n'y a pas d'enquête au sens strict au sein de l'OLAF.
Assistance pénale: dossiers relevant de la compétence légale de l'OLAF où les autorités compétentes d'un État membre mènent une enquête pénale et demandent l'assistance de l'OLAF. Il n'y a pas d'enquête au sens strict au sein de l'OLAF.

6 Quelques modifications peuvent survenir dans le cadre de ces trois phases.

7 Le CEPD a émis un avis sur les opérations de traitement qui se déroulent au cours de la phase d'évaluation et d'enquête en rapport avec des enquêtes internes dans le cadre desquelles un traitement ultérieur des messages conservés dans le SNF peut avoir lieu. Cf. l'avis du CEPD du 23 juin 2006 concernant une notification en vue d'un contrôle préalable relatif aux enquêtes internes de l'OLAF (Dossier 2005-418). Il convient également de souligner que le CEPD a évalué les notifications en vue d'un contrôle préalable liées au traitement de données à caractère personnel par l'OLAF, entre autres dans le cadre d'enquêtes externes, d'affaires classées à première vue, d'affaires classées et de dossiers de suivi.

La ***responsabilité principale du traitement de données*** incombe au conseiller anti-corruption de l'OLAF. Cependant, comme expliqué plus en détail ci-après, les enquêteurs des départements Enquêtes et opérations (différents départements au sein de la Direction A et B) se chargent de certains des traitements de données dans le cadre de l'exploitation du SNF. Par ailleurs, le département Services de l'information (D8) est responsable de plusieurs aspects liés à la gestion et à la maintenance technique du SNF.

Comme décrit plus en détail ci-après, les ***traitements automatiques et manuels de données*** sont étroitement liés et peuvent être décrits globalement comme suit:

Étape 1: Le public peut fournir les informations de deux manières différentes. Premièrement, il peut remplir un questionnaire comprenant un champ de texte libre, auquel il peut également joindre un fichier. Deuxièmement, il peut s'inscrire pour bénéficier de communications bidirectionnelles avec l'OLAF sous forme de messages électroniques transmis au sein du SNF. Dans ces cas, un nom d'utilisateur est généré et communiqué à l'utilisateur, qui est invité à choisir un mot de passe. Le système permet à l'utilisateur de fournir les informations de façon anonyme et constitue un canal de communication sécurisé. De telles communications se présentent généralement sous forme de questions formulées par l'enquêteur responsable de l'OLAF et de réponses fournies par l'utilisateur. Les messages entrants sont sauvegardés automatiquement sur le serveur autonome, qui est géré par le département D.8.

Étape 2: Le contrôle initial des messages au sein du système s'effectue comme suit:

1) Contrôle automatique des questionnaires par le système:

1. S'ils sont totalement dépourvus de contenu (autrement dit si aucun texte libre, aucune pièce jointe ni aucun autre champ n'a été sélectionné), le système génère automatiquement un message signalant à l'utilisateur que le questionnaire n'a pas été soumis.
2. S'ils ne contiennent aucun texte libre ni aucune pièce jointe mais que l'un des autres champs a été sélectionné, alors le système les place dans le "dossier vierge". Le responsable du contrôle (un enquêteur de la Direction A ou B mandaté par son chef d'unité pour contrôler les messages du SNF sur la base de son expérience et de ses connaissances linguistiques) peut soit (i) programmer une suppression, auquel cas ils seront transmis à l'administrateur système[8] (qui peut soit les supprimer définitivement du système, soit les estimer pertinents et les transmettre au chef d'unité responsable du secteur concerné), ou (ii) les juger pertinents et les transmettre au chef d'unité responsable du secteur concerné.
3. Si le système les juge sans intérêt sur la base de statistiques accumulées à partir des messages déjà classifiés, il les place dans le "dossier sans intérêt". Les messages dans ce dossier sont traités de la même manière que les messages dans le "dossier vierge" décrit au paragraphe précédent.

2) Contrôle humain

Les responsables du contrôle analyseront l'ensemble des messages qui n'ont pas été supprimés au cours de la première phase décrite ci-dessus. Le système reconnaît la langue du questionnaire entrant et le transmet automatiquement au responsable du contrôle chargé de cette langue. Celui-ci reçoit par e-mail une notification générée automatiquement l'informant qu'il y a un nouveau

[8] L'administrateur système est responsable de la gestion de l'accès des enquêteurs, du contrôle et de la suppression de messages destinés à être supprimés par les responsables du contrôle, de l'accès aux statistiques générées par le système, et de la vérification des journaux de sauvegarde et de contrôle. Au cours des 12 premiers mois de l'opération, l'administrateur système sera M. S. Knolle, qui travaille sous l'égide du responsable du traitement des données du système.

message dans le système. L'administrateur système fournit à chaque responsable du contrôle un nom d'utilisateur ainsi qu'un mot de passe. Le responsable du contrôle décide si ces informations sont pertinentes ou non. Le questionnaire/message est envoyé par le responsable du contrôle via le système au chef d'unité responsable du secteur concerné (qui reçoit par e-mail une notification l'informant qu'il y a un nouveau message dans le système).

Étape 3: Le contrôle ultérieur du message par le responsable de l'unité pour le secteur concerné par le message se déroule comme suit.

Dès réception, le chef d'unité supprime les messages sans intérêt et transmet les messages pertinents à un enquêteur au sein de son unité. L'enquêteur commence par déterminer si un canal de communication a bien été sélectionné par l'utilisateur. Dans ce cas, l'enquêteur peut activer le canal de communication avec l'utilisateur, et correspondre ainsi avec l'utilisateur via le système par le biais de la boîte aux lettres anonyme. Après réception d'une quelconque information complémentaire par le biais de telles communications, l'enquêteur traite les informations de la même manière que toute information entrante, conformément aux procédures décrites dans le manuel de l'OLAF. Enfin, le chef d'unité décide si le dossier nécessite d'entamer l'étape d'évaluation ou s'il doit être considéré comme une affaire classée à première vue. Si une évaluation est entamée, un numéro CMS est affecté au dossier et l'enquêteur intègre l'ensemble des informations reçues par le biais du système dans le fichier CMS.

Comme c'est le cas avec toute autre information entrante, le chef d'unité compétent peut juger les informations pertinentes pour l'autorité d'un État membre au regard de son travail dans le cadre de la lutte contre la fraude et la corruption portant atteinte aux intérêts financiers de l'UE. Dans ce cas, il transmettra les informations au service de renseignement opérationnel de l'OLAF, qui transmettra le message à l'autorité de l'État membre concerné.

