

**Avis sur les notifications reçues du délégué à la protection des données de l'Office européen de lutte antifraude en vue d'un contrôle préalable concernant l'unité de coopération opérationnelle virtuelle, le courtier d'assistance mutuelle et le système d'information douanier**

Bruxelles, le 17 octobre 2011 (dossiers conjoints 2010-0797, 2010-0798, 2010-0799)

## **1. Procédure**

Le 11 octobre 2010, le Contrôleur européen de la protection des données (**CEPD**) a reçu trois notifications du délégué à la protection des données (**DPD**) de l'Office européen de lutte antifraude (**OLAF**) en vue d'un contrôle préalable concernant le traitement de données à caractère personnel relatives à l'unité de coopération opérationnelle virtuelle (**UCO-V**), au courtier d'assistance mutuelle (**CAM**) et au système d'information douanier (**SID**).

Les notifications étaient accompagnées des documents suivants:

- pour l'UCO-V:
  - Manuel d'assistance de l'UCO-V
  - Déclaration de confidentialité
  - Exemples d'écrans des différents modules (Consur, Marsur, Viasur)
- pour le CAM:
  - Déclaration de confidentialité
  - Annexe I des procédures de MAR-/YAC-INFO
- pour le SID:
  - Déclaration de confidentialité
- jointe à l'ensemble des notifications:
  - Politique de sécurité AFIS (AFIS-SEC-POL)

Le CEPD a posé une première série de questions à l'OLAF, auxquelles cette dernière a répondu le 20 octobre 2010. Une deuxième série de questions a été envoyée à l'OLAF le 26 novembre 2010, dont les réponses ont été reçues le 26 mai 2011. Entre-temps, le délai prévu pour rendre l'avis de contrôle préalable a été suspendu.

Les réponses étaient accompagnées des documents justificatifs supplémentaires suivants:

- pour l'UCO-V:
  - Plan opérationnel pour l'ODC Sirocco
  - Formation Consur de l'UCO-V
  - Manuel d'assistance de l'UCO
  - Liste de pays tiers et d'organisations internationales
- pour le SID:

- Manuel d'utilisation de l'outil d'enregistrement des utilisateurs
- Exigences de qualité du SID et de l'UCO-V
- sur la politique de sécurité AFIS (AFIS-SEC-POL):
  - Lignes directrices sur la sécurité du terminal AFIS
  - Procédure de traitement des opérations AFIS (annexe 1 du document principal de la politique de sécurité AFIS)
  - Exigences de base en matière de sécurité AFIS UNIX
  - Exigences de base en matière de sécurité AFIS Windows

Le 10 juin 2011, le CEPD a demandé qu'une réunion soit organisée avec l'OLAF afin de discuter des questions en suspens que ce dernier n'avait pas traitées dans ses réponses. Cette réunion s'est tenue le 1<sup>er</sup> juillet 2011. Dans l'intervalle, le dossier a de nouveau été suspendu. Suite à la réunion, l'OLAF a remis au CEPD une copie du manuel d'utilisation des dossiers CAM. Compte tenu du caractère complexe des dossiers considérés, le CEPD a décidé le 1<sup>er</sup> juillet 2011 de prolonger de deux mois le délai prévu pour soumettre son avis.

Le CEPD a envoyé son projet d'avis au DPD le 27 septembre 2011 afin qu'il puisse soumettre ses observations, lesquelles ont été reçues le 10 octobre 2011.

## **2. Les faits**

### **2.1. Remarques générales**

Le présent avis de contrôle préalable examine les trois notifications soumises par le DPD de l'OLAF, qui concernent toutes la coopération dans le domaine de la lutte contre la fraude douanière et agricole. Étant donné que ces trois notifications sont liées entre elles, le CEPD a décidé de les examiner dans un seul avis.

Les trois applications remplissent des fonctions étroitement liées, sont régies par la même politique de sécurité et sont en partie intégrées les unes aux autres; c'est pourquoi il convient d'adopter une approche globale. Les notifications pour l'UCO-V et le CAM sont des mises à jour d'une notification précédente concernant les échanges d'informations relevant de l'assistance mutuelle, tandis que la notification sur le SID met à jour une notification précédente sur le même système. Pour ces notifications précédentes, le CEPD a publié des avis le 19 octobre 2007 et le 24 juillet 2007 (dossiers CEPD n° 2007-0202 et 2007-0177), respectivement. À cet égard, le présent avis fait également office de suivi aux avis susmentionnés et mettra l'accent sur les nouveaux aspects du traitement notifié. Les points communs applicables à toutes les notifications seront tout d'abord examinés avant de considérer les questions concernant les applications individuelles uniquement. Le cas échéant, des références seront faites aux précédents avis de contrôle préalable et aux recommandations qui y figurent.

#### *Description et finalité du traitement*

Bien qu'il existe des différences entre les applications, elles ont toutes pour objectif général de renforcer la coopération en matière douanière entre les États membres et la Commission, dans le but de prévenir, rechercher et poursuivre les violations des réglementations douanière ou agricole. Les applications permettent aux États membres de partager des informations, tant sous une forme structurée que déstructurée (texte libre), relatives à des personnes qui sont impliquées ou soupçonnées d'être impliquées dans de telles violations ainsi qu'aux autorités chargées d'enquêter sur ces dossiers. L'accès à l'ensemble des informations se fait via le

portail AFIS, une application de navigateur qui fournit une interface unifiée à un certain nombre de bases de données et d'applications. Dans certains cas, l'autorité ayant introduit les données dans le système peut également autoriser des transferts vers des pays tiers.

Chacun des systèmes consiste en une base de données centrale à laquelle peuvent accéder la Commission, un certain nombre d'autorités compétentes des États membres et parfois certains pays tiers, organisations internationales ainsi qu'Europol et Eurojust. L'accès par des pays tiers et des organisations internationales<sup>1</sup> est régi par des accords d'assistance mutuelle contenant des clauses à cet effet.<sup>2</sup> Europol et Eurojust peuvent obtenir un accès relevant de leurs compétences, mais ils ne peuvent pas introduire de données. L'UCO-V se différencie des autres systèmes dans le sens où un accès est uniquement accordé pour une durée limitée aux autorités des pays prenant part à une opération douanière conjointe (ODC) déterminée comme indiqué dans le plan opérationnel respectif de l'ODC. Le traitement est, dans l'ensemble, automatisé. Cependant, la décision d'inclure ou d'exclure des données constitue un traitement manuel. Une description plus détaillée est exposée dans les sous-sections suivantes concernant les différents systèmes.

#### *Bases juridiques*

Les trois applications trouvent leur base juridique au moins en partie dans le règlement (CE) n° 515/97,<sup>3</sup> modifié en dernier lieu par le règlement (CE) n° 766/2008.<sup>4</sup> Le SID est régi par des règles spécifiques relevant du titre V (articles 23 à 41) dudit règlement, tandis que le rôle de la Commission (dans ce cas l'OLAF) dans le CAM et l'UCO-V repose sur le titre III (articles 17 et 18). Les applications peuvent concerner des transferts de données à caractère personnel en dehors de l'UE comme mentionné au titre IV (articles 19 à 22) du règlement n° 515/97. La partie du SID relevant de l'ancien troisième pilier est régie par la décision 2009/917/JAI<sup>5</sup> du Conseil depuis son entrée en vigueur le 27 mai 2011. L'OLAF lui-même a été institué par le règlement (CE) n° 1073/99.<sup>6</sup>

#### *Contrôle & responsabilités*

Les trois applications notifiées sont toutes gérées par l'OLAF; selon ces notifications, un fonctionnaire de l'unité C.3 (Assistance mutuelle & Renseignements) au sein de l'OLAF est le responsable délégué du traitement des données. Les applications utilisent des serveurs situés dans les locaux de l'OLAF et gérés par ce dernier.

Des données sont ajoutées, modifiées et utilisées par les autorités des États membres (et, parfois, par des pays tiers). Seule l'autorité qui a ajouté des données peut les modifier. Ces autorités peuvent faire fonction de coresponsables du traitement. La question sera examinée plus en détail à la section 3.4.

#### *Utilisateurs et gestion utilisateur*

Les utilisateurs des trois applications sont gérés à l'aide d'un outil unifié, l'outil d'enregistrement des utilisateurs (OEU). Une copie du manuel d'utilisation pour cet outil a été remise au CEPD. Il existe plusieurs catégories d'utilisateurs bénéficiant de différents droits.

---

<sup>1</sup> Selon les informations obtenues auprès de l'OLAF, l'Organisation mondiale des douanes (OMD) peut recevoir des données dépersonnalisées du CAM sur les dossiers Marinfo, Ciginfo et Yachtinfo (p. 23, 28 du manuel d'utilisation des dossiers CAM); les informations figurant dans le CAM sont en partie accessibles aux membres de MarInfo, ces derniers n'étant pas tous des États membres de l'UE. Interpol a participé en tant qu'observateur à au moins une ODC (p. 13, annexe 2 à Q12).

<sup>2</sup> Voir la liste qui peut être consultée à l'adresse suivante: [http://ec.europa.eu/dgs/olaf/assist\\_3rd/index\\_en.html](http://ec.europa.eu/dgs/olaf/assist_3rd/index_en.html).

<sup>3</sup> JO L 82 du 22.03.1997, p. 1.

<sup>4</sup> JO L 218 du 13.08.2008, p. 48.

<sup>5</sup> JO L 323 du 10.12.2009, p. 20.

<sup>6</sup> JO L 136 du 31.05.1999, p. 1.

Ces fonctions sont les suivantes: utilisateur normal, officier de liaison, représentant légal autorisé, service d'assistance informatique. Les utilisateurs normaux peuvent prendre la forme de comptes personnels ou institutionnels. Ces utilisateurs sont gérés et créés par l'agent de liaison national. Cet agent peut créer des demandes pour de nouveaux utilisateurs et de nouvelles organisations et gérer leurs droits. Les demandes qui nécessitent une autorisation légale sont vérifiées et validées par le représentant légal autorisé, qui est un fonctionnaire de l'OLAF, et mises en œuvre par le service d'assistance informatique, qui fait également partie du personnel de l'OLAF. Les demandes qui ne nécessitent pas d'autorisation légale sont directement mises en œuvre par le service d'assistance à la demande de l'agent de liaison.

#### *Catégories de données et personnes concernées*

Selon les notifications, les trois systèmes traitent des données à caractère personnel relatives à deux catégories différentes de personnes concernées:

##### Catégorie I: Personnes mentionnées dans des dossiers à propos desquelles des informations sont détenues ou échangées.

Cette catégorie concerne les personnes mentionnées dans les messages transférés entre l'OLAF et les États membres ou des pays tiers, dans le cadre des applications notifiées, ainsi que les personnes à propos desquelles des informations sont détenues. Elle concerne plus particulièrement les personnes qui sont ou qui paraissent être impliquées dans des opérations détectées ou planifiées qui sont contraires aux réglementations douanière et agricole.

