LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

**Avis sur la notification d'un contrôle préalable reçue du délégué à la protection des données de l'Office de lutte antifraude (OLAF) concernant la «Investigative Data Consultation Platform»**

Bruxelles, le 18 juillet 2013 (affaire 2012-0280)

## 1. PROCÉDURE

Le 23 mars 2012, le contrôleur européen de la protection des données («CEPD») a reçu du délégué à la protection des données («DPD») de l'Office de lutte antifraude («OLAF») une notification en vue d'un contrôle préalable à propos de la «Investigative Data Consultation Platform» (la «plateforme IDCP»). Le DPD a joint les documents suivants à la notification:

- une note contenant une description du traitement (la «note») et
- une annexe contenant une liste des types d'entités et champs de données qui seront utilisés pour créer la base de données (l'«annexe»).

Au cours de la procédure, le CEPD a demandé à l'OLAF de fournir certaines informations complémentaires par écrit et lors de réunions, à diverses occasions. Compte tenu de la complexité de l'affaire, le CEPD a prolongé de deux mois le délai de remise de l'avis, conformément à l'article 27, paragraphe 4, du règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires, et à la libre circulation de ces données (le «règlement»).

Le 13 mai 2013, l'OLAF a retiré la notification initiale pour la remplacer par une nouvelle notification.

## 2. LES FAITS

La nouvelle notification porte sur la conception, le développement et l'utilisation d'une plateforme destinée à l'échange réciproque d'informations relatives à des enquêtes entre l'OLAF et ses partenaires internationaux. Elle soulève des problèmes complexes très importants, tant pour les enquêtes antifraude que pour la politique de protection des données.

L'OLAF considère la fraude et la corruption comme des phénomènes mondiaux qui doivent être traités au niveau international avec des instruments flexibles, rapides et efficaces, ainsi que dans le cadre d'une coopération renforcée et d'un échange d'informations entre les services d'enquête. La coopération avec des pays tiers et des organisations internationales est donc considérée comme un élément essentiel des activités de l'OLAF. Dans l'exercice de sa mission de protection des ressources financières de l'Union européenne, l'OLAF entend se baser sur un

Adresse postale: rue Wiertz 60 – B-1047 Bruxelles
Bureaux: rue Montoyer 30
Courriel: edps@edps.europa.eu – Site Internet: www.edps.europa.eu
Tél.: 02-283 19 00 – Fax: 02-283 19 50

réseau de partenaires d'enquête, administratifs et judiciaires, ainsi que de partenaires équivalents au sein d'organisations internationales. L'OLAF relève que ces partenaires ont souvent un rôle clé dans l'exercice de responsabilités de contrôle majeures dans divers projets financés par l'Union européenne, qui se déroulent en dehors de son territoire. Dans de telles situations, selon l'OLAF, la réussite d'une enquête dépend en grande partie de sa capacité à recueillir les informations nécessaires auprès de ses homologues internationaux.

Du point de vue de la protection des données, la présente affaire a également de vastes implications politiques. Conformément au règlement (CE) n° 45/2001 (le «règlement»), les transferts de données à des pays tiers ou à des organisations internationales sont soumis à des conditions strictes. Dans la mesure où les transferts réguliers de données à des pays tiers ou des organisations internationales n'assurent pas un niveau de protection adéquat, ils sont en principe interdits. Dans ces situations, le CEPD peut accorder des autorisations, mais uniquement sous réserve de la mise en place de garanties adéquates. Afin d'apprécier l'adéquation des garanties, il est nécessaire de tenir compte non seulement du contenu des règles applicables aux données transférées à des pays tiers ou à des organisations internationales, mais également des mécanismes destinés à assurer l'efficacité de telles règles.

Le CEPD considère qu'une enquête antifraude efficace doit en principe être compatible avec un niveau élevé de protection des données à caractère personnel, dès lors que toutes les garanties nécessaires en matière de protection des données sont mises en place. Nous reconnaissons que la lutte contre la criminalité transnationale ne peut fonctionner sans un certain niveau d'échange d'informations. De la même façon, l'échange renforcé d'informations utiles devrait intervenir dans le respect du droit fondamental à la protection des données et, partant, sur la base des conditions strictes énoncées par la législation. Les considérations relatives à la protection des données devraient être perçues comme facilitant la confiance dans la lutte contre la fraude, par la promotion d'un traitement équitable, proportionné et efficace des données à caractère personnel.