Toutes les informations dans le système sont cryptées et accessibles par un seul membre du personnel de l'OLAF à un moment donné. Les informations reçues ne sont sauvegardées dans le serveur autonome du SNF que durant les trois étapes décrites ci-dessus. Les messages sans intérêt seront définitivement supprimés du système par l'administrateur système. Les messages entraînant une évaluation seront supprimés par l'enquêteur compétent une fois un fichier CMS créé. Au total, les informations seront conservées pendant une période ne dépassant pas un an.

Le traitement de données implique les ***types de personnes concernées*** suivants: *(i)* personnes choisissant d'utiliser le système et de laisser leurs coordonnées et *(ii)* toute personne citée par un utilisateur du système.

En ce qui concerne les catégories de données à caractère personnel, les données à caractère personnel fournies par les utilisateurs du système comprennent la date et l'heure auxquelles ils ont laissé un message, leur pays d'origine et le contenu du message, qui peut également contenir d'autres informations à caractère personnel les concernant. Les données à caractère personnel ainsi recueillies peuvent également inclure l'identité de personnes citées par les utilisateurs du système ainsi que d'autres informations qui sont fonction de chaque message.

En ce qui concerne les ***périodes de conservation,*** les informations qui sont jugées sans intérêt sont supprimées. Une telle suppression peut survenir automatiquement, via le système de classification automatique décrit ci-dessus, ou bien après examen par le responsable du contrôle, l'administrateur système et le chef d'unité responsables du dossier.

Si les données deviennent partie intégrante d'un dossier d'enquête, les informations sont conservées pendant 20 ans, pendant 10 ans si elles sont échangées avec un État membre dans le cadre d'une

assistance mutuelle, pendant 3 ans si elles sont échangées avec un État membre dans le cadre d'irrégularités et pendant 5 ans si elles sont considérées comme une affaire classée.

En ce qui concerne les ***transferts de données,*** le CEPD souligne que les messages ne sont pas transférés en dehors de l'OLAF. Ils peuvent être transférés à des enquêteurs au sein des unités d'enquête et du service de renseignement opérationnel lorsqu'ils sont jugés pertinents pour les États membres, lorsqu'ils deviennent partie intégrante d'un dossier ou si une enquête est ouverte. Les transferts de données pouvant survenir dans ces deux cas ne relèvent pas du traitement mis en œuvre au sein du SNF. Certains de ces traitements de données ont été préalablement contrôlés par le CEPD dans le cadre de la notification des traitements de données effectués dans le cadre d'enquêtes (externes ou internes) ou de dossiers.

En ce qui concerne les ***droits à l'information des personnes concernées***, la notification en vue d'un contrôle préalable fait référence à une déclaration de confidentialité destinée à fournir des informations aux personnes utilisant le SNF.

La déclaration de confidentialité contient des informations sur les finalités du traitement, les destinataires des données, l'existence d'un droit d'accès et de rectification, y compris le nom de la personne à contacter pour faire valoir ces droits. Elle mentionne également les délais de conservation des données et le droit de saisir le contrôleur européen de la protection des données.

En ce qui concerne la manière dont les informations sont fournies aux différentes personnes concernées, il est souligné dans la Notification qu'un lien vers la déclaration de confidentialité figurera sur la page d'accueil du SNF, sur le site de l'OLAF Europe. Ainsi, les utilisateurs du système auront accès à la déclaration de confidentialité lorsqu'ils accèdent au site pour utiliser le système.

Les personnes citées par les utilisateurs du système seront informées comme suit: si les informations sont finalement utilisées dans le cadre d'une enquête de l'OLAF ou d'un dossier, elles deviendront partie intégrante du dossier; ainsi, la personne citée sera informée dans le cadre du dossier, comme stipulé dans les contrôles préalables des différents types de dossiers OLAF. L'information peut être différée si une des exceptions définies dans l'article 20 du règlement (CE) n° 45/2001 est applicable. Si les informations sont jugées sans intérêt et ne deviennent pas partie intégrante d'une enquête ou d'un dossier, aucune donnée à caractère personnel ne sera fournie.
En ce qui concerne le ***droit d'accès et de rectification*** des utilisateurs du SNF, la déclaration de confidentialité stipule que les particuliers disposent de ces droits à l'égard des informations les concernant détenues par l'OLAF. Elle fournit le nom et l'adresse électronique du responsable du traitement qui est la personne à contacter pour exercer ces droits et répondre à toute question complémentaire portant sur le traitement des informations à caractère personnel les concernant. La déclaration de confidentialité ne fait aucune distinction entre les différents types de personnes concernées (personnes citées dans les messages ou personnes ayant laissé les messages).

Le CEPD observe que l'OLAF a mis en œuvre des ***mesures de sécurité***.

2.2. Aspects juridiques

2.2.1. Contrôle préalable

Le règlement (CE) n° 45/2001 (ci-après dénommé "le règlement") s'applique au *"traitement de données à caractère personnel, automatisé en totalité ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier*" ainsi qu'au traitement *"par l'ensemble des institutions et organismes communautaires, dans la*

mesure où un tel traitement est mis en œuvre pour l'exercice d'activités qui relèvent en totalité ou en partie du droit communautaire"[9].

Pour les raisons décrites ci-après, l'exploitation du SNF réunit tous les éléments qui justifient l'application du règlement:

Premièrement, l'exploitation du SNF implique la collecte et le traitement ultérieur de *données à caractère personnel*, définis à l'article 2, point a), du règlement. En effet, comme le précise la Notification, les données à caractère personnel de personnes utilisant le SNF pour laisser des messages sont conservées, comme par exemple l'heure du message vocal, le pays d'origine et le contenu du message. Par ailleurs, le SNF peut également entraîner le traitement de l'identité et autres informations relatives aux personnes citées par les utilisateurs du système.

Deuxièmement, comme le précise la Notification, les données à caractère personnel recueillies sont soumises à des "traitements automatisés", définis à l'article 2, point b), du règlement. Le simple fait de conserver des messages électroniques, ainsi que leur transfert en ligne parmi les enquêteurs de l'OLAF, constitue un exemple de traitement automatisé des données.