##### Catégorie II: Les fonctionnaires travaillant sur ces dossiers.

Dans le cas de l'UCO-V et du CAM, ces personnes peuvent être des fonctionnaires des États membres et de pays tiers travaillant sur les dossiers, tandis que pour le SID, seuls des fonctionnaires des États membres sont mentionnés. Pour l'UCO-V et le CAM, les fonctionnaires de certaines organisations internationales peuvent obtenir un accès; cependant, les membres de leur personnel ne sont pas mentionnés comme relevant de cette catégorie dans les notifications.

Dans la première catégorie, le volume d'informations traitées diffère selon les systèmes notifiés, mais contient au moins les noms, adresses, date et lieu de naissance, ainsi que des détails sur les pièces d'identité. Des listes exhaustives sont incluses ci-dessous dans les sous-sections sur les différents systèmes. Parfois, elles contiennent également des champs de texte libre ou des champs concernant les signes, qui pourraient en théorie contenir des informations permettant de tirer des conclusions quant à l'origine raciale, ethnique ou religieuse, des informations relatives à la santé ou d'autres types particuliers de données. Les manuels pour tous les systèmes informent les utilisateurs sur la protection particulière accordée à ce type de données et précisent que ces dernières ne doivent pas être enregistrées dans les systèmes.

En ce qui concerne la seconde catégorie de personnes concernées, à savoir les fonctionnaires travaillant sur les dossiers en question, les trois systèmes utilisent la même liste de champs de données:

- 1) nom, prénom
- 2) service
- 3) numéro de téléphone, de téléphone portable, de télécopie, adresse de courrier électronique<sup>7</sup>.

---

<sup>7</sup> La notification sur le SID intitule ce point «données de contact». On peut raisonnablement supposer que le contenu est identique.

### *Information et droits des personnes concernées*

Les personnes concernées relevant de la catégorie I sont informées de la collecte possible de données les concernant au moyen de déclarations de confidentialité qui seront diffusées sur le site web de l'OLAF et le portail AFIS, dans une partie accessible au public.

Les déclarations de confidentialité pour les trois systèmes sont en grande partie similaires. Elles informent les éventuelles personnes concernées des finalités et des bases juridiques du traitement, ainsi que de l'identité des personnes auxquelles les données peuvent être divulguées et des délais de conservation. Les déclarations pour l'UCO-V et le CAM mentionnent que sous certaines conditions, les données peuvent également être envoyées à des pays tiers et des organisations internationales. Seule la déclaration pour le SID contient une liste des champs de données pouvant être traités. Les droits d'accès, de rectification et d'effacement tels que mentionnés dans les déclarations sont les mêmes pour les trois applications: les personnes peuvent demander une copie des données enregistrées les concernant en contactant le responsable du traitement dont le nom et les coordonnées sont communiqués et peuvent demander la rectification de données inexacts.

Les personnes concernées sont informées que les limitations visées à l'article 20 du règlement (CE) n° 45/2001 peuvent s'appliquer. Les déclarations pour l'UCO-V et le CAM mentionnent également que si les données en question ont été communiquées par un État membre, celui-ci aura la possibilité de donner son avis sur la demande avant que l'accès ne soit accordé. Ces deux déclarations mentionnent également que si des informations sont utilisées lors d'importants transferts interinstitutionnels aux fins de détecter des tendances et une activité inhabituelle, aucune déclaration individuelle de leur utilisation ne sera communiquée.

Le délai pour verrouiller/effacer des données suite à une demande justifiée est d'un mois pour les trois bases de données. Les personnes concernées sont informées de leur droit de saisir le CEPD dans les trois déclarations de confidentialité.

L'OLAF a mis en place des procédures permettant de fournir des informations personnalisées allant au-delà de ce qui est mentionné dans les déclarations de confidentialité aux personnes concernées.<sup>8</sup> Ces informations seront uniquement communiquées avec le consentement préalable du responsable du traitement des données du partenaire opérationnel ayant introduit les données dans le système respectif. En outre, les exceptions visées à l'article 20 du règlement (CE) n° 45/2001 peuvent s'appliquer. Les lignes directrices en vigueur attirent l'attention sur le fait que ces exceptions peuvent uniquement s'appliquer au cas par cas.

Pour les personnes concernées relevant de la catégorie II, l'OLAF demande aux autorités respectives des États membres de leur communiquer toutes les informations utiles. Les personnes concernées relevant de la catégorie II qui sont des membres du personnel de l'OLAF ont également accès aux «lignes directrices à l'intention des fonctionnaires de l'OLAF concernant la mise en œuvre pratique des exigences en matière de protection des données», adoptées par le directeur général de l'OLAF en octobre 2010.

### *Conservation des données*

L'OLAF applique les mêmes procédures de base pour la conservation des données aux trois systèmes. Selon les informations communiquées dans les notifications, les données à caractère personnel enregistrées dans les systèmes peuvent être conservées pendant une durée

---

<sup>8</sup> Lignes directrices à l'intention du personnel de l'OLAF concernant la mise en œuvre pratique des exigences en matière de protection des données, octobre 2010, titre 1.5. Annexe 5 du manuel de l'OLAF, disponible à l'adresse suivante: <http://ec.europa.eu/dgs/olaf/legal/manual/annexes/Guidelines-October2010.pdf>.

maximale de dix ans. Le CEPD a déjà demandé à l'OLAF de justifier ce délai de conservation dans son avis du 19 octobre 2007, qui portait sur les précédents systèmes de l'UCO-V et du CAM, puis à nouveau dans une série de questions posées le 26 novembre 2010.

Dans ses réponses, l'OLAF a souligné que les dossiers devaient être réexaminés tous les ans afin de déterminer la nécessité de continuer à les conserver. Après 11 mois, les utilisateurs sont informés que les données vont être réexaminées. En l'absence de décision de conserver les données dans le délai de réexamen (un mois), elles sont effacées. Selon l'OLAF, des décisions favorables peuvent uniquement être rendues pour les dossiers du SID. L'OLAF a également informé le CEPD qu'il n'avait pas publié d'autres lignes directrices destinées aux responsables prenant cette décision.

Les registres d'accès aux systèmes accessibles via le portail AFIS sont conservés pendant 15 ans. Une procédure a été mise en place pour accorder l'accès à ces registres aux autorités compétentes des États membres à des fins d'audit. Le DPD d'Eurojust a introduit une demande pour recevoir un extrait mensuel des registres AFIS, laquelle a été accordée. Une procédure sera mise en place et notifiée au CEPD. Le CEPD a été informé par l'OLAF que le DPD d'Europol a soumis une demande similaire.

#### *Aspects de sécurité*

[...]

Ce sont là les points clés que les trois applications ont en commun. Les remarques spécifiques suivantes contiennent une description plus détaillée des propriétés de chacun des systèmes.

## **2.2. Remarques spécifiques**

### **2.2.1. UCO-V**

L'UCO-V est un outil qui permet d'échanger des informations sur des suspicions non confirmées et de demander la prise de mesures par d'autres autorités compétentes. Une version précédente de l'UCO-V avait déjà été notifiée au CEPD, ce qui l'a conduit à émettre un avis le 19 octobre 2007 (dossier n° 2007-0202), accompagné d'un certain nombre de recommandations.

#### *Description du traitement*

L'UCO-V est une application de navigateur accessible via le portail AFIS visant à collecter et vérifier des informations sur les mouvements et contrôles de marchandises et de personnes pour les États membres, ainsi que pour des pays tiers et des organisations internationales avec lesquels l'UE a conclu des accords d'assistance mutuelle contenant des clauses à cet effet. Ces informations concernent des suspicions non confirmées, qui peuvent être introduites par des fonctionnaires des États membres et des pays tiers ou des organisations internationales qui prennent part à des opérations douanières conjointes (ODC) et à d'autres opérations similaires à court terme. Les ODC sont des opérations coordonnées menées par les autorités des États membres et éventuellement de pays tiers. Chaque ODC dispose d'un accès particulier aux données contenues dans l'UCO-V qui est uniquement accordé aux pays déterminés prenant part à l'ODC en question. À titre d'exemple, le CEPD a reçu une copie du projet de plan opérationnel pour une ODC passée.

Le traitement des données est engagé par l'introduction des données (enregistrement des mouvements) dans le système par les autorités compétentes des États membres et d'autres autorités ayant un accès à l'UCO-V. Ces enregistrements de mouvements contiennent des informations sur les mouvements suspects (basés sur un certain nombre d'indicateurs, comme des expéditeurs/destinataires connus, une documentation incohérente, etc.) de marchandises et peuvent également inclure des données à caractère personnel, p.ex. de chauffeurs de camions. Ces entrées peuvent également demander à ce que des actions spécifiques soient prises, p. ex. des contrôles et des scannages d'expéditions. D'autres parties peuvent saisir des commentaires libres sur les enregistrements, tels que «cette personne est associée à la contrefaçon de produits de marque», ou sur les résultats des contrôles. Ces données sont enregistrées dans une base de données centrale<sup>9</sup> et sont accessibles à d'autres parties dans un laps de temps limité durant le cycle de vie d'ODC concrètes. Ce cycle de vie est généralement divisé en trois phases: pré-opérationnelle (sélection de cibles pour une surveillance spéciale), opérationnelle (réalisation de contrôles) et post-opérationnelle (suivi).

En fonction du type d'entrée considérée, les écrans, appelés modules, prennent différentes formes, donnent des informations détaillées sur l'expédition ou l'observation en question et les commentaires soumis par d'autres parties. Les différents modules sont les suivants:

- **Viasur** concerne la collecte de renseignements sur le trafic routier;
- **Censure** collecte également des renseignements mais pour le trafic maritime conteneurisé;
- **Marsur** remplit la même fonction pour le trafic maritime non commercial.

---

<sup>9</sup> Il s'agit de la principale différence avec les formats d'échange traditionnels qui ne prévoyaient aucun stockage central des données.

L'OLAF a fourni au CEPD des captures d'écrans de ces modules. Les échanges d'informations prennent la forme de messages structurés dans l'application de messagerie du système AFIS, c'est-à-dire de courriers CAM (voir la section 2.2.2 sur le CAM ci-dessous). En outre, l'UCO-V contient une application de messagerie qui permet d'échanger des messages avec texte libre entre les participants.

#### *Base juridique*

La notification contient uniquement une référence générale au règlement (CE) n° 515/97 comme base juridique. Plus précisément, le rôle de la Commission est basé sur le titre III de ce règlement (articles 17 et 18). L'accès par les pays tiers est régi par le titre IV dudit règlement et les accords d'assistance mutuelle en vigueur. L'UCO-V vise à faciliter les demandes de «surveillance spéciale» soumises au titre de l'article 7 du règlement (CE) n° 515/97.

