

Avis sur une notification en vue d'un contrôle préalable adressée par la déléguée à la protection des données de l'Office européen de lutte antifraude concernant le système d'alerte précoce

Bruxelles, le 4 octobre 2007 (dossier 2007-243)

1. Procédure

Le 30 mars 2007, le Contrôleur européen de la protection des données (ci-après "CEPD") a reçu une notification en vue d'un contrôle préalable adressée par la déléguée à la protection des données (ci-après "DPD") de l'Office européen de lutte antifraude (ci-après "OLAF") concernant le traitement de données préalable à l'établissement d'une demande de signalement dans le cadre du système d'alerte précoce (ci-après "SAP"). Le CEPD a demandé des informations complémentaires le 10 mai 2007; la DPD y a répondu le 3 juillet. Un courrier électronique a été envoyé pour proroger le délai d'un mois, en raison de la complexité du dossier. La procédure a été suspendue pendant 11 jours pour permettre à la DPD de présenter des observations.

Le SAP en tant que tel a déjà fait l'objet d'un contrôle préalable du CEPD¹. Le traitement visé par la présente notification porte sur le rôle spécifique joué par l'OLAF dans le SAP.

2. Les faits

Conformément à l'article 95 du règlement (CE, Euratom) n° 1605/2002 du Conseil du 25 juin 2002 portant règlement financier applicable au budget général des Communautés européennes (ci-après dénommé "le règlement financier"), une base de données centrale doit être créée et gérée par la Commission, dans le respect de la réglementation communautaire relative à la protection des données à caractère personnel. La base de données centrale doit contenir des informations détaillées concernant les candidats et les soumissionnaires qui sont dans l'une des situations visées à l'article 93, à l'article 94 ou à l'article 96, paragraphe 1, point b), et paragraphe 2, point a), du règlement financier.

Comme indiqué à l'article 1^{er}, paragraphe 2, de la décision n° C(2004) 193/3 de la Commission relative au système d'alerte précoce, telle que modifiée, en dernier lieu, par les règles internes 2007 (ci-après dénommée "la décision relative au SAP"), le SAP vise à assurer la circulation d'informations de diffusion restreinte concernant les tiers qui pourraient représenter une menace pour les intérêts financiers et la réputation des Communautés ou pour tout autre fonds géré par elles, si la Commission a des chances raisonnables de nouer ou a déjà noué avec eux des relations contractuelles ou conventionnelles. Les informations peuvent également inclure des cobénéficiaires/cocontractants en cas de procédures d'octroi de subventions ou d'attribution de marchés à des bénéficiaires/contractants multiples ainsi que leurs sous-traitants et les personnes

¹ Avis sur une notification en vue d'un contrôle préalable adressée par le délégué à la protection des données de la Commission concernant le système d'alerte précoce (n° de dossier CEPD: 2005-120).

physiques ayant le pouvoir de représentation, de décision ou de contrôle sur les personnes morales concernées.

En ce qui concerne la fonction de l'OLAF dans le cadre du SAP, il convient de distinguer deux rôles:

- En tant qu'organe d'enquête, l'OLAF peut fournir des informations conduisant à des signalements W1a et W1b conformément à l'article 2, paragraphes 1 et 2, de la décision relative au SAP, et à des signalements W2a et W3b conformément aux articles 3 et 4 de ladite décision.
- Comme les autres DG de la Commission européenne, l'OLAF est habilité à prendre l'initiative de différents signalements qui ne relèvent pas des compétences que lui confère sa qualité d'organe d'enquête. Ces signalements ne sont pas analysés dans le présent avis. La relation qu'a l'OLAF avec le SAP en tant que "Direction générale normale" de la Commission européenne a déjà fait l'objet d'un contrôle préalable² du CEPD. L'accès aux signalements ne relève pas non plus du champ d'application du présent avis.

Conformément à l'article 2, paragraphe 1, de la décision relative au SAP, selon la nature des données et du signalement, les informations se répartissent dans le SAP en cinq catégories de signalements représentant un risque croissant, désignés par les sigles W1 à W5.