Le CEPD analysera le traitement notifié à la lumière des considérations susvisées, dans le but de trouver le bon équilibre, en conformité avec le règlement, entre la protection des données à caractère personnel et les intérêts publics liés à l'enquête sur la fraude et les activités de corruption et leur détection. En particulier, le CEPD concentrera l'analyse sur les modalités et garanties du traitement des données permettant des échanges nécessaires et proportionnés et assurant la responsabilité des parties prenantes.

### 2.1. Finalité du traitement

L'analyse ci-après repose sur la description du traitement fournie par l'OLAF.

La plateforme IDCP est décrite comme une base de données développée à l'aide de la technologie iBase. Elle contiendra un sous-ensemble de données provenant des fichiers d'enquête de l'OLAF et de partenaires internationaux choisis (les «partenaires IDCP»). La plateforme IDCP doit permettre aux utilisateurs d'échanger efficacement des informations sur des enquêtes en cours. Le fonctionnement de la base de données est décrit plus en détail dans la partie 2.2. L'OLAF a indiqué que des accords pratiques concernant la plateforme IDCP seraient d'abord conclus avec une organisation internationale donatrice. À l'avenir, un nombre limité d'autres organisations internationales d'importance similaire et, éventuellement, des autorités compétentes d'États membres et de tiers, devraient devenir partenaires.

Dans le cadre de son activité, l'OLAF négocie et conclut les «accords de coopération administrative» (les «accords de coopération») avec certains partenaires choisis. Les accords de coopération encadrent la coopération pratique entre l'OLAF et les pays tiers et organisations internationales qui sont ses partenaires, et fournissent notamment des règles et des garanties en matière d'échange d'informations. Ils énoncent également en annexe des clauses et des principes de protection des données qui doivent être respectés par les parties aux accords de coopération lors de l'échange de données à caractère personnel. La conclusion d'un accord de coopération avec l'OLAF est une condition préalable pour devenir un partenaire de la plateforme IDCP. Le projet d'accord de coopération type et les clauses types en matière de protection des données ont été soumis au CEPD pour consultation préalable en vertu de l'article 46, point d), du règlement, le 26 janvier 2012. Le CEPD a fait part de sa position les 3 avril et 16 juillet 2012[1].

## 2.2. Description du traitement

La plateforme IDCP contiendra un sous-ensemble de données extraites des fichiers d'enquête des partenaires IDCP. Ce sous-ensemble de données correspond aux principales caractéristiques de l'enquête, qui sont regroupées sous les «entités de données» suivantes: 1) enquête, 2) personne, 3) organisation/entreprise, 4) lieu, 5) adresse, et 6) communication. Chaque entité de données contient un certain nombre de «champs de données». Par exemple, les champs de l'entité de données «enquête» sont les suivants:

- nom de l'affaire,
- numéro de l'affaire,
- type d'affaire (par exemple enquête, coordination),
- brève description de l'affaire (par exemple «fraude alléguée au sein d'un réseau d'entreprises en lien avec des fonds de l'Union européenne dans le pays X»),
- allégation principale (par exemple détournement de fonds, escroquerie et malversation, soumission modifiée d'offres avant le début de la phase d'évaluation),
- méthode d'escroquerie (par exemple demandes et frais irrecevables, non-respect de clauses contractuelles, conflit d'intérêts, irrégularité dans la procédure d'adjudication),
- zone géographique,
- date d'ouverture,
- date de clôture,
- stade de l'affaire.

L'ensemble des champs de données est repris dans la partie 2.4 ci-dessous.

Pour chacun de leurs fichiers d'enquête, les partenaires IDCP extrairont les champs de données correspondant aux six entités. S'agissant des fichiers de l'OLAF, les données seront notamment extraites de fichiers d'affaires en lien avec les domaines de l'aide extérieure et des dépenses directes, mais pourront aussi inclure d'autres secteurs de dépenses. L'extraction sera limitée aux documents postérieurs à 2003.

En outre, toutes les entités comprennent les champs de données suivants, à des fins de maintenance: hyperlien source, date de création, utilisateur ayant créé le fichier, date de dernière mise à jour, dernier utilisateur ayant mis le fichier à jour et identificateur d'enregistrement.