#### *Catégories de données*

La liste spécifique des données à caractère personnel relatives aux personnes concernées relevant de la catégorie une (voir section 2.1 remarques générales ci-dessus) qui doit être enregistrée dans l'UCO-V contient les éléments suivants:

- 1) nom, prénom
- 2) lieu et date de naissance
- 3) nationalité
- 4) documents d'identité
- 5) données relatives au rôle dans le dossier (texte libre)

L'OLAF a confirmé que les données relatives aux membres de la famille des suspects seront uniquement incluses dans le champ de texte libre concernant les données relatives au rôle dans le dossier si elles présentent un intérêt pour le dossier considéré; le nom de jeune fille des femmes mariées peut être inclus pour la même raison. Cette demande avait été formulée dans les recommandations soumises dans le cadre du précédent contrôle préalable. Les utilisateurs de l'UCO-V sont informés des principes de qualité des données applicables, par écrit et lors de sessions de formation (apprentissage en ligne ou sur le terrain) avant le lancement d'une ODC.

#### *Destinataires des données*

En ce qui concerne les destinataires potentiels, la notification mentionne les fonctionnaires désignés des autorités compétentes de la Commission et des États membres chargés d'appliquer le règlement (CE) n° 515/97. La déclaration de confidentialité mentionne les fonctionnaires désignés des «autorités administratives, législatives et judiciaires compétentes des États membres, des institutions, organes et agences de l'UE, des organisations internationales et/ou des autorités administratives de pays tiers». La notification et la déclaration de confidentialité mentionnent également que les données peuvent être transmises aux autorités de pays tiers si des accords d'assistance mutuelle ont été conclus entre l'Union et ces derniers.<sup>10</sup> Les organisations internationales en tant que destinataires sont mentionnées dans la description du traitement objet de la notification, mais non dans le champ sur les destinataires. Les aspects techniques de la gestion des utilisateurs ont été décrits dans la section générale ci-dessus.

Selon la déclaration de confidentialité jointe à la notification, «les informations sont analysées au moyen d'outils informatiques et peuvent être utilisées par l'OLAF à des fins de

---

<sup>10</sup> Voir [http://ec.europa.eu/dgs/olaf/assist\\_3rd/index\\_en.html](http://ec.europa.eu/dgs/olaf/assist_3rd/index_en.html).



renseignement (voir les notifications DPD-88: banques de données d'informations et de renseignements, et DPD-89: bases de données de renseignements)». Ces notifications ont amené le CEPD à publier un avis de contrôle préalable conjoint le 21 novembre 2007.

#### *Droits des personnes concernées*

Les droits des personnes concernées sont passés en revue lors de l'examen des déclarations de confidentialité dans les remarques générales. Dans les réponses qu'il a soumises le 26 mai 2011, l'OLAF a souligné que les demandes d'accès seraient probablement refusées pendant toute la durée de l'ODC (généralement 10 à 14 jours).

### **2.2.2. CAM**

Le CAM est un système de gestion des dossiers destiné à échanger des informations sur différentes bases de données associées aux douanes. Une version précédente du CAM a déjà été notifiée au CEPD. Un avis de contrôle préalable pour ce système a été publié le 19 octobre 2007 (dossier n° 2007-0202) et comprenait un certain nombre de suggestions que l'OLAF devait mettre en œuvre conformément au règlement (CE) n° 45/2001.

#### *Base juridique*

La base juridique pour le rôle de la Commission est la même que pour l'UCO-V, à savoir le titre III du règlement n° 515/97/CE.

#### *Description du traitement*

Le CAM fournit une interface commune à cinq systèmes d'échange d'informations. Ces systèmes sont Yachtinfo, Marinfo, Ciginfo, la messagerie du CAM et le SID.

- **Yachtinfo** concerne des informations et des saisies confirmées sur des navires non commerciaux. [...].
- **Marinfo** concerne des informations et des saisies confirmées dans le cadre du trafic maritime conteneurisé. [...].
- **Ciginfo** concerne des informations et des saisies confirmées de cigarettes et de produits du tabac ainsi que des marchandises contrefaites.
- **Le SID** aide les autorités douanières participantes à coopérer les unes avec les autres en autorisant l'échange d'informations sur des (suspensions) de violations des réglementations douanière et agricole. Il sera décrit plus en détail ci-dessous étant donné qu'il s'agit de l'objet d'une des trois notifications proprement dite.
- **La messagerie du CAM** permet d'envoyer des messages non structurés (texte libre) à d'autres participants dans le système. Il s'agit du même système que la précédente messagerie AFIS. Comme susmentionné, elle est également utilisée pour échanger des messages dans le contexte de l'UCO-V.

Les quatre premiers sous-systèmes sont utilisés pour créer des dossiers et échanger des informations structurées;<sup>11</sup> le dernier permet d'échanger des messages avec texte libre entre les participants.

Lorsqu'ils créent un dossier, les responsables peuvent sélectionner des types de dossiers multiples; par exemple, un dossier Marinfo associé à un dossier Ciginfo. Les données saisies au stade de la création du dossier seront ensuite automatiquement introduites dans tous les

---

<sup>11</sup> Ces échanges prennent la forme de messages structurés dans l'application de messagerie AFIS (c'est-à-dire la messagerie du CAM).

dossiers, dans la mesure où elles partagent les mêmes champs de données.<sup>12</sup> Cependant, une fois créés, les dossiers deviennent indépendants les uns par rapport aux autres, et aucune donnée n'est transférée entre eux. Les données sont détenues centralement par l'OLAF.

#### *Catégories de données*

Les champs de données qui peuvent être inclus dans la partie structurée (les trois premiers sous-systèmes susmentionnés, le SID sera examiné au point 2.2.3) du CAM sont les suivants:

- 1) nom, prénom, nom de jeune fille, nom d'emprunt, sexe
- 2) signes
- 3) lieu et date de naissance
- 4) nationalité
- 5) profession
- 6) une alerte avertissant que la personne a déjà porté une arme, fait usage de violence, consommé des drogues, tenté de se suicider et autres alertes (à sélectionner sur une liste mais également texte libre)
- 7) document d'identité (type, numéro, date et lieu d'émission)
- 8) adresse (boîte postale, rue, n°, boîte, code postal, ville, pays)
- 9) description du rôle (à sélectionner sur une liste, et également texte libre, comprenant une évaluation de la qualité des informations)
- 10) action suggérée

Le champ prévu pour les alertes peut comprendre des informations sur la consommation de drogues et les tendances suicidaires qui n'ont pas été incluses dans la notification précédente sur les échanges d'informations relevant de l'assistance mutuelle (dossier CEPD n° 2007-0202). Le champ sur les signes physiques pourrait en principe également inclure des données permettant de tirer des conclusions sur les origines raciales, ethniques ou religieuses ou la santé.

La messagerie du CAM est quant à elle une application de messagerie qui permet à ses utilisateurs d'échanger des messages non structurés (c'est-à-dire du texte libre). Lors des sessions de formation qui sont organisées avant l'octroi d'un accès, les utilisateurs sont priés de ne pas saisir de données sensibles dans ces messages avec texte libre et dans les autres champs.

#### *Destinataires des données*

En ce qui concerne les destinataires potentiels, la notification mentionne les fonctionnaires désignés des autorités compétentes de la Commission et des États membres chargés d'appliquer le règlement (CE) n° 515/97. La déclaration de confidentialité mentionne les fonctionnaires désignés des «autorités administratives, législatives et judiciaires compétentes des États membres, des institutions, organes et agences de l'UE, des organisations internationales et/ou des autorités administratives de pays tiers». En outre, des informations peuvent être échangées avec les membres des groupes MarInfo et YachtInfo, tous n'étant pas des États membres de l'UE. Les données peuvent être transmises aux autorités de pays tiers si des accords d'assistance mutuelle ont été conclus entre l'Union et ces derniers. Les informations provenant des dossiers Yachtinfo, MarInfo et CigInfo peuvent également être transmises à l'Organisation mondiale des douanes (OMD); dans ce cas, seul un sous-ensemble dépersonnalisé des informations<sup>13</sup> est envoyé. Cependant, aucune organisation

---

<sup>12</sup> Par exemple, des cigarettes introduites en contrebande dans un conteneur sur un navire commercial pourraient être saisies dans le SID, MarInfo et CigInfo; cependant, le connaissance serait uniquement inclus dans MarInfo.

<sup>13</sup> Voir le manuel d'utilisation des dossiers CAM, p. 23.

internationale n'est mentionnée dans la notification comme étant le destinataire des données à caractère personnel.

Selon la déclaration de confidentialité incluse dans la notification, les données peuvent être utilisées à des fins de renseignements. Le CEPD a publié un avis de contrôle préalable conjoint sur deux notifications relatives au traitement à des fins de renseignements («Banques de données d'informations et de renseignements» et «Bases de données de renseignements») le 21 novembre 2007 (dossiers CEPD n° 2007-0027 et 2007-0028).

#### *Droits des personnes concernées*<sup>14</sup>

Il convient de noter que la déclaration de confidentialité pour le CAM ne contient pas de liste des éléments de données à conserver. En ce qui concerne l'utilisation du SID dans le cadre du CAM, la déclaration de confidentialité mentionne le SID tel que notifié dans la DPO-17, c'est-à-dire l'ancienne version de la notification, et non la version actualisée DPO-17-2 qui est soumise au présent contrôle préalable.

### **2.2.3. SID**

Une version antérieure de ce système a déjà fait l'objet d'un avis de contrôle préalable publié le 24 juillet 2007 (dossier CEPD n° 2007-0177). Cependant, étant donné que sa base juridique a été modifiée par le règlement (CE) n° 766/2008 entre-temps, et que le traitement de données à caractère personnel dans le système a changé, il convient de rendre un nouvel avis de contrôle préalable.

#### *Description du traitement*

Le SID a pour mission d'aider les autorités nationales compétentes et la Commission («partenaires du SID») à prévenir, rechercher et poursuivre les opérations contraires aux réglementations douanière et agricole. À cette fin, il permet aux partenaires du SID de déclencher des alertes dans le système demandant à d'autres partenaires du SID d'entreprendre certaines actions. Plus précisément, ces alertes sont: observation et compte rendu, surveillance discrète, contrôles spécifiques et analyse opérationnelle. Ces alertes peuvent concerner des marchandises, des moyens de transport, des entreprises et des personnes. Pour les utilisateurs, il n'existe aucune différence visible entre le SID tel qu'établi par le règlement (CE) n° 515/97 et la décision 2009/917/JAI du Conseil.

#### *Base juridique*

Le SID est basé sur le titre V du règlement (CE) n° 515/97 et la décision SID (2009/917/JAI) du Conseil qui, depuis le 27 mai 2011, a remplacé la convention SID. Aux termes de l'article 23, paragraphe 2, du règlement n° 515/97, l'objectif du SID est d'aider «à prévenir, à rechercher et à poursuivre les opérations qui sont contraires aux réglementations douanière ou agricole, en renforçant, par une diffusion plus rapide des informations, l'efficacité des procédures de coopération et de contrôle des autorités compétentes visées par le présent règlement.» L'article 25, paragraphe 2, dresse une liste exhaustive des catégories de données pouvant être incluses, cette liste étant identique à celle mise en œuvre dans la base de données telle qu'énoncée ci-dessous. Les relations avec des pays tiers sont régies par le titre IV (articles 19 à 22) dudit règlement. La décision SID du Conseil contient des dispositions allant dans le même sens.