1. Un signalement W1 est introduit lorsque des informations donnent des raisons suffisantes de penser que des fraudes, des erreurs administratives graves ou d'autres irrégularités seront enregistrées contre des tiers. L'OLAF intervient dans deux catégories de signalements W1:
 - W1a: C'est à l'OLAF (au niveau du directeur général ou d'un directeur) qu'incombe la responsabilité de demander l'activation d'un signalement W1a par le service visé à l'article 8, après information du ou des OD³ concernés, lorsque ses enquêtes donnent, à un stade précoce, des raisons suffisantes de penser que des erreurs administratives graves ou des fraudes seront constatées en rapport avec un tiers bénéficiant ou ayant bénéficié de fonds communautaires.
 - W1b: C'est à l'OLAF et au Service d'audit interne (SAI) (dans ces deux cas au niveau du directeur général ou d'un directeur) qu'incombe la responsabilité de demander l'activation d'un signalement W1b, après information du ou des OD concernés, lorsque leurs enquêtes (OLAF) ou audits (SAI) donnent des raisons suffisantes de penser que des erreurs administratives graves ou des fraudes seront constatées de manière définitive en rapport avec un tiers bénéficiant ou ayant bénéficié de fonds communautaires.
2. Un signalement W2 est introduit lorsque des tiers sont visés par des constatations de graves erreurs administratives ou de fraudes. L'OLAF intervient dans les signalements W2a:
 - W2a: C'est à l'OLAF et au SAI (dans les deux cas au niveau du directeur général ou d'un directeur) qu'incombe la responsabilité de demander l'activation d'un signalement W2a lorsque leurs enquêtes les amènent à constater de graves erreurs administratives ou des fraudes impliquant un tiers.
3. Un signalement W3 est introduit lorsque des tiers font l'objet d'une action en justice. L'OLAF intervient dans les signalements W3b:

² Voir la note de bas de page 1.

³ Les acronymes "OD" et "OSD" désignent respectivement les ordonnateurs délégués et les ordonnateurs subdélégués.

- W3b: L'OD (ou l'OSD ayant rang de directeur) demande l'activation d'un signalement W3b lorsqu'il apprend que des tiers, en particulier si ces derniers bénéficient ou ont bénéficié de fonds communautaires relevant de sa responsabilité, font l'objet de poursuites judiciaires en raison d'erreurs administratives graves ou de fraudes. Lorsque des poursuites judiciaires sont engagées à la suite des enquêtes de l'OLAF ou font l'objet d'une assistance ou d'un suivi par l'OLAF, celui-ci (au niveau du directeur général ou d'un directeur) demande l'activation du signalement W3b correspondant.

Procédure conduisant à la notification des signalements

Une fois que les faits justifiant la notification de l'un desdits signalements par l'OLAF ont été détectés, l'enquêteur/l'agent chargé du suivi (demandeur) remplit un formulaire demandant le signalement dans le SAP d'une personne physique ou morale. Ce formulaire est envoyé à l'agent SAP de l'OLAF (chef de l'Unité C.2) et une copie est adressée à un agent SAP adjoint. Ce dernier analyse les informations figurant sur le formulaire afin d'établir la nécessité et la pertinence du niveau de signalement requis. Le formulaire de demande de signalement (RESTREINT UE) à adresser au comptable de la Commission, à la DG Budget, est établi selon le modèle figurant à l'annexe 3 de la décision relative au SAP.

Ce formulaire comporte le numéro de référence du fichier "entités juridiques"⁴ de l'ABAC⁵, ainsi que le nom, l'adresse et la référence du projet. Le formulaire doit également indiquer quel signalement est demandé et présenter brièvement les faits qui le justifient. Pour les personnes physiques, une copie de la carte d'identité, du titre de séjour ou du passeport doit être jointe. Pour les "entités publiques", une copie de la résolution, de la loi, du décret ou de la décision établissant l'entité en question ou de tout autre document officiel relatif à cette entité doit être jointe. Enfin, pour les "entités privées", un extrait du registre (ou son équivalent) doit être joint.

Des copies du formulaire interne, de la note de demande adressée au comptable et, le cas échéant, des pièces justificatives sont conservées dans un dossier placé dans une armoire fermée à clé. Une feuille de calcul est remplie pour toutes les demandes de SAP formulées par les agents SAP adjoints, et l'un de ces agents compare régulièrement les relevés, à des fins de vérification, aux données enregistrées dans le système de comptabilité de la Commission (ABAC). La feuille de calcul est conservée dans un ordinateur autonome distinct. Les copies papier sont conservées dans une armoire fermée à clé.