Enfin, le CEPD confirme que le traitement est effectué par une institution communautaire, en l'occurrence l'OLAF, l'Office européen de lutte antifraude, qui fait partie de la Commission Européenne, dans le cadre du droit communautaire (article 3, paragraphe 1, du règlement). Ainsi, l'exploitation du SNF réunit clairement tous les éléments qui entraînent l'application du règlement.

Les traitements relèvent-ils de l'article 27 du règlement?

L'article 27, paragraphe 1, du règlement soumet au contrôle préalable du CEPD *"les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités"*. Le paragraphe 2 contient une liste des traitements susceptibles de présenter de tels risques.

Le CEPD estime que la notification concernant le SNF qui lui a été adressée en vue d'un contrôle préalable relève de toute évidence de diverses hypothèses prévues par l'article 27, paragraphe 2, point a), du règlement, stipulant que les traitements liés à des "*suspicions, infractions, condamnations pénales ou mesures de sûreté*" doivent être soumis au contrôle préalable du CEPD. Dans le présent dossier, du fait de la mise en place du SNF, différents services de l'OLAF traiteront des informations pouvant avoir un lien avec des allégations de fraude et autres irrégularités ayant une incidence sur le budget de l'UE ainsi qu'avec des allégations de corruption et autres fautes graves commises par des membres ou le personnel d'institutions européennes. En tout état de cause, le SNF étant un instrument qui permet à l'OLAF de mettre au jour de telles irrégularités et fautes, il recueillera dans certains cas des informations liées à des infractions.

Par ailleurs, le CEPD estime que la notification relève également de l'article 27, paragraphe 2, point b), du règlement, qui mentionne les traitements *"destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur (...) comportement*". Dans le présent dossier, divers aspects de la personnalité des personnes concernées sont évalués de façon systématique, qu'il s'agisse des personnes utilisant le système pour fournir des informations ou des personnes citées par d'autres.

La notification de la déléguée à la protection des données (DPD) de l'OLAF a été reçue le 23 juillet 2007. Conformément à l'article 27, paragraphe 4, du règlement, en raison des demandes

[9] Article 3, paragraphe 2.

d'informations et afin de permettre à la DPD de faire des observations sur le projet d'avis du CEPD, la procédure a été suspendue pendant 65 jours, outre le mois d'août. L'avis sera par conséquent adopté au plus tard le 3 janvier 2008 (le 28 décembre 2007 et les jours suivants n'étant pas des jours ouvrés).

2.2.2. Légitimité du traitement

Les données à caractère personnel ne peuvent être traitées que sur la base des fondements juridiques visés à l'article 5 du règlement.

Comme l'indique la Notification, les traitements notifiés en vue d'un contrôle préalable relèvent de l'article 5, point a), selon lequel les données ne peuvent être traitées que si le traitement est "*nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités*".

Afin de déterminer si les traitements sont conformes à l'article 5, point a), du règlement, il convient de se demander, premièrement, si le traité ou d'autres actes législatifs prévoient les traitements effectués par l'OLAF; deuxièmement, si les traitements sont effectués dans l'intérêt public; et troisièmement, si les traitements sont nécessaires. Evidemment, les trois questions sont étroitement liées.

Fondements juridiques pertinents dans le traité ou dans d'autres actes législatifs. Pour déterminer quels sont les fondements juridiques figurant dans le traité ou dans d'autres actes législatifs qui justifient les traitements effectués dans le cadre de l'exploitation du SNF, le CEPD souligne les points suivants.

Premièrement, il convient de rappeler que le traitement s'inscrit, souvent en tant que première étape, dans le cadre de la collecte d'informations susceptibles d'entraîner l'ouverture d'une enquête. Ainsi, il est expliqué dans la Notification que les fondements juridiques justifiant le traitement effectué durant l'enquête justifient également le traitement effectué avant la phase d'enquête, autrement dit notamment durant la phase d'évaluation préalable, en l'occurrence le traitement effectué dans le cadre du SNF. En ce qui concerne les enquêtes internes, comme souligné dans l'avis du CEPD sur les enquêtes internes effectuées par l'OLAF[10], les fondements juridiques résident principalement dans l'article 4 du règlement 1073/1999 relatif aux enquêtes menées par l'OLAF[11]. L'article 2 de la décision 1999/352 de la Commission instituant l'OLAF[12] est également pertinent. En ce qui concerne les enquêtes externes, les sources juridiques sont multiples. Par exemple, le traitement effectué lorsque l'OLAF ouvre une enquête antifraude horizontale au sujet des dépenses communautaires, directes ou indirectes, et des recettes collectées directement au nom des Communautés (ressources propres traditionnelles) se fonde sur l'article 2 du règlement n° 2185/96[13] du Conseil en liaison avec l'article 3 du règlement n° 1073/99 relatif aux enquêtes effectuées par

[10] Avis de contrôle préalable du 23 juin 2006 sur les enquêtes internes de l'OLAF (dossier 2005-418).

[11] La partie correspondante de l'article 4 du règlement 1073/1999 stipule ce qui suit: "1. Dans les domaines visés à l'article 1, l'Office effectue les enquêtes administratives à l'intérieur des institutions, organes et organismes (ci-après dénommées "enquêtes internes"). (...) 2. Pour autant que les dispositions mentionnées au paragraphe 1 soient respectées: (...), l'Office peut demander des informations orales aux membres des institutions et organes, aux dirigeants des organismes ainsi qu'aux membres du personnel des institutions, organes et organismes. 3. (...) Par ailleurs, l'Office peut demander à toute personne concernée l'information qu'il juge utile pour ses enquêtes."

[12] Cet article stipule ce qui suit: "(...) L'Office est chargé d'effectuer des enquêtes administratives internes destinées : (a) à lutter contre la fraude, la corruption et toute autre activité illégale portant atteinte aux intérêts financiers de la Communauté, (b) à rechercher les faits graves, liés à l'exercice d'activités professionnelles, pouvant constituer un manquement aux obligations des fonctionnaires et agents des Communautés susceptible de poursuites disciplinaires et, le cas échéant, pénales ou un manquement aux obligations analogue des membres des institutions et organes non soumis au statut des fonctionnaires des Communautés européennes ou au régime applicable aux autres agents de ces Communautés. (...)".