Officiellement, le SID est composé de deux parties distinctes: une établie en vertu du règlement n° 515/97 («SID UE») et une établie en vertu de la décision 2009/917/JAI du

---

<sup>14</sup> Voir l'analyse des déclarations de confidentialité dans les remarques générales.

Conseil («SID EM»). La différence entre elles réside dans les types de marchandises auxquels elles se rapportent: le SID établi en vertu de la décision du Conseil concerne les stupéfiants, les armes et certaines autres catégories telles que l'argent blanchi et les voitures volées, tandis que toutes les autres catégories relèvent du SID tel qu'établi par le règlement n° 515/97. L'avis de contrôle préalable du CEPD susmentionné tenait uniquement compte du SID tel qu'établi par le règlement n° 515/97.

#### *Catégories de données*

Les données peuvent être saisies par les autorités désignées des États membres. La distinction au niveau de la base juridique se retrouve dans les deux différents types de dossiers «SID UE» et «SID EM», en fonction de la marchandise concernée dans le dossier en question. Pour les dossiers ayant trait à des marchandises, des moyens de transport, des entreprises et des personnes, les champs de données suivants peuvent être inclus:

- 1) nom, nom de jeune fille, prénoms, noms de famille antérieurs et noms d'emprunt;
- 2) date et lieu de naissance;
- 3) nationalité;
- 4) sexe;
- 5) numéro, lieu et date d'émission des documents d'identité (passeports, cartes d'identité, permis de conduire);
- 6) adresse;
- 7) signes particuliers effectifs et permanents;
- 8) un code d'alerte avertissant que la personne a déjà porté une arme, fait usage de violence ou échappé aux autorités;
- 9) motif d'introduction des données;
- 10) action suggérée;
- 11) numéro d'immatriculation du moyen de transport.

Pour les dossiers concernant de l'argent et des marchandises détenus, saisis ou confisqués, seuls les points 1 à 4 et 6 de la liste susmentionnée seront inclus. Enfin, pour les dossiers concernant la disponibilité de l'expertise, seuls les noms et prénoms des experts seront enregistrés.

Lorsqu'une action requise a été entreprise, le partenaire du SID ayant procédé au contrôle ou entrepris une autre action requise peut transmettre cette information au partenaire du SID qui en fait la demande.

#### *Utilisateurs et gestion des utilisateurs*

Comme indiqué dans la partie générale ci-dessus, la gestion des utilisateurs se fait via l'OEU. Dans le cas du SID, l'article 29, paragraphe 2, du règlement n° 515/97, prévoit l'obligation supplémentaire de publier au Journal officiel de l'Union européenne (JO) la liste des autorités bénéficiant d'un accès. L'OLAF a informé le CEPD que la liste était actuellement réexaminée. Cette liste est indépendante de celle établie via l'OEU; l'OLAF a annoncé qu'à l'avenir, il mettrait à jour et publierait cette liste à intervalles réguliers.

#### *Destinataires des données et transferts de données*

Selon la notification, l'accès est limité aux fonctionnaires de la Commission européenne et des États membres chargés de l'application du règlement (CE) n° 515/97. Parmi ces derniers, un accès direct est uniquement accordé à ceux qui possèdent un identifiant et un mot de passe. Avec l'autorisation préalable du partenaire du SID qui a introduit les données, et sous réserve des conditions imposées par ce dernier, les informations peuvent également être transférées à d'autres autorités des États membres. L'OLAF n'introduit pas ses propres données dans le

système et il n'est donc pas en mesure d'autoriser ces transferts. Alors que la notification et la déclaration de confidentialité indiquent toutes les deux qu'il est possible de transférer des données à caractère personnel enregistrées dans le SID vers des pays tiers, l'OLAF a maintenu dans ses réponses soumises au CEPD le 26 mai 2011 qu'il ne transférerait pas de données à des pays tiers, ou à d'autres institutions, organes ou agences de l'UE, ni aux États membres; comme indiqué, des transferts vers des pays tiers peuvent être effectués avec l'autorisation de l'État membre qui a saisi les données.

#### *Droits des personnes concernées*<sup>15</sup>

Contrairement à la déclaration du CAM, cette déclaration contient une liste des catégories de données. Comparée à la liste qui figure dans la notification, elle ne mentionne aucune information concernant les documents d'identité et les adresses.

### **3. Analyse juridique**

#### **3.1. Remarques générales**

Les parties de l'analyse suivante qui s'appliquent indistinctement aux trois notifications seront examinées conjointement. Cela concerne notamment l'applicabilité du règlement n° 45/2001<sup>16</sup> («le règlement»), la question du contrôle, les droits d'accès et de rectification, ainsi que les mesures de sécurité. Lorsque les notifications diffèrent les unes des autres, elles seront examinées séparément.

#### **3.2. Contrôle préalable**

##### **3.2.1. Applicabilité du règlement**

Aux termes de l'article 3, paragraphe 1, le règlement «s'applique au traitement de données à caractère personnel par toutes les institutions et tous les organes communautaires, dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire». L'article 2, point a), définit les données à caractère personnel comme étant «toute information concernant une personne physique identifiée ou identifiable». L'article 3, paragraphe 2, dispose que le règlement s'applique «au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier».

Le traitement de données dans les trois applications constitue un traitement de données à caractère personnel. Le traitement des données est effectué par un organe de l'Union européenne dans l'exercice d'activités qui relèvent du champ d'application du droit de l'UE (article 3, paragraphe 1, du règlement, lu à la lumière du traité de Lisbonne). Le traitement des données est au moins en partie automatisé. Cet élément concerne les trois systèmes notifiés. Par conséquent, le règlement est applicable.

##### **3.2.2. Motifs de contrôle préalable**

L'article 27, paragraphe 1, du règlement, soumet au contrôle préalable du CEPD tous les «traitements susceptibles de présenter des risques particuliers au regard des droits et libertés

---

<sup>15</sup> Voir l'analyse exposée dans la partie intitulée «remarques générales».

<sup>16</sup> JO L 8 du 18.12.2000, p. 1.

des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités». L'article 27, paragraphe 2, du règlement, contient une liste de traitements susceptibles de présenter de tels risques. Cette liste comprend notamment les traitements de données «relatives à [...] des suspicions, infractions, condamnations pénales ou mesures de sûreté» (article 27, paragraphe 2, point a)). Ces données peuvent être traitées dans le cadre des trois applications notifiées. Comme l'OLAF l'a indiqué dans les notifications, ces traitements sont également destinés à «évaluer des aspects de la personnalité des personnes concernées» (article 27, paragraphe 2, point b)). Les données relatives au rôle dans le dossier sont destinées à évaluer le comportement des personnes concernées quant à la violation des réglementations douanière et agricole. Les applications sont donc soumises au contrôle préalable du CEPD.

Le contrôle préalable ayant pour objet d'étudier les situations susceptibles de présenter certains risques, le CEPD devrait rendre son avis avant que le traitement ne commence. Cependant, en l'espèce, le traitement a déjà été établi. En tout état de cause, il ne s'agit pas d'un problème grave dans la mesure où toute recommandation faite par le CEPD peut toujours être adoptée en conséquence.

### **3.2.3. Procédure**

La notification du DPD a été reçue le 11 octobre 2010. Conformément à l'article 27, paragraphe 4, du règlement, le présent avis doit être rendu dans un délai de deux mois. Au total, le délai prévu pour la publication de l'avis a été suspendu pendant 215 jours dans l'attente des réponses aux demandes de complément d'informations, d'une réunion et d'observations sur le projet d'avis définitif. Compte tenu de la complexité des dossiers, le délai a été prolongé de deux mois. Les dossiers ont en outre été suspendus durant le mois d'août 2011. Compte tenu de ces suspensions et du prolongement du délai, l'avis devrait être rendu le 15 octobre 2011 au plus tard; étant donné que cette date tombe un samedi, le CEPD rendra son avis le 17 octobre 2011 au plus tard.

### **3.3. Licéité du traitement**

Le traitement de données à caractère personnel doit être justifié au titre de l'article 5 du règlement. Dans les dossiers en question, l'article 5, point a), est applicable. Il dispose que le traitement 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 [...]». Cette disposition contient trois conditions qui doivent toutes être remplies: 1) le traitement doit être basé sur un acte juridique (les traités ou un autre acte), 2) il doit servir l'intérêt public et 3) il doit être nécessaire à la poursuite de cet intérêt public.

Les trois instruments sont au moins en partie basés sur le règlement (CE) n° 515/97. L'UCO-V et le CAM reposent entièrement sur ce dernier, tandis que le SID a ses propres dispositions dans ledit règlement, ainsi que dans la décision n° 2009/917/JAI du Conseil. Les bases juridiques de l'UCO-V et du CAM feront donc l'objet d'une analyse commune.

#### **3.3.1. UCO-V et CAM**

Ces deux instruments trouvent leur base juridique dans le règlement (CE) n° 515/97. Les articles 17 et 18 dudit règlement constituent la base du rôle de la Commission dans ces

échanges et disposent que les autorités compétentes des États membres communiquent toutes informations utiles à la Commission.

Aux termes de l'article 17, les autorités compétentes des États membres communiquent à la Commission toutes informations qui leur paraissent utiles en ce qui concerne les marchandises qui ont fait ou sont présumées avoir fait l'objet d'opérations contraires aux réglementations douanière ou agricole, les demandes d'assistance, les actions entreprises et les informations échangées en application des articles 4 à 16 (assistance spontanée et assistance sur demande) du règlement n° 515/97.<sup>17</sup> La Commission quant à elle communique aux autorités compétentes des États membres, dès qu'elle en dispose, toutes informations de nature à leur permettre d'assurer le respect des réglementations douanière et agricole.<sup>18</sup>

Aux termes de l'article 18, paragraphe 1, les États membres sont tenus d'informer la Commission des actions contraires ou paraissant être contraires aux réglementations douanière et agricole et la Commission est tenue de transmettre ces informations à l'ensemble des États membres.<sup>19</sup>

L'article 7 du règlement n° 515/97 dispose que sur demande, les autorités compétentes des États membres «exercent une surveillance spéciale» sur les mouvements de personnes et les moyens de transport dont il y a lieu raisonnablement de croire qu'ils sont utilisés pour effectuer des opérations contraires aux réglementations douanière et agricole.<sup>20</sup> L'UCO-V a pour objectif de mettre en œuvre cet article.