Une fois que l'inscription dans le SAP a été confirmée par le comptable, et attestée par l'inscription dans l'ABAC, l'agent SAP adjoint envoie au demandeur un courrier électronique sécurisé via le système SECHEM, l'informant que la demande de signalement SAP a été mise à exécution et indiquant la durée de validité. L'agent SAP adjoint imprime une fois par mois la liste des inscriptions ABAC, triées en fonction de la date de validité, et rappelle aux demandeurs initiaux concernés que le signalement SAP arrivera bientôt à expiration. Ces listes sont également conservées dans des armoires fermées à clé.

En cas de signalement W1, l'OLAF informe à l'avance les DG concernées. À partir de l'été 2007, l'agent chargé du suivi aura la possibilité de constituer, dans le système de gestion des cas ("Case Management System" - ci-après "CMS"), un dossier comportant les informations suivantes: le

⁴ Le FEJ (fichier "entités juridiques") recense tous les tiers avec lesquels la Commission effectue des opérations de recettes et de dépenses.

⁵ L'ABAC (acronyme de "Accrual Based Accounting" - ("comptabilité d'exercice")) est un système d'information transversal sur les transactions, permettant l'exécution et le suivi de toutes les opérations budgétaires et comptables par la Commission, une agence ou une institution.

numéro d'entité juridique ABAC, le type de signalement et la date d'expiration, afin que les informations sur les signalements en cours soient facilement accessibles et tenues à jour.

Le chef de l'Unité "Prévention de la fraude et Intelligence" est déclaré responsable du traitement.

Politique de conservation des données

L'OLAF conserve différents documents comportant des renseignements relatifs aux signalements SAP. Parmi ces documents figurent le formulaire interne, la demande adressée au comptable, les pièces justificatives et des versions imprimées du contenu de la feuille de calcul. Des versions imprimées de la liste mensuelle reçue par l'agent SAP sont également conservées.

En fonction de la catégorie du signalement, un délai actif peut lui être appliqué. Dans ce cas, le signalement SAP est désactivé dès l'expiration du délai fixé.

- Un signalement W1 reste actif pendant un délai maximal de six mois, à l'échéance duquel la désactivation intervient automatiquement. S'il convient que l'alerte soit maintenue dans le SAP et qu'elle ne peut pas être remplacée par un autre type de signalement, l'OLAF peut demander un nouveau signalement au comptable de la Commission.
- Un signalement W2 reste actif pendant un délai maximal de six mois, à l'échéance duquel la désactivation intervient automatiquement. S'il convient que l'alerte soit maintenue dans le SAP et qu'elle ne peut pas être remplacée par un autre type de signalement, l'OLAF peut demander un nouveau signalement au comptable de la Commission.
- Les signalements W3 demeurent actifs jusqu'à ce que soit rendu un jugement ayant autorité de chose jugée ou que le litige soit réglé d'une autre manière.

L'ensemble des documents, des versions imprimées et des données est conservé pendant une durée de sept ans à compter de la fin de l'année durant laquelle le signalement de l'OLAF est désactivé. Ce délai est fondé sur les articles 49 et 65 du règlement relatif aux modalités d'exécution du règlement financier, qui précisent que les pièces doivent être conservées pendant une période de cinq ans au moins à compter de la date d'octroi de la décharge par le Parlement européen pour l'année budgétaire (qui se situe généralement deux ans après la fin de l'année budgétaire à laquelle ces pièces se rapportent). Une fois ce délai expiré, les données sont rendues anonymes. À titre d'exemple, si l'OLAF signale une entité juridique du 3/11/2006 au 3/5/2007, les données seront rendues anonymes sept ans après le 31/12/2007, c'est-à-dire le 31/12/2014.

Les données ne sont pas collectées à des fins historiques, statistiques ou scientifiques.

Finalité du traitement

Le traitement vise à: a) faire en sorte que des données exactes soient transmises au comptable lorsqu'une inscription dans le SAP est demandée; b) à veiller à ce que l'OLAF tienne un registre des inscriptions demandées mais pas encore mises à exécution par le comptable; c) à permettre à l'OLAF de répondre aux questions d'autres services concernant les motifs d'une demande d'inscription dans le SAP; et d) à permettre à l'OLAF de demander en temps utile un nouveau signalement en cas de désactivation automatique si l'inscription reste nécessaire.