[1] Voir avis du CEPD des 3 avril et 16 juillet 2012 sur les clauses types de l'OLAF en matière de protection des données, à utiliser dans les accords de coopération administrative (ACA) conclus avec les autorités de pays tiers ou avec des organisations internationales, disponibles sur le site Internet du CEPD.

Les partenaires de l'OLAF lui enverront par voie électronique des ensembles de données identiques concernant les entités de données susvisées. L'OLAF saisira les données dans la base de données et effectuera toutes les opérations nécessaires à son fonctionnement. Ce transfert se déroulera de façon régulière et par l'intermédiaire d'un «protocole spécifique de courriel sécurisé».

La plateforme IDCP permettra aux partenaires IDCP d'effectuer des recherches à partir de termes. Il n'est prévu aucune limitation ni aucune règle particulière concernant le choix des termes: le système affichera toutes les entités de la base de données de la plateforme IDCP qui correspondent au terme utilisé. Par exemple, une recherche sur le nom d'une personne affichera toutes les entités de données dont les champs contiennent ce nom, y compris l'entité «enquête» associée pour toutes les affaires sauvegardées dans la base de données. En outre, la base de données montrera les *liens* entre cette entité et les autres entités «enquête», «communication», «adresse» et «organisation/entreprise» liées. Une recherche sur le nom d'une personne pourrait donc donner des résultats dans l'entité de données «*personne*» si le nom correspond à celui d'une personne qui fait l'objet d'une enquête et dans l'entité «*organisation/entreprise*» si le nom est compris dans le ou les noms de l'organisation (y compris l'adresse pertinente). En outre, la base de données montrera les *liens* entre cette entité «personne» et les autres entités «enquête», «communication», «adresse» et «organisation/entreprise» liées. Il est techniquement possible de limiter le nombre de résultats fournis aux utilisateurs pour une recherche donnée. Ainsi, l'utilisateur verra uniquement les résultats jusqu'à un certain seuil prédéfini (si le seuil est fixé à 200, l'utilisateur ne verra que les 200 premiers résultats).

Le partenaire (ou l'OLAF) pourra demander un affichage graphique schématique des liens. Si le partenaire clique ensuite sur l'une des entités correspondantes sur l'affichage schématique, toutes les autres entités liées à l'entité sélectionnée apparaîtront. Le partenaire pourra aussi demander une présentation des champs de données pour chaque entité. Cette extension des entités liées sera limitée au seuil prédéfini.

Le partenaire ou l'OLAF, s'il souhaite obtenir des informations complémentaires, devra contacter l'OLAF ou le partenaire IDCP concerné et solliciter un accès aux informations, conformément à l'accord de coopération applicable. Cet éventuel échange ultérieur de données à caractère personnel (qui doit également satisfaire aux exigences des transferts de données prévues à l'article 9 du règlement) n'est pas couvert par le présent contrôle préalable.

### 2.3. Personnes concernées

Les personnes concernées par ce traitement relèvent des catégories suivantes:

- personnes physiques qui font ou ont fait l'objet d'enquêtes externes de l'OLAF;
- personnes physiques qui ont fourni des informations à l'OLAF ou à ses partenaires en qualité de témoins;
- personnes physiques dont le nom apparaît dans les informations fournies par les partenaires IDCP de l'OLAF.

Lors d'échanges ultérieurs avec le CEPD, l'OLAF a précisé que les informateurs, dénonciateurs et témoins seraient spécifiquement exclus de la plateforme IDCP.

## 2.4. Catégories de données

Dans la notification, l'OLAF indique que les entités et champs de données correspondants suivants seront traités dans la base de données IDCP:

- données d'identification: nom complet, nom de famille, prénom, surnom, date de naissance, âge, lieu de naissance et pays de naissance (tableau «personne»);
- données de contact: adresse, téléphone, courriel, site Internet et télécopieur (tableaux «communication» et «adresse postale»);
- données professionnelles: rôle au sein de l'entreprise, adresse, téléphone, courriel, site Internet et télécopieur (tableau «organisation/entreprise»);
- données relatives à l'implication dans l'affaire: nom de l'affaire, brève description de l'affaire, allégation principale. La nature de l'implication d'une personne/d'un opérateur économique n'est pas indiquée.