Les relations avec les pays tiers sont régies par l'article 19 dudit règlement et les accords d'assistance mutuelle conclus entre l'Union et les pays tiers. Les transferts potentiels vers des pays tiers ont lieu directement entre les États membres qui ont introduit les données à caractère personnel et les pays tiers; l'OLAF ne prend pas part à ces transferts.

---

<sup>17</sup> Article 17, paragraphe 1, du règlement n° 515/97: «Les autorités compétentes de chaque État membre communiquent à la Commission, dès qu'elles en disposent:

a) toutes informations qui leur paraissent utiles en ce qui concerne:

— les marchandises qui ont fait ou sont présumées avoir fait l'objet d'opérations contraires aux réglementations douanière ou agricole, [...]

— les demandes d'assistance, les actions entreprises et les informations échangées en application des articles 4 à 16 qui sont susceptibles de faire apparaître des tendances de fraude dans les domaines douanier ou agricole; [...].»

<sup>18</sup> Article 17, paragraphe 2, du règlement n° 515/97: «La Commission communique aux autorités compétentes de chaque État membre, dès qu'elle en dispose, toutes informations de nature à leur permettre d'assurer le respect des réglementations douanière et agricole.»

<sup>19</sup> Article 18, paragraphe 1, du règlement n° 515/97: «Lorsque des opérations contraires ou paraissant être contraires aux réglementations douanière et agricole sont constatées par les autorités compétentes d'un État membre et présentent un intérêt particulier sur le plan communautaire, notamment: — lorsqu'elles ont ou pourraient avoir des ramifications dans d'autres États membres ou dans des pays tiers — lorsque des opérations similaires paraissent auxdites autorités susceptibles d'avoir été également effectuées dans d'autres États membres, ces autorités communiquent à la Commission dans les meilleurs délais [...], toutes informations appropriées [...]. La Commission communique ces informations aux autorités compétentes des autres États membres.»

<sup>20</sup> Une «surveillance spéciale» peut également être demandée pour les mouvements de marchandises et les lieux de dépôt; dans ces cas, il suffit qu'ils soient «signalés comme pouvant faire l'objet d'opérations contraires aux réglementations douanière et agricole», ou qu'ils soient utilisés pour «constituer des dépôts [de marchandises] dans des conditions telles qu'elles laissent raisonnablement supposer» qu'ils ont pour but d'alimenter de telles opérations.

### **3.3.2. SID**

Le SID se différencie des autres traitements notifiés en ce sens qu'il dispose de sa propre base juridique explicite dans le règlement (CE) n° 515/97. Son objectif est énoncé à l'article 23, paragraphe 2, qui est libellé comme suit:

«L'objectif du SID, conformément aux dispositions du présent règlement, est d'aider à prévenir, à rechercher et à poursuivre les opérations qui sont contraires aux réglementations douanière ou agricole, en renforçant, par une diffusion plus rapide des informations, l'efficacité des procédures de coopération et de contrôle des autorités compétentes visées par le présent règlement.»

L'article 24 dispose que pour atteindre cet objectif, le SID «comprend exclusivement les données, y compris les données à caractère personnel, nécessaires à l'accomplissement de son objectif, tel que visé à l'article 23, paragraphe 2» regroupées dans un certain nombre de catégories, dont la liste exhaustive figure à l'article 25.

La seconde partie de sa base juridique est fournie par la décision 2009/917/JAI du Conseil, dont l'article premier, paragraphe 2, est libellé comme suit:

«L'objectif du système d'information des douanes, conformément à la présente décision, est d'aider à prévenir, rechercher et poursuivre les infractions graves aux lois nationales en rendant les données plus rapidement disponibles et en renforçant ainsi l'efficacité des procédures de coopération et de contrôle des administrations douanières des États membres.»

L'article 4, paragraphe 2, de cette décision, dresse une liste exhaustive des catégories de données à caractère personnel pouvant être incluses dans le SID.

### **3.3.3. Intérêt public et nécessité**

Afin d'être licite en vertu de l'article 5, point a), du règlement, le traitement doit également contribuer à l'intérêt public. L'objectif des trois applications qui ont été notifiées au CEPD consiste à renforcer la coopération entre la Commission, les autorités des États membres et dans certains cas les autorités de pays tiers afin de prévenir, de rechercher et de poursuivre les opérations contraires aux réglementations douanière et agricole. Le fait de garantir l'application efficace des réglementations douanière et agricole contribue à protéger les intérêts financiers de la Commission et des États membres et sert également l'intérêt public. Les traitements devraient donc être considérés comme poursuivant l'intérêt public.

Dans l'abstrait, ces échanges peuvent contribuer à protéger les intérêts financiers de la Commission et des États membres. Sans ces échanges, l'application des réglementations douanière et agricole serait considérablement entravée. L'exécution de demandes de «surveillance spéciale» serait probablement, sur une base bilatérale, inefficace pour les mouvements traversant plusieurs pays. En ce sens, l'UCO-V, le CAM et le SID peuvent être considérés comme des instruments nécessaires pour lutter contre la fraude. Il n'est pas possible d'évaluer, à un niveau abstrait, si l'introduction de données dans ces systèmes est nécessaire dans un dossier donné. En l'espèce, la nécessité doit être démontrée concrètement au cas par cas pour chaque dossier.



### **3.4. Contrôle**

Aux termes de l'article 2, point d), du règlement, on entend par «responsable du traitement: l'institution ou organe communautaire, la direction générale, l'unité ou toute autre entité organisationnelle qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel.» Pour déterminer qui est le responsable du traitement, il convient d'établir quelle est la personne qui se charge réellement du traitement.

La notification se contente d'indiquer qu'un fonctionnaire de l'OLAF est la personne responsable du traitement. Cependant, il ressort clairement de la description des traitements que les autorités compétentes des États membres devraient également être considérées comme des responsables du traitement en plus de l'OLAF.

L'organisation des systèmes laisse supposer que certaines des tâches d'un responsable du traitement ne peuvent pas être exécutées par l'OLAF mais uniquement par les autorités compétentes des États membres. Par exemple, aux termes de l'article 4, paragraphe 2, du règlement, le responsable du traitement est tenu de s'assurer que le principe de la qualité des données est respecté. L'OLAF peut y contribuer en organisant le système de telle sorte qu'aucune donnée manifestement non pertinente ne soit traitée et en fournissant des informations sur sa bonne utilisation, mais l'introduction et la modification effectives des données, la décision d'étendre ou non la conservation aux dossiers du SID<sup>21</sup>, ainsi que l'évaluation concrète des données qui devraient être introduites incombent aux autorités compétentes des États membres. Elles sont également les seules à pouvoir modifier les données qu'elles ont introduites et elles doivent garantir le droit de rectification qui selon l'article 14 incombe au responsable du traitement. Ce sont elles, et non l'OLAF, qui autorisent les transferts vers des pays tiers lorsque cela est possible.<sup>22</sup> Cela montre bien qu'elles ne peuvent pas être considérées comme de simples utilisateurs du système, étant donné que leurs décisions ont un impact considérable sur les finalités du traitement.

Pour le SID, cette approche est également confirmée par l'article 34, paragraphe 3, du règlement (CE) n° 515/97, qui prévoit que les États membres et la Commission «considèrent le SID comme un système de traitement de données à caractère personnel qui est soumis aux dispositions nationales mettant en œuvre la directive 95/46/CE, aux dispositions du règlement (CE) n° 45/2001 et aux dispositions plus strictes du présent règlement». Si l'OLAF était le seul responsable du traitement, la mention des dispositions nationales mettant en œuvre la directive 95/46/CE serait sans objet. En conséquence, le règlement (CE) n° 515/97 qualifie les autorités compétentes et la Commission de «partenaires du SID».

À cet égard, l'UCO-V, le CAM et le SID reflètent d'autres systèmes informatiques à grande échelle comme Eurodac ou le système d'information du marché intérieur dans lesquels la Commission est responsable de la mise en place et de la gestion opérationnelle, mais non du contenu exact des données introduites dans le système. L'OLAF est la partie mettant en place le système et donnant une forme concrète à l'autorisation dans la base juridique. En ce sens, il détermine (en partie) les moyens et les finalités du traitement. Les autorités compétentes quant à elles sont plus que de simples utilisateurs du système et déterminent (en partie) la finalité du traitement. Il convient donc de considérer les autorités compétentes liées aux systèmes et l'OLAF comme des co-responsables des systèmes. Cet aspect a également des implications pour la responsabilité, chaque responsable du traitement étant responsable de ses propres traitements. L'OLAF est responsable de la gestion du système central, y compris de

---

<sup>21</sup> Voir la section 3.7.1 ci-dessous.

<sup>22</sup> Voir la section 3.8.3 ci-dessous.

sa sécurité. Les autorités compétentes des États membres sont responsables de l'introduction et de la modification des données et de leur propre utilisation des systèmes.

### **3.5. Traitement portant sur des catégories particulières de données**

L'article 10, paragraphe 1, du règlement dispose que le traitement des données à caractère personnel qui révèlent 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 généralement interdits, sous réserve de certaines dérogations visées aux paragraphes 2 à 5 dudit article. L'article 10, paragraphe 2, expose les dérogations portant sur l'ensemble des catégories particulières; l'article 10, paragraphe 3, crée une dérogation pour le traitement de données relatives à la santé par des praticiens de la santé, ou par d'autres personnes soumises à une obligation de secret équivalente, pour des raisons médicales; l'article 10, paragraphe 4, autorise des dérogations supplémentaires qui peuvent être prévues par les traités ou d'autres actes législatifs adoptés sur la base de ces traités pour un motif «d'intérêt public important» ou par décision du CEPD, sous réserve de garanties appropriées. Aux termes de l'article 10, paragraphe 5, le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que sur une base juridique spécifique ou s'il est autorisé par le CEPD.

Les trois traitements notifiés portent sur des catégories particulières de données; les catégories concernées et la portée exacte de ces traitements varient selon les applications. Elles seront examinées successivement.

#### **3.5.1. UCO-V**

L'UCO-V peut être utilisée pour échanger des informations sur les suspicions de violations des réglementations douanière et agricole, à savoir les données concernant des suspicions. Le traitement de ces données particulières par l'OLAF est autorisé par l'article premier, paragraphe 2, du règlement (CE) n° 1073/99 et les dispositions respectives du règlement (CE) n° 515/97; les conditions visées à l'article 10, paragraphe 5, sont donc remplies.

#### **3.5.2. CAM**

Plusieurs catégories particulières de données peuvent être traitées dans le contexte du CAM. Selon les informations obtenues auprès de l'OLAF, le champ destiné aux alertes peut désormais contenir des informations sur la consommation de drogues et les tendances suicidaires, lesquelles constituent des données relatives à la santé. Ces dernières n'ont pas été incluses dans la notification précédente concernant les échanges d'informations relevant de l'assistance mutuelle (dossier CEPD n° 2007-0202). Il ressort du manuel d'utilisation des dossiers CAM que, en plus du fait que ces alertes proposent une sélection dans une «liste déroulante», un champ de texte libre est également prévu pour d'autres alertes. Qui plus est, le champ destiné aux traits physiques pourrait en principe également inclure des données révélant l'origine raciale, ethnique ou religieuse ou encore des données relatives à la santé. Enfin, le champ destiné aux données relatives au rôle dans le dossier est susceptible d'inclure des informations sur les suspicions.