Information des personnes concernées

Les personnes concernées sont informées du traitement de données au moyen de la déclaration de confidentialité figurant sur le site web de l'OLAF⁶. Ce document comporte des informations sur les

⁶ Déclaration de confidentialité pour le traitement de données à caractère personnel effectué par l'OLAF

points suivants : la finalité du SAP, les signalements dont l'OLAF peut prendre l'initiative en sa qualité d'organe d'enquête, les données traitées, les moyens de stockage des données, l'accès aux données, les délais de conservation. La déclaration de confidentialité informe les personnes concernées de leur droit d'accès aux données les concernant faisant l'objet d'un traitement et de leur droit de rectification ou de suppression de ces données. Cette déclaration mentionne également l'identité du responsable du traitement et des éventuels destinataires, ainsi que le droit des personnes concernées de saisir à tout moment le CEPD.

Catégories de données traitées et transferts

Le traitement porte sur les données suivantes : données d'identification et coordonnées (nom et adresse de l'intéressé, copie du document d'identité s'il y a lieu), informations relatives au dossier (numéro de dossier OLAF, projet/contrat auquel l'intéressé est lié, service de la Commission concerné, manquement relevé), données relatives au système de comptabilité (numéro d'entité juridique, nom de l'entité juridique, forme juridique, adresse) et données SAP (type de signalement, durée de validité).

Les données traitées dans le cadre du SAP sont transmises à l'agent SAP de l'OLAF, à l'agent SAP adjoint, aux agents SAP des DG concernées et au comptable de la DG Budget. En cas d'activation d'un signalement W1, les données sont également transmises à l'OD de la DG concernée (conformément à l'article 2, paragraphe 2, de la décision relative au SAP).

3. Aspects juridiques

3.1. Contrôle préalable

La notification reçue le 30 mars 2007 porte sur un traitement de données à caractère personnel ("*toute information concernant une personne physique identifiée ou identifiable*" - article 2, point a), du règlement (CE) n° 45/2001 (ci-après dénommé "le règlement"). De fait, le système d'alerte précoce (SAP) renferme des données relatives à des personnes physiques non seulement en leur qualité de représentants d'une personne morale, mais également à titre individuel en tant que personnes susceptibles de faire l'objet d'une évaluation dans le cadre du SAP.

Le traitement de données en question est effectué par une institution pour l'exercice d'activités qui relèvent du champ d'application du droit communautaire (article 3, paragraphe 1, du règlement).

Dans la procédure d'enregistrement des personnes concernées dans le SAP, le traitement est en partie automatisé au sens de l'article 3, paragraphe 2, du règlement, mais le contenu est appelé à figurer dans un fichier automatisé. Le règlement s'applique donc conformément à l'article 3, paragraphe 2.

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. L'article 27, paragraphe 2, dresse une liste des traitements susceptibles de présenter de tels risques, qui comporte notamment, au point d), "*les traitements visant à exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat*". L'enregistrement d'une personne physique⁷ dans le SAP peut notamment entraîner son exclusion d'un marché ou d'un octroi de subvention, ou un refus de fonds; il relève donc de l'article 27, paragraphe 2, point d), et, à ce titre, est soumis au contrôle préalable du CEPD.

conformément à la décision C(2004) 193/3 de la Commission du 3/2/2004 relative au système d'alerte précoce.

⁷ Ainsi que de personnes morales (ne relevant pas du règlement n° 45/2001).

Le règlement soumet également au contrôle préalable *"les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur compétence, leur rendement ou leur comportement"* (article 27, paragraphe 2, point b)). Le SAP est incontestablement lié à une procédure d'évaluation menée par l'OLAF et doit, à ce titre, faire l'objet d'un contrôle préalable.

De plus, le traitement porte sur des données relatives à des suspicions ou infractions. Le contrôle préalable est donc justifié en vertu de l'article 27, paragraphe 2, point a), du règlement.

En principe, le CEPD devrait procéder à ces contrôles avant la mise en œuvre du traitement. Dans le cas présent, le CEPD ayant été nommé après la mise en place du système, le contrôle doit forcément avoir lieu a posteriori, ce qui ne change toutefois rien à la nécessité de mettre en œuvre les recommandations émises par le CEPD.