Le rapport de conception iBase joint en annexe à la notification contient une configuration plus détaillée des types d'entités et des champs de données qui seront utilisés aux fins de la base de données. La liste des champs de données a été modifiée et mise à jour dans le cadre des procédures. Selon les informations reçues, la liste complète se présente comme suit:

Les champs de données présentés pour l'entité «*enquête*» seront les suivants:

- nom de l'affaire,
- numéro de l'affaire,
- type d'affaire (par exemple enquête, coordination),
- brève description de l'affaire (par exemple «fraude alléguée au sein d'un réseau d'entreprises en lien avec des fonds de l'Union européenne dans le pays X»),
- allégation principale (par exemple détournement de fonds, escroquerie et malversation, soumission modifiée d'offres avant le début de la phase d'évaluation),
- méthode d'escroquerie (par exemple demandes et frais irrecevables, non-respect de clauses contractuelles, conflit d'intérêts, irrégularité dans la procédure d'adjudication),
- zone géographique,
- date d'ouverture,
- date de clôture,
- stade de l'affaire.

Les champs de données présentés pour l'entité «*personne*» seront les suivants:

- nom complet,
- icône,
- prénom,
- nom de famille,
- surnom,
- date de naissance,
- âge,
- date de naissance incomplète,
- lieu de naissance,
- pays de naissance.

Les champs de données présentés pour l'entité «*organisation/entreprise*» seront les suivants:

- icône,
- nom de l'organisation,
- nom du profil commercial,
- type,
- nationalité,
- activité.

Les champs de données présentés pour l'entité «*adresse*» seront les suivants:

- nom de la rue,
- numéro du bâtiment,
- étage,
- code postal,
- ville, région,
- pays,
- nom d'emplacement.

Les champs de données présentés pour l'entité «*communication*» seront les suivants:

- icône,
- numéro de dispositif,
- région,
- code pays,
- ville.

L'OLAF indique qu'aucune catégorie spéciale de données ne sera transférée par l'intermédiaire de la plateforme IDCP.

### 2.5. Droits d'information

D'après la notification, les personnes concernées seront informées normalement du traitement réalisé dans le contexte de telles enquêtes par la voie des déclarations relatives à la protection des données et par d'autres moyens prévus dans le contexte de ces enquêtes. Si une dérogation s'applique en vertu de l'article 20 du règlement, ces informations seront fournies dès que les conditions de la dérogation ne seront plus satisfaites.

Sur demande, l'OLAF fournira aux personnes concernées une copie de l'accord de coopération correspondant et de son annexe. Les procédures pertinentes sont présentées dans les notifications relatives aux enquêtes externes et ont été analysées dans le contexte de l'avis du CEPD sur les procédures d'enquête révisées de l'OLAF[2].

### 2.6. Catégories de destinataires auxquels des données peuvent être communiquées

L'accès à la plateforme est réservé à un petit nombre de collaborateurs de l'OLAF chargés de la sélection des affaires, à des analystes opérationnels, et au personnel désigné du partenaire correspondant de l'OLAF. Ces destinataires auront directement accès à la plateforme et aux données à caractère personnel correspondantes.

[2] Avis du CEPD sur les procédures d'enquête révisées de l'OLAF, du 3 février 2012, disponible sur le site Internet du CEPD dans la rubrique Supervision/Contrôles préalables/Avis.

La notification mentionne aussi d'éventuels destinataires dans le cadre d'échanges manuels ultérieurs de données à caractère personnel. Ces échanges ne font cependant pas l'objet du présent contrôle préalable.

### 2.7. Conservation des données

Les données à caractère personnel qui font l'objet du présent traitement seront sauvegardées pendant dix ans. À l'issue d'une période de conservation de trois ans, les données seront soumises à des examens annuels dans le cadre de contrôles automatisés et manuels, afin de garantir qu'elles sont détenues conformément à la période de conservation convenue. L'OLAF pourra conserver des données à caractère personnel pertinentes dans ses fichiers d'enquête pour une durée maximale de 15 ans, conformément aux règles applicables à de telles enquêtes[3]. Les données reçues de partenaires IDCP seront conservées par l'OLAF pendant la période demandée par le partenaire transmettant les données. Dans ces situations, la période de conservation fondamentale sera de dix ans.

### 2.8. Droit d'accès

S'agissant du droit d'accès, l'OLAF renvoie aux déclarations relatives à la protection des données pour les enquêtes externes. Les procédures applicables sont présentées dans la notification de l'OLAF relative aux enquêtes externes et ont été analysées dans le contexte de l'avis correspondant du CEPD[4].