Compte tenu des informations reçues, il n'y a aucune raison de penser que l'une quelconque des dérogations visées à l'article 10 du règlement s'applique aux nouvelles alertes qui peuvent être sélectionnées dans la «liste déroulante». Les dérogations prévues à l'article 10, paragraphe 2, du règlement, ne semblent pas s'appliquer. Elles ne peuvent pas non plus se

résumer à la dérogation visée à l'article 10, paragraphe 3, qui autorise le traitement de données relatives à la santé par un praticien de la santé ou par une autre personne soumise à une obligation de secret équivalente, aux fins de l'administration de soins ou de traitements et certains autres usages médicaux. Même si les obligations de secret des fonctionnaires de l'OLAF et des États membres étaient réputées équivalentes à celles de la profession médicale, cela n'entraînerait pas l'applicabilité de cette dérogation au traitement par l'OLAF, étant donné que ses fonctionnaires ne participeraient en aucun cas à l'administration de ces soins. L'article 10, paragraphe 4, autorise des dérogations supplémentaires pouvant être prévues par les traités, par des actes adoptés sur la base de ces traités ou sur décision du CEPD pour un motif d'intérêt public important et sous réserve de garanties appropriées. Contrairement aux alertes avertissant que la personne a déjà porté une arme, fait usage de violence ou échappé aux autorités, les nouveaux champs d'alertes ne sont pas mentionnés dans la base juridique. Par conséquent, la dérogation supplémentaire au traitement prévue dans les traités ou des actes juridiques adoptés sur la base de ces traités et visée à l'article 10, paragraphe 4, du règlement, ne s'applique pas non plus. Selon le manuel d'utilisation des dossiers CAM, un champ de texte libre est également prévu pour d'autres alertes et pourrait également inclure des catégories particulières de données.

En ce qui concerne le champ sur les signes, les utilisateurs de ce système reçoivent une formation les informant que des données permettant de tirer des conclusions quant à l'origine raciale ou ethnique ou d'autres catégories particulières de données ne doivent pas être introduites.<sup>23</sup> Outre cette information, une documentation est également mise à la disposition des utilisateurs du système notifié. Ce rappel permet de garantir qu'aucune donnée relevant du champ d'application de l'article 10, paragraphe 1, n'est traitée. Cependant, compte tenu des nombreux champs de données qui peuvent être insérés dans le CAM (voir point 2.2.2 ci-dessus), il n'est pas clairement établi si ce champ de données supplémentaire est nécessaire à l'identification des personnes concernées. Compte tenu des risques associés au champ (c'est-à-dire une interprétation erronée de ce que constituent des données relatives à la santé ou une simple désobéissance aux instructions reçues), le CEPD recommande à l'OLAF d'évaluer si ce champ est nécessaire. À cette fin, l'OLAF devrait recueillir des statistiques sur l'utilisation de ce champ et informer le CEPD des résultats dans un délai de 6 mois.

En ce qui concerne les données relatives au rôle dans le dossier, le traitement de ces données particulières par l'OLAF est autorisé par l'article premier, paragraphe 2, du règlement (CE) n° 1073/99 et les dispositions respectives du règlement (CE) n° 515/97 et remplit les conditions visées à l'article 10, paragraphe 5, du règlement.

L'OLAF devrait envisager de retirer les champs «toxicomane» et «tendances suicidaires» de la liste d'alertes. Il devrait également indiquer les raisons de l'inclusion du champ de texte libre pour les alertes et envisager de le retirer si les alertes prédéfinies sont jugées suffisantes.

### **3.5.3. SID**

La liste des données qui peuvent être introduites dans le SID, établie à l'article 25, paragraphe 2, du règlement n° 515/97, comprend au point g) «tous signes particuliers effectifs et permanents». Le paragraphe 5 dudit article précise que «[...] les données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi les données relatives à la santé ou à la vie sexuelle, ne sont pas incluses.» L'OLAF a expliqué qu'avant que les utilisateurs ne soient autorisés à accéder au système, ces limitations leur étaient rappelées lors des sessions

---

<sup>23</sup> Voir également les lignes directrices à l'intention du personnel de l'OLAF concernant la mise en œuvre pratique des exigences en matière de protection des données, p. 8-9.

de formation. Ces limitations sont également réitérées dans la documentation accessible aux utilisateurs. Ce rappel permet de garantir qu'aucune donnée relevant du champ d'application de l'article 10, paragraphe 1, n'est traitée dans ce champ. Cependant, compte tenu des nombreux champs de données qui peuvent être insérés dans le SID (voir point 2.2.3 ci-dessus), il n'est pas clairement établi si ce champ de données supplémentaire est nécessaire à l'identification des personnes concernées. Compte tenu des risques associés au champ (c'est-à-dire une interprétation erronée de ce que constituent des données relatives à la santé ou une simple désobéissance aux instructions reçues), le CEPD recommande à l'OLAF d'évaluer si ce champ est nécessaire. À cette fin, l'OLAF devrait recueillir des statistiques sur l'utilisation de ce champ et informer le CEPD des résultats dans un délai de 6 mois.

Le point i) de la liste établie à l'article 25, paragraphe 2, est «motif d'introduction des données». Cette disposition fournit une base juridique explicite pour le traitement de données relatives à des suspicions, rendant applicable la dérogation visée à l'article 10, paragraphe 5, du règlement.

L'article 4, paragraphe 2, tirets g) et h), et paragraphe 5, de la décision 2009/917/JAI du Conseil contient des dispositions qui vont dans le même sens, fournissant une base juridique pour le traitement de données relatives à des suspicions dans la partie du SID établie en vertu de cette décision.

### **3.6. Qualité des données**

L'article 4, paragraphe 1, du règlement, renferme le principe de la qualité des données. Plus précisément, l'article 4, paragraphe 1, point c), du règlement, dispose que les données à caractère personnel doivent être «adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement». En outre, les données doivent, si nécessaire, être mises à jour (article 4, paragraphe 1, point d)).

#### **3.6.1. UCO-V et CAM**

Le principe de la qualité des données est respecté dans l'UCO-V et le CAM en ce sens que i) la liste des catégories de données semble être adéquate au regard des finalités respectives, ii) les lignes directrices internes de l'OLAF stipulent que les détails concernant les personnes sont uniquement saisis si elles «sont soupçonnées d'être concernées par l'irrégularité ou la fraude» (lignes directrices à l'intention du personnel de l'OLAF concernant la mise en œuvre pratique des exigences en matière de protection des données, p. 7) et iii) lesdites lignes directrices exigent également du personnel de l'OLAF qu'il prenne «toutes les mesures raisonnables [...] pour garantir l'exactitude et la mise à jour des informations provenant des autorités nationales et utilisées et conservées par l'OLAF, ainsi que des informations collectées par l'OLAF et transmises aux autorités nationales» (p. 7), par exemple en veillant à ce que les informations mises à jour soient rapidement transférées. Pour les fonctionnaires des États membres qui ajoutent des données, l'OLAF fournit des recommandations contenant les mêmes informations.

Cela étant, le CEPD ne peut décider dans l'abstrait si ces catégories de données devraient être incluses dans tous les dossiers particuliers. La décision d'inclure ou non des catégories particulières de données doit être prise au cas par cas. L'OLAF a publié des recommandations sur la façon de satisfaire à ces exigences pour les gestionnaires de dossiers, y compris des recommandations sur la mise à jour des données (Lignes directrices à l'intention du personnel

de l'OLAF concernant la mise en œuvre pratique des exigences en matière de protection des données, titre 1.3).

Le CEPD note que les recommandations contenues dans les lignes directrices à l'intention du personnel de l'OLAF concernant la mise en œuvre pratique des exigences en matière de protection des données s'inspirent des recommandations soumises sur le plan de la qualité des données dans les précédents contrôles préalables susmentionnés.

### **3.6.2. SID**

La notification comprenait une liste de catégories de données pouvant être incluses dans le SID (champ 17). Elle est identique à la liste établie à l'article 25, paragraphe 2, du règlement (CE) n° 515/97.

Le SID respecte le principe de la qualité des données dans la mesure où i) la liste de catégories de données qui doivent être traitées semble appropriée au regard de la finalité visée, ii) les données ne peuvent être insérées que «[...] si, notamment sur la base d'activités illégales préalables ou d'une information fournie dans le cadre de l'assistance, des indices réels portent à croire que la personne en question a effectué, est en train d'effectuer ou effectuera des opérations qui sont contraires aux réglementations douanière ou agricole et qui présentent une importance particulière sur le plan communautaire» (article 27, paragraphe 2, du règlement (CE) n° 515/97), et iii) les informations sur la mise à jour des données qui sont fournies aux utilisateurs de l'UCO-V et du CAM sont également mises à la disposition de l'utilisateur du SID.

Quant à l'UCO-V et au CAM, le CEPD ne peut décider dans l'abstrait si ces catégories de données devraient être incluses dans tous les dossiers particuliers. Là encore, il est nécessaire de prendre des décisions au cas par cas. Les mêmes recommandations internes susmentionnées s'appliquent également au SID.

## **3.7. Conservation des données**

L'article 4, paragraphe 1, point e), du règlement, établit le principe selon lequel «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.» Le règlement n° 515/97 mentionne uniquement des délais de conservation pour le SID. L'OLAF a informé le CEPD que, en pratique, les procédures établies pour le SID sont également utilisées pour les autres applications notifiées. Pour cette raison, la présente section commencera par une analyse du SID avant d'examiner les autres systèmes. Dans les réponses reçues le 26 mai 2011, l'OLAF a également annoncé qu'une notification supplémentaire concernant le traitement de données à caractère personnel dans les répertoires AFIS sera ultérieurement notifiée au CEPD.

### **3.7.1. SID**

D'un point de vue juridique, l'article 33 du règlement n° 515/97 dispose que les données introduites dans le SID ne sont conservées que le temps nécessaire pour atteindre l'objectif qui a motivé leur insertion. Les partenaires ayant fourni les données examinent au moins une fois par an la nécessité de les conserver. En l'absence de réponse du partenaire ayant fourni les données dans le délai d'examen prévu pour le SID, celles-ci sont transférées dans une

partie restreinte du SID dont l'accès est limité, tant au niveau des personnes pouvant y accéder que de la finalité pour laquelle elles peuvent être utilisées (article 33, paragraphe 4). L'accès est limité aux représentants du comité qui assiste la Commission (article 43), lorsque ce comité examine la sécurité du système, la nécessité de conserver les données dans le SID, ou la confidentialité des informations enregistrées (article 43, paragraphe 4, tirets 7, 8, 9), et aux autorités de contrôle désignées par les États membres (article 37). Les données enregistrées dans cette partie du SID peuvent uniquement être consultées pour vérifier leur exactitude et la licéité du traitement et doivent être effacées au bout d'un an (article 33, paragraphe 4). Si le partenaire décide que les données sont toujours nécessaires, elles seront conservées jusqu'au prochain examen.