[13] Le règlement du Conseil (Euratom, CE) n° 2185/96 relatif aux contrôles et vérifications sur place effectués par la Commission pour la protection des intérêts financiers des Communautés européennes contre les fraudes et autres irrégularités, JO L 292 du 15.11.1996, p. 2. L'article 2 stipule ce qui suit: "La Commission peut procéder à des contrôles et vérifications sur place en application du présent règlement: – soit en vue de la recherche d'irrégularités graves ou transnationales ou d'irrégularités dans lesquelles sont susceptibles d'être impliqués des opérateurs économiques agissant dans plusieurs États membres, – soit en vue de la recherche d'irrégularités, lorsque la situation dans un État membre exige dans un cas particulier le renforcement des contrôles et vérifications sur place afin d'améliorer l'efficacité de la protection des intérêts financiers et ainsi d'assurer un niveau de protection équivalent au sein de la Communauté, – soit à la demande des États membres intéressés".

l'OLAF[14]. Il existe en outre un certain nombre d'actes législatifs sectoriels justifiant le traitement de données dans des secteurs spécifiques, visés à l'article 9, paragraphe 2, du règlement 2988/95 du Conseil relatif à la protection des intérêts financiers des Communautés européennes, qui autorise la Commission à "*effectuer des contrôles et vérifications sur place dans les conditions prévues par les réglementations sectorielles"*. D'autres fondements juridiques s'appliquent à d'autres types de dossiers.

Deuxièmement, le CEPD prend acte de la législation ci-dessus qui autorise l'OLAF à ouvrir des enquêtes (de différentes catégories) pour allégations de fraude, corruption et autres irrégularités portant atteinte à la Communauté. Il convient avec l'OLAF que ces actes législatifs constituent également une base juridique appropriée, selon l'article 5, point a), pour justifier la collecte et le traitement ultérieur de données à caractère personnel dans le cadre du SNF. Comme l'indique la Notification, le traitement effectué dans le cadre du SNF *"fait partie de la collecte initiale d'informations pouvant entraîner l'ouverture d'une enquête"*. L'OLAF étant tenu d'enquêter sur les irrégularités graves, il semble approprié qu'il ait recours à des instruments tels que le SNF, qui permet à des informateurs ou des témoins de lui divulguer des informations, et ainsi l'aider à lutter contre la fraude, la corruption et autres irrégularités.

Les traitements sont effectués dans l'intérêt public. Le CEPD souligne que l'OLAF effectue les traitements dans l'exercice légitime de son autorité publique. En effet, les articles 9 et 10, en liaison avec les articles 4 et 5, du règlement (CE) n° 1073/1999 et la décision 1999/352 de la Commission instituant l'OLAF confèrent à ce dernier la compétence et l'obligation d'ouvrir des enquêtes et de garantir la bonne mise en œuvre de leurs dispositions en coopération avec les autorités nationales et communautaires compétentes.

Test de nécessité. Conformément à l'article 5, point a), du règlement, le traitement de données doit être *"nécessaire à l'exécution d'une mission*", comme indiqué ci-dessus. Il est donc pertinent de déterminer si le traitement de données effectué dans le cadre du SNF est pertinent pour l'exécution d'une mission.

Á cet effet, il convient de déterminer en premier lieu si la mise en place du SNF peut en soi s'avérer nécessaire à l'exécution d'une mission. Pour répondre à cette question, il est utile de rappeler que la principale compétence ou mission de l'OLAF consiste à mener des enquêtes en vue de lutter contre diverses malversations susceptibles de porter atteinte aux intérêts financiers de la Communauté. Le CEPD est conscient que la capacité de l'OLAF à exécuter efficacement sa mission dépend entre autres de sa capacité à recueillir et recevoir des informations susceptibles de révéler l'existence de malversations, qui doit pouvoir intervenir pendant toute la durée d'une enquête éventuelle, autrement dit depuis la phase d'évaluation préalable jusqu'à la phase de suivi. Le CEPD considère donc le SNF comme un instrument nécessaire qui aide l'OLAF au cours de la phase de collecte des informations initiales. Le SNF peut être considéré comme l'équivalent d'autres instruments servant également à signaler des fraudes présumées et, à ce titre, il s'avère tout aussi nécessaire que les autres instruments décrits sur le site Web de l'OLAF, y compris la possibilité donnée au public d'envoyer des courriels et des courriers pour informer l'OLAF de l'existence d'une éventuelle malversation ou d'utiliser le service d'appel gratuit de l'OLAF.

Après avoir examiné la nécessité du SNF proprement dit, il est important de souligner qu'il faut également examiner concrètement la "nécessité" de traiter les données dans chaque cas spécifique et, en l'occurrence, lors de chaque utilisation spécifique du SNF. Dans cette perspective, il convient de garder à l'esprit que le traitement de données à caractère personnel qu'il y a lieu d'effectuer dans le cadre du traitement des informations reçues par le SNF doit être proportionnel à la finalité générale du traitement (lutte contre la fraude, la corruption, etc.) et à la finalité spécifique du

[14] "L'Office fera valoir les pouvoirs conférés à la Commission en vertu du règlement (Euratom, CE) n° 2185/96 en vue de procéder à des contrôles et vérifications sur place dans les États membres et, conformément aux accords de coopération en vigueur, dans des pays tiers".

traitement effectué dans le cadre du dossier à l'étude. La proportionnalité doit dès lors être évaluée au cas par cas. Il conviendrait par exemple de ne pas conserver les informations qui, de toute évidence, ne relèvent pas de la compétence de l'OLAF et qui ne l'aideraient pas à atteindre ses objectifs.

2.2.3. Traitement de catégories spéciales de données

Le service de notification des fraudes ayant pour finalité de faciliter la collecte d'informations au sujet de malversations alléguées portant atteinte aux intérêts financiers de la Communauté, ces informations devraient se rapporter dans un certain nombre de cas à des infractions, des condamnations pénales ou des mesures de sûreté. À cet égard, le CEPD rappelle l'article 10, paragraphe 5, du règlement, qui stipule que *"le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que s'il est autorisé par les traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités ou, si cela s'avère nécessaire, par le contrôleur européen de la protection des données"*. Dans le présent dossier, le traitement des données mentionnées est autorisé par les actes législatifs visés au point 2.2.2 ci-dessus.

En ce qui concerne les catégories spéciales de données, l'article 10, paragraphe 1, du règlement stipule que "*le traitement des données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé ou à la vie sexuelle sont interdits*". Compte tenu de l'objectif global poursuivi par l'OLAF lorsqu'il effectue un traitement de données, le CEPD présume que l'OLAF n'a pas l'intention de collecter de telles catégories de données à caractère personnel.