### 2.9. Mesures de sécurité

La notification fournit des informations de base sur les contrôles de sécurité mis en œuvre au sein de l'OLAF (contrôles de sécurité de base), quels que soient les besoins spécifiques du système. Ces contrôles de sécurité contribuent à l'assurance globale du niveau de sécurité mis en œuvre sur tous les systèmes de l'OLAF.

Une description complémentaire des contrôles de sécurité spécifiques à la plateforme IDCP a été fournie à la suite, et en réponse aux questions du CEPD. [...]

## 3. ASPECTS JURIDIQUES

### 3.1. Contrôle préalable

La plateforme IDCP est destinée à l'échange réciproque d'informations relatives à des enquêtes entre l'OLAF et ses partenaires IDCP, c'est-à-dire des organisations internationales et éventuellement les autorités nationales d'États membres et de pays tiers. Les informations échangées contiendront des données à caractère personnel sur les personnes qui font l'objet d'une enquête. La plateforme impliquera donc le traitement de données à caractère personnel. Le traitement sera effectué par une institution européenne, dans l'exercice d'activités qui relèvent du champ d'application du droit communautaire (article 3, paragraphe 1, du règlement). Le traitement de données à caractère personnel sera automatisé (article 3, paragraphe 2, du règlement). Par conséquent, le règlement trouve application.

---

[3] *Ibidem*.

[4] Cité ci-dessus. Voir également avis du CEPD sur les enquêtes externes de l'OLAF du 4 octobre 2007 (affaires 2007-0047 et autres), disponible sur le site Internet du CEPD.

L'article 27, paragraphe 1, du règlement, soumet à un contrôle préalable du CEPD tous «*les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités*». L'article 27, paragraphe 2, du règlement, contient une liste des traitements susceptibles de présenter de tels risques. Conformément à l'article 27, paragraphe 2, point a), du règlement, des opérations de traitement relatives à des «suspicions, infractions, condamnations pénales ou mesures de sûreté» doivent faire l'objet d'un contrôle préalable par le CEPD. En l'espèce, le traitement pourrait être lié au traitement de ces types de données.

La notification du DPD a été reçue le 23 mars 2012. Conformément à l'article 27, paragraphe 4, du règlement, le présent avis doit être rendu sous deux mois. Compte tenu de la complexité de l'affaire, le CEPD a prolongé pour une nouvelle période de deux mois le délai de remise du présent avis conformément à l'article 27, paragraphe 4, du règlement. La procédure a été suspendue pendant 273 jours au total, afin de permettre au CEPD d'obtenir les informations complémentaires nécessaires.

Le 23 avril 2013, l'OLAF a retiré la notification originale pour la remplacer par une nouvelle notification. Un nouveau délai a commencé à courir à partir de cette date. La procédure a été suspendue pendant trois jours pour permettre au CEPD d'obtenir les informations complémentaires nécessaires.

La procédure a ensuite été suspendue pendant 16 jours pour permettre la remise d'observations sur le projet d'avis. Par conséquent, le présent avis doit être rendu au plus tard le 22 juillet 2013.

### 3.2. Licéité du traitement

Le traitement de données à caractère personnel doit reposer sur l'un des motifs visés à l'article 5 du règlement.

#### *3.2.1. Article 5, point b)*

Dans la notification, l'OLAF indique que la base légale du présent traitement est l'article 5, point b), du règlement, qui concerne le traitement nécessaire au respect d'une obligation légale. Selon le CEPD, seule une obligation suffisamment claire et spécifique peut justifier le traitement de données à caractère personnel en vertu de l'article 5, point b), du règlement. Aux termes de l'article 5, point b), du règlement, il doit être établi que le responsable du traitement (en l'espèce l'OLAF) est soumis à une obligation légale de collecte et de traitement de données qui ne lui laisse aucune marge de discrétion[5].

La notification mentionne spécifiquement les dispositions suivantes: article 3 du règlement 1073/2001 et article 2 de la décision 1999/352 de la Commission, législation horizontale (en particulier règlements n° 2185/96[6] et n° 2988/95[7] du Conseil), ainsi que législation spécifique au secteur ou autres dispositions légales applicables (par exemple

[5] L'article 5, point b), autorise un traitement «*nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis*».

[6] Règlement (EURATOM, CE) n° 2185/96 du Conseil, du 11 novembre 1996, relatif aux contrôles et vérifications sur place effectués par la Commission pour la protection des intérêts financiers des Communautés européennes contre les fraudes et autres irrégularités, JO L 292 du 15.11.1996, p. 2-5.