Pour la mise en œuvre pratique de ces exigences, l'OLAF a informé le CEPD qu'une procédure annuelle d'examen avait été mise en place. Après 11 mois, les gestionnaires de dossiers sont informés que le dossier doit faire l'objet d'un examen et sont priés d'examiner s'il est nécessaire de continuer à conserver les données. S'il n'est pas signalé dans le délai d'examen (un mois) que la durée de conservation des données doit être prolongée, les données sont effacées. La durée maximale de conservation des données est de 10 ans, la durée minimale, d'une année. En outre, le partenaire du SID ayant fourni les données peut effacer des dossiers à tout moment s'il estime qu'il est inutile de continuer à les conserver. Cette possibilité est uniquement prévue pour le SID; les autres systèmes ne contiennent pas de possibilité similaire.

Dans son avis sur la première notification concernant le SID, le CEPD a demandé à l'OLAF de fournir davantage d'informations sur la façon dont la possibilité de prolonger la durée de conservation des données est uniquement utilisée lorsque cela est nécessaire. L'OLAF a informé le CEPD qu'il n'existait aucune recommandation particulière pour aider les gestionnaires de dossiers à prendre cette décision.

Le CEPD encourage donc l'OLAF à publier des recommandations définissant une méthodologie permettant d'apprécier s'il est nécessaire ou non de continuer à conserver des données.

### **3.7.2. UCO-V**

Comme susmentionné, l'OLAF a informé le CEPD que les procédures de base utilisées pour le SID sont également appliquées à l'UCO-V. Cependant, déjà à la fin de la période post-opérationnelle, l'accès est verrouillé et les données ne sont plus accessibles. En outre, aucun prolongement de la durée de conservation n'est possible. Cela signifie qu'en pratique, les données sont effacées après un an.

L'effacement des données directement après la fin de la période post-opérationnelle semblerait être une meilleure solution, étant donné qu'il semble n'y avoir aucune raison de prolonger la durée de conservation des données: les contrôles qui établissent une violation des réglementations douanière ou agricole conduiraient à la création d'un rapport de saisie dans l'un des autres systèmes; les contrôles qui ne donnent pas de résultats positifs ne sont plus pertinents. Dans les deux cas, il ne semble pas être nécessaire de continuer à conserver des données dans l'UCO-V.

L'OLAF devrait indiquer les raisons de cette durée de conservation, étant donné qu'il ne semble pas être nécessaire de continuer à stocker les données après la conclusion d'une ODC, et informer le CEPD sur les possibilités de raccourcir cette durée.

### **3.7.3. CAM**

Les règles pour le SID sont également appliquées à d'autres types de dossiers CAM. Comme avec l'UCO-V, il n'est pas possible de prolonger la durée de conservation, ce qui signifie en pratique que celle-ci est d'un an. Le CEPD se félicite de ce changement considérable par rapport à la durée de conservation de 10 ans qui était exposée dans la notification concernant les échanges d'informations relevant de l'assistance mutuelle en vue d'un contrôle préalable.

## **3.8. Transfert de données**

Les transferts de données à caractère personnel à d'autres institutions, organes et agences de l'UE, à d'autres États membres, à des pays tiers et à des organisations internationales sont régis par les articles 7, 8 et 9 du règlement, respectivement.

### **3.8.1. Transfert à d'autres institutions, organes ou agences de l'UE**

L'OLAF a mis en place des procédures générales pour traiter les transferts à d'autres institutions et États membres de l'UE. Si ces transferts devaient avoir lieu dans le cadre des systèmes notifiés à l'avenir, elles s'appliqueraient. Ces procédures obligent le personnel de l'OLAF à vérifier i) si le destinataire visé est compétent et ii) si le transfert est nécessaire. Ces exigences doivent être satisfaites au cas par cas pour chacun des transferts. Même si le transfert est prévu dans la législation applicable, cette vérification doit toujours être effectuée (Lignes directrices à l'intention du personnel de l'OLAF concernant la mise en œuvre pratique des exigences en matière de protection des données, p. 15). Cette procédure serait également applicable pour les transferts à d'autres unités au sein de l'OLAF. Elle reflète les recommandations formulées dans le précédent dossier de contrôle préalable 2007-0202.

Dans la notification, l'OLAF a également mentionné que les DPD d'Eurojust et d'Europol ont demandé l'accès aux fichiers-journaux pour le portail AFIS, dont les systèmes examinés dans le cadre du présent avis font partie. Cela a permis à l'OLAF de se rendre compte que des données à caractère personnel sont traitées dans les journaux. L'OLAF a informé le CEPD qu'une procédure sera mise en place afin de fournir un extrait mensuel des fichiers-journaux aux deux DPD qui en ont demandé l'accès. Le CEPD invite l'OLAF à s'assurer que ces transferts satisfont aux conditions exposées dans le règlement et à en apporter la preuve.

### **3.8.2. Transfert à des États membres**

Alors que les notifications mentionnent la possibilité de tels transferts, l'OLAF a précisé qu'ils n'ont pas lieu dans la pratique.

Dans le cas du CAM et de l'UCO-V, les déclarations de confidentialité mentionnent que les données peuvent être transmises à «des autorités administratives, législatives et judiciaires compétentes des États membres». L'article premier, paragraphe 1, du règlement n° 515/97 indique clairement que la coopération entre les autorités administratives des États membres et la Commission est l'objectif dudit règlement. De même, les notifications désignent les destinataires potentiels des États membres comme étant les «autorités compétentes des États membres [...] chargées de l'application du règlement (CE) n° 515/97». Les catégories d'autorités mentionnées dans les déclarations de confidentialité sont considérablement plus larges que celles qui sont définies dans la base juridique. En revanche, la déclaration de confidentialité pour le SID indique que les données peuvent être transmises aux «autorités administratives compétentes des États membres», conformément à la base juridique.

En vertu de l'article 30, paragraphe 4, du règlement (CE) n° 515/97, les données à caractère personnel provenant du SID peuvent être transférées à d'autres autorités nationales ou à des pays tiers, avec l'autorisation préalable du partenaire du SID qui a introduit les données dans le système et sous réserve des conditions qu'il a imposées au transfert. Si à l'avenir, l'OLAF devait introduire des données, les procédures telles qu'établies dans les lignes directrices à l'intention du personnel de l'OLAF concernant la mise en œuvre pratique des exigences en matière de protection des données (p. 14 à 17) s'appliqueraient.

La liste des autorités ayant accès au SID telle qu'établie en vertu du règlement n° 515/97 devra, conformément à l'article 29, paragraphe 2, dudit règlement, être publiée au JO, ce qui n'a pas été le cas jusqu'à présent. Hormis ces listes officielles, des listes internes ont été établies par l'OLAF pour la gestion des utilisateurs sur le plan technique, lesquelles ont été mentionnées dans la partie générale ci-dessus (2.1, rubrique «utilisateurs et gestion des utilisateurs»). Il n'existe aucun lien officiel entre ces listes.

L'OLAF devrait détailler la procédure d'établissement des listes internes des autorités ayant accès au SID pour la gestion des utilisateurs sur le plan technique. Ces listes devraient être régulièrement mises à jour. En outre, l'OLAF devrait également, dans la mesure du possible, promouvoir activement la mise à jour et la publication des listes officielles. Les types d'autorités renseignés dans les déclarations de confidentialité du CAM et de l'UCO-V devraient être mis à jour afin de refléter la base juridique et les autorités bénéficiant d'un accès.

### **3.8.3. Transfert à des pays tiers et des organisations internationales**

Selon les notifications ou les documents d'accompagnement, des transferts à des pays tiers peuvent être effectués dans les trois applications. Dans ses réponses du 26 mai 2011, l'OLAF a précisé qu'en réalité ces transferts n'avaient pas lieu pour le SID. Les transferts vers des pays tiers sont régis par l'article 9 du règlement.

Pour les données introduites dans les systèmes par les États membres, des transferts depuis le SID peuvent être effectués «avec l'autorisation préalable de, et sous réserve des conditions imposées» par l'État membre qui a introduit les données, comme prévu à l'article 30, paragraphe 4, du règlement (CE) n° 515/97. L'OLAF ne joue aucun rôle dans ce processus. De ce fait, l'évaluation des procédures mises en place ne relèverait pas du champ d'application du présent avis de contrôle préalable. Cependant, le second alinéa de la disposition mentionnée dispose qu'elle s'applique mutatis mutandis vis-à-vis de la Commission lorsque c'est elle qui a introduit les données dans le système. Comme susmentionné dans la description des faits, les données sont introduites par les États membres uniquement. Si cette situation devait changer, et que l'OLAF devait commencer à introduire des informations dans les systèmes, lesquelles pourraient alors être transférées vers des pays tiers, l'OLAF devrait également mettre en place des mesures appropriées pour s'assurer que les conditions visées à l'article 9 du règlement sont bien remplies.

La question des transferts de données à des pays tiers et des organisations internationales est traitée de manière horizontale dans les dossiers 2005-0154 et 2006-0493. Il n'y a pas lieu d'examiner cet aspect plus avant dans le présent avis.



### **3.9. Droit d'accès et de rectification**

Les articles 13 et 14 du règlement confèrent aux personnes concernées un droit d'accès et de rectification. Ce droit est soumis à certaines exceptions et limitations qui sont exposées à l'article 20 du règlement. Étant donné que les dispositions correspondantes dans les déclarations de confidentialité des applications notifiées sont presque identiques, elles peuvent être considérées conjointement.

Les trois déclarations de confidentialité contiennent des dispositions presque identiques aux termes desquelles les personnes concernées «peuvent» obtenir l'accès à leurs données, à moins que les exceptions visées à l'article 20 du règlement ne s'appliquent. La seule différence réside dans le fait que les déclarations pour le CAM et l'UCO-V citent l'article 20 en général, tandis que la déclaration pour le SID précise que les exceptions visées à l'article 20, paragraphe 1, points a), b) et c), peuvent s'appliquer.

Les procédures mises en place par l'OLAF pour traiter ces demandes sont détaillées au titre 1.5 des lignes directrices à l'intention du personnel de l'OLAF concernant la mise en œuvre pratique des exigences en matière de protection des données. Les instructions qui y sont contenues mettent en œuvre les recommandations faites par le CEPD dans ses précédents avis sur le SID et les échanges d'informations relevant de l'assistance mutuelle (dossiers 2007-0177 et 2007-0202).