Le CEPD a reçu la notification de la DPD le 30 mars 2007. Conformément à l'article 27, paragraphe 4, du règlement, le présent avis doit être rendu dans les deux mois qui suivent la réception de la notification. Le délai de deux mois a été suspendu pendant 54 jours, des informations complémentaires ayant été demandées. Un courrier électronique a été envoyé pour proroger le délai d'un mois, en raison de la complexité du dossier. Le délai a été suspendu pendant 11 jours pour permettre à la DPD de présenter des observations, ce qui donne un total de 65 jours (+ le mois d'août). Le présent avis doit donc être rendu au plus tard le 4 octobre 2007.

3.2. Licéité du traitement

La licéité du traitement doit être examinée à la lumière de l'article 5, point a), du règlement qui prévoit que le traitement de données à caractère personnel ne peut être effectué que s'il 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 ou relevant de l'exercice légitime de l'autorité publique dont est investi[e] l'institution (...) communautaire"*.

Le traitement de données à caractère personnel dans le cadre du SAP relève de l'exercice légitime de l'autorité publique dont est investi l'OLAF puisqu'il vise à assurer la circulation d'informations de diffusion restreinte concernant des tiers qui pourraient représenter une menace pour les intérêts financiers et la réputation des Communautés, si la Commission noue ou a déjà noué avec eux des relations contractuelles ou conventionnelles.

La base juridique du traitement est la décision de la Commission relative au SAP, qui entre dans des détails non prévus à l'article 95 du règlement financier ni dans les modalités d'exécution, qui comportent des dispositions analogues. Pour l'OLAF, considéré en sa qualité d'organe d'enquête, les règles portent spécifiquement sur les signalements relevant des catégories W1, W2 et W3. La base juridique vient à l'appui de la licéité du traitement.

3.3. Traitement portant sur des catégories particulières de données

L'OLAF traite notamment des données appartenant à des catégories particulières de données relatives aux signalements SAP initiés conformément à l'article 10, paragraphe 5, du règlement: *"[l]e 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, sous réserve des garanties spécifiques et appropriées"*. Ces données incluent des informations relatives à des suspicions et infractions, essentiellement en matière de fraude, détenues par l'OLAF.

Il convient de considérer la base juridique susmentionnée comme la base juridique spéciale pour le traitement de catégories particulières de données. Le CEPD estime que le traitement par l'OLAF de données relatives à des suspicions et infractions est conforme à l'article 10, paragraphe 5, du règlement.

3.4. Qualité des données

L'article 4 du règlement énonce un certain nombre d'obligations concernant la qualité des données à caractère personnel.

Les données doivent être "*traitées loyalement et licitement*" (article 4, paragraphe 1, point a)). La licéité du traitement a déjà été examinée (voir le point 3.2 ci-dessus). La loyauté porte quant à elle sur les informations fournies aux personnes concernées (voir le point 3.8 ci-dessous).

Les données à caractère personnel doivent être collectées "*pour des finalités déterminées, explicites et légitimes*" (article 4, paragraphe 1, point b)). Cette disposition signifie qu'un traitement de données à caractère personnel ne peut être effectué que pour une finalité déterminée. Elle implique également qu'il convient de trouver un juste équilibre entre, d'une part, la nécessité de traiter des données à caractère personnel et, d'autre part, les conséquences que cela peut avoir en termes d'intrusion dans la vie privée des personnes concernées ou d'atteinte à leurs intérêts légitimes. L'introduction d'un signalement contre une personne peut avoir de graves effets négatifs pour la personne concernée; c'est pourquoi il convient de mettre en place certaines garanties visant à sauvegarder les intérêts légitimes de la personne concernée. Ces garanties devraient notamment se traduire par le droit de la personne concernée à être informée et à avoir accès aux données la concernant, ce qui implique que soient accordés des droits d'accès et de rectification, que soit expliquée la manière dont les informations sont protégées et garanties et que soit précisé qui a accès à ces informations (voir le point 3.8 ci-dessous). L'article 4, paragraphe 1, point b), est donc respecté.