2.2.4. Qualité des données

Conformément à l'article 4, paragraphe 1, point c), du règlement, les données à caractère personnel doivent être *"adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et/ou traitées ultérieurement"*. C'est ce que l'on appelle le principe de la qualité des données.

Le CEPD observe que c'est aux personnes utilisant le SNF qu'il revient de décider quelles sont les informations qu'elles souhaitent fournir à l'OLAF: elles peuvent fournir des informations adéquates et pertinentes, mais aussi des informations qui ne présentent absolument aucun intérêt au regard des finalités du SNF et des compétences globales de l'OLAF. D'autre part, l'OLAF dispose de différents moyens pour éviter ou minimiser cet état de fait. L'OLAF peut par exemple indiquer quel est le type d'informations pertinentes et relevant de ses compétences dans la section de son site Web consacré au SNF, comme c'est le cas pour le service d'appel gratuit de l'OLAF. Par ailleurs, dans toute correspondance entretenue via des messages électroniques, les enquêteurs de l'OLAF devraient éviter de poser des questions pouvant inciter les informateurs à divulguer des informations sans intérêt pour la détection de cas de fraude et de corruption portant atteinte aux intérêts financiers de la Communauté. Les données à caractère personnel traitées dans ce cadre doivent se limiter aux données strictement et objectivement nécessaires pour vérifier les allégations. Les enquêteurs de l'OLAF devraient être informés de cette règle.

Lorsqu'une personne laisse un message comportant des informations sans intérêt au regard des finalités qui sont en jeu, ces informations ne devraient pas être conservées. A cet égard, le CEPD salue la pratique de l'OLAF consistant à supprimer sur-le-champ les messages inappropriés et inutiles, en observant dans tous les cas une période de conservation maximale d'un an.

Outre ce qui précède, il est important de rappeler que l'article 4, paragraphe 1, point d), du règlement stipule que les données à caractère personnel doivent être *"exactes et, si nécessaire, mises à jour"* et que *"toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées"*. Ce principe est étroitement lié à l'exercice du droit d'accès, de la rectification, du verrouillage et de la suppression (cf. le point 2.2.7 ci-après). Bien entendu, si des efforts ont été consentis pour que les données à caractère personnel soient fiables et complètes, les demandes de rectification seront probablement moins nombreuses.

Garanties pour les dénonciateurs et les informateurs. La législation communautaire ne prévoit pas de cadre juridique pour les informateurs qui, en principe, ne bénéficient pas de la même garantie que les fonctionnaires et autre personnel de l'UE qui fourniraient des informations à l'OLAF. Dans ce cadre, l'OLAF a adopté une politique qui consiste à garantir la confidentialité de l'identité des informateurs jusqu'à ce que les informations soient transmises aux autorités judiciaires nationales, qui ne donnent pas une telle garantie. En ce qui concerne le droit à la confidentialité qui s'applique aux fonctionnaires et au personnel de l'UE, le CEPD constate que le cadre juridique de l'UE n'est pas très clair: il est question du droit à la confidentialité dans une communication de la Commission qui prévoit des mesures spécifiques pour garantir une protection optimale aux membres du personnel qui recourent de façon appropriée aux procédures de dénonciation; une de ces dispositions prévoit que *"toute information relative à l'identité du dénonciateur sera traitée de façon confidentielle"*[15]. Toutefois, ce droit n'a pas été consacré dans un acte législatif contraignant. Comme indiqué dans l'avis du CEPD concernant les enquêtes internes[16], le CEPD estime que la confidentialité de l'identité des dénonciateurs et des informateurs devrait être garantie pendant toute la durée d'une affaire, depuis la phase d'évaluation préalable jusqu'aux phases d'évaluation et d'enquête, dans la mesure où cela ne va pas à l'encontre des règles nationales régissant les procédures judiciaires. À cet effet, le CEPD recommande, dans son avis concernant la proposition de règlement modifiant le règlement (CE) n° 1073/1999 relatif aux enquêtes effectuées par l'OLAF[17], que celle-ci comporte un nouveau paragraphe garantissant la confidentialité de l'identité des dénonciateurs.

2.2.5. Conservation des données

Conformément à l'article 4, paragraphe 1, point e), du règlement, les données à caractère personnel peuvent 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 sont collectées et/ou traitées ultérieurement"*.

En ce qui concerne la politique de conservation dans le cadre du SNF, il convient de distinguer deux règles différentes: une pour les messages sans intérêt et une pour les messages pertinents. Si les informations sont jugées sans intérêt, elles sont supprimées peu après cette évaluation, ce qui peut se faire à différents moments: par l'administrateur système (suivant la proposition du responsable du contrôle) ou après vérification par l'unité d'enquête. Un message sans intérêt peut être conservé pendant un an au maximum.

Le CEPD estime que l'intention qu'a l'OLAF de supprimer les messages sans intérêt tout de suite après cette évaluation est positive. Il encourage par ailleurs l'OLAF à réduire autant que possible la

---

15 (SEC/2004/151/2) du 6 février 2004 du vice-président Kinnock.

16 Avis du 23 juin 2006 concernant une notification en vue d'un contrôle préalable reçue du délégué à la protection des données de l'Office européen de lutte antifraude (OLAF) à propos des enquêtes internes (dossier 2005-418).

17 Avis du 27 octobre 2006 concernant la proposition de règlement modifiant le règlement (CE) n° 1073/1999 relatif aux enquêtes effectuées par l'Office européen de lutte antifraude (OLAF).

période de conservation maximale pour ce type de données, qui ne pourra dans tous les cas dépasser un an.

Si les informations sont jugées pertinentes et font donc partie d'un dossier d'enquête, elles sont conservées pendant une période de 20 ans, de 10 ans si elles sont échangées avec un État membre dans le cadre d'une assistance mutuelle, de 3 ans si elles sont échangées avec un État membre dans le cadre d'irrégularités et de 5 ans si elles sont considérées comme une affaire classée. Le présent avis n'aborde pas l'adéquation de telles périodes de conservation des données étant donné que le CEPD a déjà analysé les périodes de conservation de données des traitements effectués par les unités d'enquête dans différents avis correspondant à chaque type de dossier ou enquête. Par exemple, le CEPD a émis des avis comportant une appréciation des périodes de conservation de données mises en œuvre pour des enquêtes internes ainsi que des dossiers de contrôle[18].