Pour l'UCO-V, l'OLAF a indiqué dans les réponses soumises au CEPD le 26 mai 2011 que l'accès serait probablement refusé durant la phase opérationnelle d'une ODC. L'article 20, paragraphe 1, point a), du règlement autorise de telles limitations si elles constituent des mesures nécessaires pour assurer «la prévention, la recherche, la détection et la poursuite d'infractions pénales». Plus précisément, l'article 36, paragraphe 2, second alinéa, du règlement n° 515/97 dispose que «l'accès peut être refusé à toute personne dont les données sont traitées pendant la période durant laquelle des actions sont menées aux fins d'observation et de compte rendu ou de surveillance discrète ainsi que pendant la période durant laquelle l'analyse opérationnelle des données ou l'enquête administrative ou pénale est en cours». En outre, l'autorité qui a introduit les données a la possibilité de donner son avis avant que toute donnée soit communiquée aux personnes concernées. Le fait de communiquer des informations à la personne concernée alors que l'enquête est toujours en cours pourrait compromettre le succès de ladite enquête; c'est pourquoi un report de l'accès pourrait être justifié dans ces cas. Cependant, tout report doit être décidé au cas par cas. Ces dispositions ne peuvent pas être utilisées pour refuser systématiquement l'accès. Les informations doivent être communiquées à la personne concernée dès que les exceptions ne s'appliquent plus. Même si l'une des exceptions visées à l'article 20, paragraphe 1, s'applique, le responsable du traitement est tenu en vertu de l'article 20, paragraphe 3, d'informer la personne concernée des raisons principales du report de l'accès et de son droit de saisir le CEPD. L'article 20, paragraphe 4, dispose que dans ces cas, lorsque le CEPD examine les réclamations des personnes concernées, il leur fait uniquement savoir si les données ont été traitées correctement et, dans la négative, si toutes les corrections nécessaires ont été apportées. Aux termes de l'article 20, paragraphe 5, ces informations peuvent être reportées aussi longtemps qu'elles privent d'effet la limitation imposée sur la base de l'article 20, paragraphe 1.

L'OLAF devrait clairement indiquer que les informations sont communiquées aux personnes concernées dès que possible et que les exceptions visées à l'article 20 du règlement ne sont utilisées qu'au cas par cas.

### **3.10. Information de la personne concernée**

Pour les personnes concernées relevant de la catégorie I, on peut supposer que les informations relatives à leurs actions fautives alléguées ne sont pas collectées auprès d'elles mais qu'elles proviennent d'autres sources. L'article 12 du règlement est donc la disposition applicable. En vertu de cet article, les personnes concernées ont le droit d'être informées de l'identité du responsable du traitement, des finalités du traitement, des catégories de données concernées, des destinataires ou des catégories de destinataires, de l'existence d'un droit d'accès aux données les concernant et de rectification de ces données, de la base juridique du traitement auquel les données sont destinées, des délais de conservation des données, du droit de saisir, à tout moment, le Contrôleur européen de la protection des données, et de l'origine des données, sauf si le responsable du traitement ne peut divulguer cette information pour des raisons de secret professionnel. Si les personnes concernées n'ont pas connaissance du fait que des données les concernant sont traitées, elles ne peuvent pas exercer leurs droits d'accès et de rectification; c'est pourquoi une information appropriée est indispensable à la garantie de leurs droits.

Les personnes concernées sont informées du traitement potentiel des données à caractère personnel les concernant au moyen des déclarations de confidentialité qui sont publiées sur le site web de l'OLAF. Ces déclarations satisfont à la plupart des exigences visées à l'article 12. Cependant, elles présentent certaines lacunes:

- les déclarations de confidentialité du CAM et de l'UCO-V ne contiennent pas de liste des catégories de données qui peuvent être incluses dans les systèmes;
- la référence au SID dans la déclaration de confidentialité du CAM renvoie au SID tel que notifié dans la DPO-17, et non dans la version examinée dans le cadre du présent contrôle préalable;
- même si la déclaration de confidentialité du SID contient une liste de catégories de données, elle n'est pas exacte: les documents d'identité et les adresses n'y figurent pas;
- dans l'ensemble des notifications, les références à la base juridique pourraient être plus précises.

En ce qui concerne les informations personnalisées, c'est-à-dire non pas les informations générales selon lesquelles des données peuvent être traitées, mais les informations sur le contenu des données traitées relatives à une personne concernée déterminée, l'OLAF a informé le CEPD que ces informations seront communiquées uniquement si elles sont «appropriées» et avec l'autorisation préalable du partenaire ayant fourni les données. Les exceptions visées à l'article 20 du règlement peuvent s'appliquer au cas par cas. Les procédures mises en place pour informer les personnes concernées de façon anticipée sont exposées à l'annexe 5 du manuel de l'OLAF, titres 1.5 et 2. Si les exceptions visées à l'article 20, paragraphe 1, sont invoquées, les personnes concernées doivent tout de même être informées des principales raisons qui motivent ces exceptions et de leur droit de saisir le CEPD. Cette information peut être reportée aussi longtemps qu'elle prive d'effet la limitation imposée sur la base du paragraphe 1. Ces dispositions ne peuvent pas être utilisées pour reporter l'accès indéfiniment; dès que les raisons du report ne sont plus valables, cette information doit être communiquée.

En ce qui concerne les informations introduites par les autorités des États membres, elles doivent être communiquées par les autorités, tenant compte de leurs obligations en tant que co-responsables du traitement.<sup>24</sup>

---

<sup>24</sup> Voir la section 3.4 ci-dessus.

S'agissant des personnes concernées relevant de la catégorie II dans les États membres, l'OLAF informe les autorités respectives des États membres qu'elles doivent fournir des informations appropriées à leurs fonctionnaires avant qu'ils ne commencent à utiliser les systèmes. Pour les personnes concernées relevant de la catégorie II qui sont fonctionnaires dans des organisations internationales, il ne ressort pas clairement des informations fournies si elles reçoivent ou non des informations similaires. De même, il n'est pas clairement établi comment les personnes employées à l'OLAF pour travailler sur ces systèmes sont informées de leurs droits et du traitement portant sur leurs données, qui est différent de celui des personnes concernées relevant de la catégorie I.<sup>25</sup> Elles ont accès aux lignes directrices à l'intention du personnel de l'OLAF concernant la mise en œuvre pratique des exigences en matière de protection des données qui contiennent des informations sur leurs droits, mais d'après les informations dont dispose le CEPD, elles ne semblent recevoir aucune déclaration de confidentialité les informant précisément de leurs droits et des modalités d'exercice de ces droits.

L'OLAF devrait donc actualiser les déclarations de confidentialité de l'UCO-V et du CAM en y intégrant des listes exhaustives de catégories de données. Il devrait également inclure une référence mise à jour à la notification du SID dans la déclaration de confidentialité du CAM, et rectifier la liste des catégories de données dans la déclaration de confidentialité du SID. Les trois notifications devraient être mises à jour et intégrer des références plus précises aux bases juridiques. Les déclarations mises à jour devraient être publiées immédiatement sur le site web de l'OLAF. L'OLAF devrait également veiller à ce que des informations appropriées soient fournies aux personnes concernées relevant de la catégorie II parmi son propre personnel et dans les organisations internationales.

### **3.11. Mesures de sécurité**

[...]

## **4. Conclusion:**

Le traitement proposé ne paraît pas entraîner de violation des dispositions du règlement n° 45/2001 pour autant qu'il soit tenu compte des observations faites ci-dessus.

Les recommandations du CEPD peuvent être résumées de la manière suivante:

Recommandations concernant l'UCO-V:

- Mettre à jour la déclaration de confidentialité en y intégrant la liste exhaustive des catégories de données et mettre à jour la liste des autorités afin de refléter la base juridique. Intégrer une référence plus précise à la base juridique. Publier immédiatement la déclaration de confidentialité mise à jour sur le site web de l'OLAF.
- Énoncer des règles claires pour les durées de conservation et indiquer les raisons de la durée de conservation, compte tenu du fait que les ODC se déroulent généralement dans un court laps de temps, et informer le CEPD des possibilités de raccourcir cette durée.

---

<sup>25</sup> La durée de conservation des journaux d'audit, p. ex., ne présente pas d'intérêt pour les personnes concernées relevant de la catégorie I mais elle en présente un pour les personnes concernées relevant de la catégorie II.

- Veiller à ce que des informations appropriées soient fournies aux personnes concernées relevant de la catégorie II parmi le personnel de l'OLAF et dans les organisations internationales.

#### Recommandations concernant le CAM:

- Envisager de retirer «toxicomane» et «tendances suicidaires» de la liste des alertes qui peuvent être introduites dans les dossiers CAM afin de refléter la base juridique. Intégrer également une référence plus précise à la base juridique. Publier immédiatement la déclaration de confidentialité mise à jour sur le site web de l'OLAF.
- Indiquer les raisons de l'inclusion du champ de texte libre pour les «autres alertes» et envisager de le retirer si les alertes prédéfinies sont jugées suffisantes. Évaluer si le champ sur les signes est nécessaire. À cette fin, l'OLAF devrait recueillir des statistiques sur l'utilisation de ce champ et informer le CEPD des résultats dans un délai de 6 mois.
- Mettre à jour la déclaration de confidentialité en y intégrant la liste exhaustive des catégories de données et inclure une référence mise à jour à la notification du SID. En outre, mettre à jour la liste des autorités mentionnées dans la déclaration de confidentialité afin de refléter la base juridique.
- Veiller à ce que des informations appropriées soient fournies aux personnes concernées relevant de la catégorie II parmi le personnel de l'OLAF et dans les organisations internationales.

#### Recommandations concernant le SID:

- Rectifier la liste des catégories de données dans la déclaration de confidentialité. Intégrer également une référence plus précise à la base juridique. Publier immédiatement la déclaration de confidentialité mise à jour sur le site web de l'OLAF. Fournir des informations appropriées également au personnel de l'OLAF travaillant dans le système.
- Évaluer si le champ sur les signes est nécessaire. À cette fin, l'OLAF devrait recueillir des statistiques sur l'utilisation de ce champ et informer le CEPD des résultats dans un délai de 6 mois.
- Envisager de soumettre des recommandations aux responsables prenant la décision de prolonger ou non la durée de conservation des données.
- La procédure d'établissement des listes internes d'autorités ayant accès au SID pour la gestion des utilisateurs sur le plan technique devrait être détaillée. Ces listes devraient être régulièrement mises à jour.
- En ce qui concerne la procédure d'établissement des listes d'autorités ayant accès au SID en vertu de l'article 29, paragraphe 2, du règlement n° 515/97, l'OLAF devrait, dans la mesure du possible, promouvoir activement la publication des listes officielles. Ces listes devraient également être régulièrement mises à jour.

#### Recommandations concernant la sécurité des systèmes associés à AFIS:

- [...]

Fait à Bruxelles, le 17 octobre 2011

(signé)

Giovanni BUTTARELLI  
Contrôleur adjoint européen de la protection des données