Les données doivent être "*adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement*" (article 4, paragraphe 1, point c)). Les données traitées qui sont décrites dans la partie relative aux faits devraient être considérées comme satisfaisant à ces conditions. Les données requises sont nécessaires au bon déroulement des différentes phases de la procédure de signalement prévue par le SAP. Le CEPD estime que l'article 4, paragraphe 1, point c), du règlement est respecté.

Conformément à l'article 4, paragraphe 1, point d), du règlement, les données doivent être "*exactes et, si nécessaire, mises à jour*". De plus, "*toutes les mesures raisonnables sont 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*". Comme décrit ci-dessus, la procédure aboutissant à la notification d'un signalement dans le SAP exige la participation de nombreuses personnes afin d'établir avec certitude que le signalement est effectivement justifié.

Dans certains cas, les signalements sont désactivés soit parce que les enquêtes n'aboutissent à rien (signalements W1), soit parce qu'un jugement ayant autorité de chose jugée blanchit la personne concernée (signalements W3). Le CEPD signale que l'OLAF, de par le rôle spécial qu'il joue dans le cadre du SAP, est responsable non seulement de l'activation des signalements, mais également de leur désactivation. Il est donc recommandé que, lorsque ces signalements W1 ou W3 ne sont plus exacts, l'OLAF en informe dans les plus brefs délais la DG BUDGET afin que celle-ci puisse

supprimer toute trace d'un signalement SAP visible des utilisateurs de base⁸, comme indiqué dans la déclaration de confidentialité (voir également le point 3.5). L'OLAF devrait également demander à la DG BUDGET de désactiver des signalements non seulement lorsque le délai fixé a expiré, mais aussi dès que le signalement n'a plus lieu d'être.

Le droit d'accès prévu par l'article 13 du règlement devrait également permettre de garantir la qualité des données. Cet aspect sera développé ci-après (voir le point 3.7). Le CEPD estime que la procédure elle-même garantit la qualité des données.

3.5. Conservation des données

Le règlement prévoit 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 sont collectées ou pour lesquelles elles sont traitées ultérieurement*" (article 4, paragraphe 1, point e)).

Il convient d'établir une distinction entre la durée pendant laquelle le signalement reste actif et la durée pendant laquelle les données pertinentes sont conservées par l'OLAF. Cet aspect, qui a une incidence sur les informations communiquées à la personne concernée, sera évoqué ci-dessous (point 3.8).

Les documents comportant des données concernant le signalement SAP sont en règle générale conservés pendant une durée de sept ans à compter de la fin de l'année durant laquelle le signalement est désactivé. Ce délai de conservation est conforme aux articles 49 et 65 du règlement relatif aux modalités d'exécution du règlement financier. Le CEPD estime que l'article 4, paragraphe 1, point e), est respecté.

Dans la partie consacrée aux faits, il est indiqué que, dans le cas de signalements W1 et W2, l'OLAF a la possibilité de demander un nouveau signalement au comptable de la Commission s'il est nécessaire de maintenir l'alerte dans le SAP et que celle-ci ne peut pas être remplacée par un autre type de signalement. Dans ce cas, le CEPD recommande qu'il soit fait un usage circonspect de cette nouvelle demande et que ce procédé ne soit pas utilisé comme un moyen de contourner une suppression. Le CEPD recommande donc également que, à chaque fois qu'un deuxième signalement de six mois est introduit, obligation soit faite d'analyser s'il peut être supprimé avant l'expiration du nouveau délai de six mois.

Comme indiqué au point 3.4, le délai de six mois prévu pour les signalements W1 et W2 est un délai maximal, et la désactivation de ces signalements devrait, s'il y a lieu, intervenir avant l'échéance dudit délai.

Les données ne sont pas collectées à des fins statistiques, historiques ou scientifiques. Les deuxième et troisième phrases de l'article 4, paragraphe 1, point e), ne sont donc pas applicables en l'espèce.

3.6. Utilisation compatible/Changement de finalité

L'article 4, paragraphe 1, point b), du règlement (CE) n° 45/2001 prévoit que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. L'utilisation par l'OLAF de données à caractère personnel obtenues à partir de ses propres enquêtes est compatible

⁸ Voir également l'avis du CEPD relatif au SAP de la Commission, dossier 2005-120, point 3.4 (qualité des données), sixième point.

avec la finalité générale pour laquelle ces données ont été collectées, à savoir la protection des intérêts financiers de l'UE.