2.2.6. Transfert de données

Les articles 7, 8 et 9 du règlement prévoient certaines obligations qui s'appliquent lorsque les responsables du traitement transfèrent des données à caractère personnel à des tiers. Les règles diffèrent selon que les données sont transférées à des institutions ou organes communautaires conformément à l'article 7, à des destinataires visés par la directive 95/46 conformément à l'article 8, ou à d'autres types de destinataires conformément à l'article 9.

Les faits décrits dans la Notification révèlent que le transfert des informations recueillies dans le cadre du SNF est limité à d'autres unités au sein de l'OLAF; l'article 7 du Règlement s'applique par conséquent. Les messages sont notamment transférés aux unités d'enquête de l'OLAF de la Direction A et B en vue de leur analyse ultérieure. Le rôle de ces unités peut être considéré comme un rôle de sous-traitant qui se charge de certaines missions au nom du responsable du traitement. Les messages sont également transférés aux unités d'enquête de l'OLAF et aux services de renseignement opérationnel, qui peuvent les transférer à leur tour aux États membres s'ils sont jugés pertinents pour d'autres organes communautaires ou nationaux.

Transferts aux unités d'enquête de l'OLAF. L'article 7 du règlement stipule que les données à caractère personnel doivent être transférées "*aux fins de l'exécution légitime de missions relevant de la compétence du destinataire"*. Les transferts d'informations aux unités d'enquête de la Direction A et B en vue de leur analyse ultérieure semblent respecter cette disposition dans la mesure où *(i)* le destinataire dispose des compétences appropriées pour exécuter l'analyse ultérieure et *(ii)* le transfert est nécessaire afin de vérifier si les informations révèlent l'existence d'une malversation. Il en va de même pour les transferts aux unités d'enquête de l'OLAF et aux services de renseignement opérationnel.

Transferts aux autorités des États membres. Dans le cadre du traitement ultérieur des informations, les unités d'enquête de l'OLAF et les services de renseignement opérationnel enverront les informations à des tiers ainsi qu'à des destinataires visés ou non par la directive 95/46. Le CEPD estime que ces transferts ultérieurs doivent être considérés comme ne relevant pas du traitement de données effectué dans le cadre du SNF; ils ne relèvent donc pas du présent avis. Ces transferts ultérieurs ont lieu dans le cadre des traitements de données incombant à ces autres unités. De tels traitements ont fait l'objet d'un contrôle préalable du CEPD et seront pris en compte dans ces

[18] Voir avis du CEPD du 23 juin 2006 concernant une notification relative à un contrôle préalable à propos des enquêtes internes effectuées par l'OLAF (dossier 2005-418) et avis sur une notification en vue d'un contrôle préalable adressée par le délégué à la protection des données de l'Office européen antifraude concernant les opérations de traitement des données de "suivi" (disciplinaire, administratif, judiciaire, financier) - Bruxelles, le 26 mars 2007 (dossiers 2006/0543, 2006/0544, 2006/0545, 2006/0546, 2006/0547).

contextes[19] ou sont en cours de traitement dans le cadre des dossiers 2005-154 et 2006-493, le CEPD analysant la conformité des transferts internationaux de données de l'OLAF.

2.2.7. Droit d'accès et de rectification

Le droit d'accès est le droit de la personne concernée d'être informée de toute donnée la concernant qui est traitée par le responsable du traitement. Conformément à l'article 13 du règlement, la personne concernée a le droit d'obtenir, sans contrainte, du responsable du traitement une communication sous une forme intelligible des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données. Les informations peuvent donc être obtenues directement par la personne concernée ("accès direct") ou, dans certaines circonstances, par une autorité publique ("accès indirect", généralement exercé par une autorité chargée de la protection des données, en l'occurrence le CEPD dans le cadre du présent dossier).

Comme indiqué ci-dessus, pour évaluer si le contrôleur de données accorde bien en l'espèce le droit à l'information, il convient de distinguer deux types de personnes concernées: premièrement, les personnes qui utilisent le SNF et choisissent de fournir des données les concernant; et deuxièmement, toute personne citée par un utilisateur du SNF.

En ce qui concerne le droit d'accès et de rectification des personnes qui appellent le SNF, la déclaration de confidentialité indique que ces personnes jouissent d'un tel droit à l'égard des informations détenues par l'OLAF à leur sujet. Elle fournit le nom et l'adresse électronique du responsable du traitement en tant que personne à contacter pour exercer ces droits et à laquelle s'adresser pour poser toute question supplémentaire concernant le traitement des données à caractère personnel les concernant. La pratique telle que décrite dans la déclaration de confidentialité est conforme à l'article 13 du règlement.

La Notification ne parle pas du droit d'accès ou de rectification des personnes citées par les utilisateurs du SNF. Le CEPD rappelle qu'en vertu de l'article 13 du règlement, ces personnes ont le droit d'accéder aux informations les concernant et de les rectifier et peuvent demander à l'OLAF de faire respecter ces droits. Toutefois, ceux-ci peuvent être restreints si une des conditions prévues aux points a), b) et c) de l'article 20 du règlement s'applique. Dans son avis sur les dénonciations, le groupe de l'article 29 indique que l'exercice de ces droits "*peut être restreint afin d'assurer la protection des droits et des libertés d'autres personnes impliquées dans le système*", ce qui est l'hypothèse prévue au point c) (cf. le point 2.2.8 ci-dessous).

Dans le cadre de l'exercice du droit d'accès, le CEPD souhaite mettre en évidence les recommandations du groupe de l'article 29 selon lesquelles: *"En aucun cas la personne mise en cause dans le signalement d'un dénonciateur ne saurait obtenir du système des informations sur l'identité du dénonciateur en invoquant son droit d'accès, sauf si le dénonciateur fait une fausse déclaration à des fins malveillantes. Dans tous les autres cas, la confidentialité de l'identité du dénonciateur doit toujours être garantie".*

Afin d'assurer le respect de ce qui précède, le CEPD recommande que, une fois l'accès accordé, les informations à caractère personnel sur des tiers, tels que des informateurs ou des dénonciateurs, soient supprimées. Si l'accès, y compris dans le cas où les données à caractère personnel sont effacées, est susceptible de divulguer des données à caractère personnel relatives à des tiers (tels que des informateurs ou des dénonciateurs), cet accès devrait être refusé.