3.7. Transferts de données

L'article 7 s'applique à tous les transferts de données à caractère personnel entre institutions ou organes communautaires ou même en leur sein. L'article 7, paragraphe 1, du règlement dispose: "*Les données à caractère personnel ne peuvent faire l'objet de transferts entre institutions ou organes communautaires ou en leur sein que si elles sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire*".

Les données traitées dans le cadre des enquêtes de l'OLAF sont transmises à l'agent SAP ou à l'agent SAP adjoint de l'OLAF, aux agents SAP des DG concernées et au comptable de la DG Budget. En cas d'activation d'un signalement W1, les données sont également transmises à l'OD de la DG concernée.

Le CEPD estime que les données transférées sont nécessaires à l'exécution des missions relevant de la compétence des destinataires mentionnés et que, par conséquent, l'article 7 du règlement est respecté.

3.8. Droit d'accès et de rectification

L'article 13 du règlement prévoit un droit d'accès et les modalités selon lesquelles la personne concernée peut, à sa demande, exercer ce droit. L'article 14 du règlement donne à la personne concernée le droit d'obtenir du responsable du traitement la rectification sans délai de données à caractère personnel inexacts ou incomplètes.

La déclaration de confidentialité informe les personnes concernées de la possibilité d'accéder à des données à caractère personnel détenues à leur sujet. Il y est également indiqué que cet accès peut être limité en application de l'article 20, paragraphe 1, points a) et b), du règlement. D'après la notification, cette limitation peut être appliquée par l'OLAF au cas par cas.

L'article 20 prévoit certaines exceptions et limitations au droit d'accès, notamment lorsqu'une telle limitation constitue une mesure nécessaire pour "*sauvegarder un intérêt économique ou financier important (...) des Communautés européennes, y compris dans les domaines monétaire, budgétaire et fiscal*" (article 20, paragraphe 1, point b), du règlement).

Si l'une de ces limitations est invoquée, l'OLAF est tenu de prendre en compte et de respecter l'article 20, paragraphe 3, qui est libellé comme suit: "*Si une limitation prévue au paragraphe 1 est imposée, 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*". En ce qui concerne le droit à l'information, cette disposition doit se lire en combinaison avec les articles 11 et 12 du règlement (voir le point 3.9 ci-dessous).

Si une limitation du droit d'accès est imposée, la personne concernée a le droit de solliciter un accès indirect en saisissant le CEPD (article 20, paragraphe 4).

L'article 20, paragraphe 5, dispose: "*L'information visée aux paragraphes 3 et 4 peut être reportée aussi longtemps qu'elle prive d'effet la limitation imposée sur la base du paragraphe 1*". Il peut se révéler nécessaire pour l'OLAF de reporter cette information conformément à cette disposition, afin de protéger les intérêts financiers de la Communauté. Les limitations d'un droit fondamental ne peuvent être appliquées de manière systématique. En effet, comme le prévoit l'article 20 du

règlement, la mesure doit être "nécessaire". Le "critère de nécessité" doit être apprécié au cas par cas. C'est ainsi, par exemple, que la nature de certaines affaires ne justifiera pas toujours le refus d'accès et de rectification au cours du traitement.

L'article 14 du règlement accorde à la personne concernée le droit d'obtenir la rectification de données inexactes ou incomplètes. Étant donné que, dans la plupart des situations, ces enquêtes revêtent un caractère sensible, ce droit est d'une importance cruciale pour garantir la qualité des données utilisées qui, dans ce cas précis, est liée aux droits de la défense. Toute limitation prévue à l'article 20 du règlement doit être appliquée à la lumière des observations qui ont été présentées dans les points ci-dessus en ce qui concerne le droit d'accès.

L'OLAF s'engage à ce que, à la demande de la personne concernée, les données soient corrigées et, si cela est dûment justifié, effacées. D'une part, il est dans l'intérêt des personnes concernées de voir le signalement supprimé dès que possible, afin de ne pas être exclues plus longtemps de l'attribution de marchés. D'autre part, tout signalement inexact pourrait entraîner des exclusions injustifiées de procédures d'attribution de marchés et nuirait aux intérêts des personnes concernées. Dans le cadre de l'introduction de signalements SAP, les demandes de rectification ou de suppression émanant des personnes concernées doivent être traitées avec une attention particulière. L'OLAF veille à ce que ce droit (expressément énoncé dans la déclaration de confidentialité) puisse être exercé par les personnes concernées. Les demandes en question sont traitées avec un soin particulier et les données à caractère personnel ne sont rectifiées que lorsque cela est nécessaire.