[19] Ces transferts peuvent par exemple être réalisés dans le cadre d'enquêtes internes, qui ont fait l'objet d'un avis que le CEPD a rendu le 23 juin 2006 au sujet des enquêtes internes (dossier 2005-418). D'autres peuvent être réalisés dans le cadre d'enquêtes externes ou de dossiers de contrôle, qui font actuellement l'objet d'une analyse de la part du CEPD à la suite de leur notification par le DPD de l'OLAF en vue d'un contrôle préalable.

2.2.8. Information de la personne concernée

Conformément aux articles 11 et 12 du règlement, les personnes qui recueillent des données à caractère personnel sont tenues d'informer les individus auxquels ces données se rapportent de la collecte et du traitement de données les concernant. Ces individus ont en outre le droit d'être informés notamment des finalités du traitement, des destinataires des données et de leurs droits spécifiques en tant que personnes concernées.

Le CEPD a vérifié le contenu des informations fournies dans la déclaration de confidentialité et estime qu'il est conforme aux dispositions des articles 11 et 12 du règlement. La déclaration contient en effet des informations sur les finalités du traitement, les destinataires des données, l'existence d'un droit d'accès et de rectification, ainsi que le nom de la personne à contacter pour faire valoir de tels droits. Elle précise également les périodes maximales de conservation des données et le droit de saisir le contrôleur européen de la protection des données.

Outre l'évaluation du contenu de la déclaration de confidentialité, il convient également de déterminer de quelle manière les informations sont fournies et si elles sont fournies à *l'ensemble* des personnes concernées dont les données à caractère personnel sont recueillies dans le cadre du SNF. À cet égard, il convient de distinguer à nouveau deux types de personnes concernées: premièrement, les personnes qui utilisent le SNF et choisissent de fournir des données à caractère personnel les concernant; et deuxièmement, toute personne citée par une personne qui utilise le système.

Informations fournies aux personnes qui utilisent le SNF et choisissent de fournir des données à caractère personnel les concernant. La Notification mentionne une déclaration de confidentialité destinée à fournir des informations aux personnes utilisant le SNF. Un lien vers la déclaration de confidentialité figurera sur la page d'accueil du SNF, sur le site de l'OLAF Europe.

Il est difficile de connaître précisément l'endroit où la déclaration de confidentialité sera disponible. Afin de s'assurer que les personnes qui utilisent le SNF soient effectivement informées, le lien vers la déclaration de confidentialité devrait être directement accessible sur la page Web par le biais de laquelle les visiteurs souhaitant utiliser le SNF doivent obligatoirement passer, ou bien de façon très visible tout de suite après ou avant d'accéder aux informations sur le SNF. Outre l'inclusion de la déclaration de confidentialité sur la page donnant des informations sur l'utilisation du SNF, un lien vers cette déclaration pourrait également être prévu dans le questionnaire en ligne et/ou dans toute correspondance électronique avec les informateurs. D'autres techniques, comme l'utilisation de fenêtres contextuelles, peuvent également être examinées, à condition que le contenu de ces fenêtres puisse être imprimé et conservé en vue d'une utilisation ultérieure.

Informations fournies à toute personne citée par un utilisateur du service de notification des fraudes. Comme indiqué ci-dessus, le traitement réalisé dans le cadre du SNF ne concerne pas uniquement les personnes qui utilisent le SNF, mais également celles qui sont citées par les utilisateurs du SNF. Selon la Notification, les personnes dont le nom est cité par les informateurs et utilisé dans le cadre d'une enquête de l'OLAF ou d'un autre dossier seront informées dans le cadre du dossier. Cependant, la Notification stipule que "*si les informations sont supprimées car jugées sans intérêt et ne sont pas devenues partie d'un dossier, il n'est par conséquent pas nécessaire de fournir les informations à une personne citée sur une base individuelle*".

Le CEPD rappelle que, conformément à l'article 12 du règlement, les personnes dont le nom est cité par des individus qui utilisent le SNF ont le droit d'être informées sur le traitement des données les concernant. En l'occurrence, les informations concernant toute personne dont le nom est cité par des individus utilisant le SNF et étant finalement jugées sans intérêt peuvent être soumises à un véritable traitement. En effet, alors que certaines informations seront automatiquement supprimées dès leur arrivée au moyen d'un système de classification automatique, d'autres

messages/informations seront transmis dans un premier temps aux responsables du contrôle, puis aux enquêteurs de la Direction A et B en vue d'une confirmation finale de leur pertinence. Les informations peuvent être traitées, visualisées, lues et analysées par un certain nombre d'enquêteurs de ces Directions. Par ailleurs, globalement, ce processus peut prendre jusqu'à un an, période durant laquelle les informations relatives à cette personne seront conservées par l'OLAF. Ainsi, en ce qui concerne les informations qui ne sont pas supprimées automatiquement à leur arrivée, sauf en cas d'exception (cf. ci-dessous), aucun fondement juridique ne semble justifier le défaut d'information des personnes concernées.

L'existence d'une obligation similaire dans la directive sur la protection des données a été soulignée par le groupe de l'article 29 dans l'avis qu'il a rendu sur les mécanismes de dénonciation[20]: "*La personne mise en cause dans le signalement d'un dénonciateur sera informée par la personne chargée du mécanisme dans les plus brefs délais après l'enregistrement des données la concernant*". L'OLAF devrait veiller au respect de cette obligation.

Ce même avis stipule que "*lorsqu'il y a un risque sérieux que cette notification compromette la capacité de la société d'enquêter efficacement sur les faits allégués ou de collecter les preuves nécessaires, l'information de la personne mise en cause peut être retardée aussi longtemps que ce risque existe. Cette exception à la règle de l'article 11 vise à sauvegarder les preuves en empêchant leur destruction ou leur modification par la personne mise en cause. Elle doit s'appliquer de manière restrictive, au cas par cas, et doit tenir compte des intérêts plus larges qui sont en jeu".* L'article 20 du règlement prévoit le même type d'exceptions, qui sont soumises à des conditions similaires. Il prévoit en particulier certaines limitations au droit à l'information, notamment lorsqu'une telle limitation constitue une mesure nécessaire pour *"a) assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales; b) sauvegarder un intérêt économique ou financier important d'un État membre ou des Communautés européennes, y compris dans les domaines monétaire, budgétaire et fiscal; c) garantir la protection de la personne concernée ou des droits et libertés d'autrui".*