Le CEPD estime que les articles 13 et 14 sont correctement appliqués au cours de la procédure à l'examen.

3.9. Information de la personne concernée

Le règlement prévoit que les personnes concernées doivent être informées du traitement de données les concernant et énumère une série d'informations à fournir obligatoirement (identité du responsable du traitement, catégories de données concernées, finalités du traitement, destinataires, caractère obligatoire ou facultatif de la réponse aux questions, origine des données, droit d'accès). De plus, dans la mesure où elles sont nécessaires pour assurer un traitement loyal des données, il convient de fournir des informations supplémentaires concernant la base juridique, les délais et le droit de saisir à tout moment le CEPD.

Les informations utilisées au cours de la procédure à l'examen émanent en partie et indirectement de la personne concernée (via le fichier "entités juridiques" de l'ABAC). D'autres informations proviennent cependant d'autres sources. Par conséquent, les articles 11 et 12 du règlement sont tous deux applicables en l'espèce.

Les personnes concernées sont informées du traitement par la déclaration de confidentialité de l'OLAF. Ce document donne des informations sur la finalité du SAP, sa base juridique, les signalements dont l'OLAF peut prendre l'initiative en sa qualité d'organe d'enquête, les données traitées, les moyens de stockage des données, l'accès aux données. La déclaration de confidentialité informe les personnes concernées de leur droit d'accès aux données les concernant faisant l'objet d'un traitement et de leur droit de rectification ou de suppression de ces données. Cette déclaration mentionne également l'identité du responsable du traitement et des éventuels destinataires, ainsi que le droit des personnes concernées de saisir à tout moment le CEPD. Étant donné que des informations sont données à la personne concernée par la déclaration de confidentialité du FEJ, qui mentionne indirectement les signalements de l'OLAF, celui-ci devrait veiller à ce que la déclaration de confidentialité transmise aux personnes concernées dans le cadre du FEJ comporte un lien vers sa propre déclaration de confidentialité.

Au point 5 de la déclaration de confidentialité intitulé "Combien de temps gardons-nous vos données?" les personnes concernées sont informées des délais pendant lesquels les différents signalements restent actifs. Cette information est essentielle. Toutefois, les personnes concernées ne sont pas informées du délai de conservation de l'ensemble des documents relatifs aux signalements. Le CEPD recommande de faire figurer cette information dans la déclaration de confidentialité.

3.10. Mesures de sécurité

Le CEPD note que les mesures de sécurité décrites dans le contexte du traitement de données préalable à l'établissement d'une demande de signalement dans le cadre du SAP sont identiques à celles utilisées lors d'autres traitements de données qui lui ont été notifiés en vue d'un contrôle préalable. Pour garantir une approche cohérente à l'égard des mesures de sécurité de l'OLAF, le CEPD a décidé de les analyser horizontalement, plutôt que dans le contexte de chaque notification en vue d'un contrôle préalable. En conséquence, le présent avis ne traitera pas des mesures de sécurité; leur analyse sera effectuée dans un avis distinct qui portera uniquement sur les questions de sécurité.

Conclusion

Rien ne permet de conclure à un manquement aux dispositions du règlement (CE) N°45/2001, sous réserve que les considérations formulées dans le présent avis soient pleinement prises en compte. L'OLAF devrait :

- demander à la DG BUDGET de désactiver un signalement dès que celui-ci n'a plus lieu d'être;
- faire un usage circonspect de la possibilité de former une nouvelle demande de signalement et ne pas utiliser ce procédé comme un moyen de contourner une suppression;
- chaque fois qu'un deuxième signalement de six mois est introduit, analyser s'il peut être supprimé avant l'expiration du nouveau délai;
- veiller à ce que la déclaration de confidentialité transmise aux personnes concernées dans le cadre du FEJ comporte un lien vers sa propre déclaration de confidentialité;
- faire figurer dans la déclaration de confidentialité des informations relatives à la conservation des données.

Fait à Bruxelles, le 4 octobre 2007

(signé)

Peter HUSTINX
Contrôleur européen de la protection des données