Dans le présent dossier, l'article 20 autorise l'OLAF à restreindre la fourniture d'informations afin de sauvegarder les intérêts visés aux points a), b) et c). En pratique, cela signifie que, lorsque les informations sont jugées pertinentes ou sans intérêt, l'OLAF doit évaluer si l'information de la personne citée par l'utilisateur du SNF serait de nature à compromettre les valeurs susmentionnées visées aux points a), b) et c) de l'article 20, auquel cas elle pourra être limitée. En particulier, si les informations sont jugées pertinentes, l'OLAF pourrait, dans certains cas, se prévaloir de l'article 20, point a). Lorsque les informations sont jugées sans intérêt, le CEPD s'interroge, pour la plupart des cas, sur le recours aux exceptions prévues aux points a) et b): dans ces circonstances, il n'y a en principe ni enquête à proprement parler ni intérêt financier en jeu. Par contre, l'OLAF peut invoquer le point c) s'il estime nécessaire de limiter l'information afin de garantir "*la protection de la personne concernée ou des droits et libertés d'autrui*", par exemple s'il considère que la divulgation d'informations peut révéler l'identité du dénonciateur ou de l'informateur, ce qui peut être le cas dans un certain nombre de dossiers. Pour déterminer s'il est tenu de fournir des informations ou si une exception s'applique, l'OLAF doit réaliser une évaluation au cas par cas des circonstances qui entourent le traitement des données en jeu.

Si l'OLAF se prévaut d'une exception pour limiter l'information, il ne devrait pas perdre de vue que les limitations d'un droit fondamental ne peuvent être appliquées de manière systématique. L'OLAF

[20] Avis 1/2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière, WP 117, adopté le 1er février 2006. D'après le Groupe de l'article 29, la personne doit être informée sur "[1] l'entité responsable du mécanisme de dénonciation, [2] les faits dont elle est accusée, [3] les directions ou services qui pourraient recevoir le signalement au sein de sa société ou d'autres entités ou sociétés du groupe dont sa société fait partie, et [4] la manière d'exercer ses droits d'accès et de rectification".

doit évaluer dans chaque cas si les conditions sont réunies pour appliquer une des exceptions prévues, par exemple, à l'article 20, paragraphe 1, point a) ou c). Par ailleurs, comme l'indique l'article 20, la mesure doit être "nécessaire". Pour ce faire, il faut que le "test de nécessité" soit réalisé au cas par cas. Par exemple, si l'OLAF souhaite invoquer l'exception prévue au point b), il doit déterminer s'il est nécessaire de suspendre l'information afin de sauvegarder un intérêt économique important. Dans le cadre de cette évaluation, l'OLAF ne doit pas perdre de vue que l'intérêt économique en jeu ne justifie pas en soi la nécessité de suspendre l'information. En d'autres termes, il doit exister un lien évident entre la nécessité de suspendre l'information et la sauvegarde d'un intérêt économique. Si l'OLAF fait valoir une exception, il doit le faire dans le respect de l'article 20, paragraphe 3, aux termes duquel *"la personne concernée est informée, conformément au droit communautaire, des principales raisons qui motivent cette limitation et de son droit de saisir le contrôleur européen de la protection des données*". Toutefois, l'OLAF peut reporter la fourniture de ces informations en se prévalant de l'article 20, paragraphe 5, aux termes duquel *"la fourniture des informations visées aux paragraphes 3 et 4 peut être reportée aussi longtemps qu'elle prive d'effet la limitation imposée sur la base du paragraphe 1".*

2.2.9. Mesures de sécurité

Le CEPD constate que l'OLAF a mis en œuvre certaines mesures de sécurité dans le but de prévenir la divulgation et l'accès non autorisés, la destruction, la perte et le traitement illégal des données. Afin d'assurer une approche cohérente de ces mesures de sécurité, le CEPD a décidé de les analyser de manière horizontale plutôt que dans le cadre de chaque notification de contrôle préalable. Par conséquent, le présent avis ne porte pas sur les mesures de sécurité, qui ont été analysées dans un autre avis exclusivement consacré à la question, avis qui a abouti à des conclusions positives.

3. Conclusion

Rien ne porte à croire à une violation des dispositions du règlement 45/2001, à condition que les considérations énoncées dans cet avis soient pleinement prises en compte. L'OLAF doit en particulier garder à l'esprit les points suivants:

- Lorsqu'une personne laisse un message comportant des informations sans intérêt au regard des finalités qui sont en jeu, ces informations ne devraient pas être conservées. Les enquêteurs devraient être informés de cette règle.
- Dans toute correspondance entretenue via des messages électroniques, les enquêteurs de l'OLAF devraient éviter de poser des questions qui porteraient les informateurs à divulguer des informations sans intérêt pour la détection de cas de fraude ou de corruption portant atteinte aux intérêts financiers de la Communauté. Les enquêteurs de l'OLAF devraient être informés de cette règle.
- Il devrait y avoir sur le site Web sur lequel le service de notification des fraudes est disponible une description du type d'informations pertinentes pour l'OLAF afin de minimiser la fourniture d'informations sans intérêt.
- Dans la mesure du possible, la confidentialité de l'identité des informateurs devrait être garantie pendant toute la durée d'une affaire, dans la mesure où cela ne va pas à l'encontre des règles nationales régissant les procédures judiciaires.
- La période de conservation d'informations sans intérêt devrait être aussi brève que possible, et dans tous les cas ne pas dépasser un an.
- Un lien devrait être inséré dans la déclaration de confidentialité figurant à la page Web par le biais de laquelle les visiteurs souhaitant utiliser le service de notification des fraudes doivent obligatoirement passer ou, de manière très visible, tout de suite après ou

avant d'accéder aux informations sur le service de notification des fraudes. Par ailleurs, un lien vers la déclaration de confidentialité devrait également être inséré dans le questionnaire en ligne et/ou dans toute correspondance électronique avec les informateurs.

- Il convient de veiller à ce que les personnes qui ont été citées par les utilisateurs du service de notification des fraudes puissent exercer leur droit à l'information, sous réserve de l'application des exceptions prévues à l'article 20 du règlement. L'OLAF doit décider au cas par cas si les exceptions s'appliquent. Cela vaut également pour les personnes qui ont été citées dans des messages jugés sans intérêt.
- Le CEPD invite l'OLAF à veiller à ce que les personnes citées par les utilisateurs du service de notification des fraudes puissent exercer leur droit d'accès et de rectification. Il rappelle que les exceptions prévues à l'article 20 du règlement peuvent s'appliquer dans certains cas.

Bruxelles, le 18 décembre 2007

(signé)

Peter HUSTINX
Contrôleur européen de la protection des données