[7] Règlement (CE, Euratom) n° 2988/95 du Conseil, du 18 décembre 1995, relatif à la protection des intérêts financiers des Communautés européennes (JO L 312 du 23.12.1995, p. 1-4).

règlements n° 1080/00[8] et n° 2666/00[9]; Conventions de Lomé et accords de Cotonou). Le CEPD considère que le lien avec les dispositions légales ci-dessus n'est pas suffisamment précis en l'espèce pour justifier l'application de l'article 5, point b), du règlement. Tandis que les dispositions susvisées établissent les pouvoirs de l'OLAF dans le cadre d'enquêtes externes, elles n'imposent pas à l'OLAF de mettre en place la plateforme IDCP ou un instrument similaire. Le fait que l'OLAF a déjà mené des enquêtes externes sans un tel instrument étaye par ailleurs la conclusion selon laquelle l'OLAF n'est pas «légalement tenu» de mettre en place la plateforme IDCP.

Compte tenu de ce qui précède, le CEPD déterminera si le traitement peut être couvert par l'article 5, point a), du règlement.

### *3.2.2. Article 5, point a)*

L'article 5, point a), du règlement, autorise le traitement de données à caractère personnel 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*». L'article 5, point a), du règlement, contient trois éléments qui doivent tous être réunis: 1) le traitement doit être réalisé en vue d'une mission effectuée dans l'intérêt public; 2) la mission doit reposer sur la législation (les traités ou un autre acte adopté sur cette base) ou relever de l'exercice de l'autorité publique dont est investie l'institution ou l'organe communautaire ou le tiers auquel les données sont communiquées; 3) il doit être nécessaire à l'exécution d'une telle mission.

#### *3.2.2.1. Exécution d'une mission dans l'intérêt public*

Sur la base des informations fournies et visées à la partie 2.1, il apparaît que la plateforme IDCP s'inscrira dans le cadre d'une mission exercée dans l'intérêt public, à savoir la conduite d'enquêtes externes destinées à lutter contre la fraude, la corruption et d'autres activités illégales affectant les intérêts financiers de l'Union européenne.

#### *3.2.2.2. Fondement juridique*

Les bases légales spécifiques aux enquêtes administratives externes ont déjà été expliquées dans les grandes lignes dans l'avis du CEPD sur le contrôle préalable concernant les enquêtes externes de l'OLAF, auquel il est fait référence[10]. Les bases légales citées par l'OLAF dans la notification sont aussi pertinentes. Toutes les dispositions ci-dessus confient à l'OLAF la mission de mener des enquêtes administratives externes dans le but de renforcer la lutte contre la fraude.

Conformément à l'article 2, paragraphe 5, point a) de la décision n° 352/1999 de la Commission, «*[l]'Office est chargé de toute autre activité opérationnelle de la Commission en matière de lutte antifraude telle que visée au paragraphe 1, et notamment: (a) de développer*

[8] Règlement (CE) n° 1080/2000 du Conseil, du 22 mai 2000, relatif au soutien à la Mission intérimaire des Nations unies pour le Kosovo (MINUK) et à l'Office du Haut Représentant en Bosnie-et-Herzégovine (OHR), JO L 122 du 24.5.2000, p.27-28.

[9] Règlement (CE) n° 2666/2000 du Conseil, du 5 décembre 2000, relatif à l'aide à l'Albanie, à la Bosnie-et-Herzégovine, à la Croatie, à la République fédérale de Yougoslavie et à l'ancienne République yougoslave de Macédoine, abrogeant le règlement (CE) n° 1628/96, et modifiant les règlements (CEE) n° 3906/89 et (CEE) n° 1360/90, ainsi que les décisions 97/256/CE et 1999/311/CE, JO L 306 du 7.12.2000, p. 1-6.

[10] Avis du CEPD sur les enquêtes externes de l'OLAF du 4 octobre 2007 (affaires 2007-0047 et autres), disponible sur le site Internet du CEPD.

*les infrastructures nécessaires; (b) d'assurer la collecte et l'exploitation d'informations; [...]. L'Office est l'interlocuteur direct des autorités policières et judiciaires.*»[11].

La plateforme IDCP sera utilisée par l'OLAF dans le but d'échanger des informations et de coopérer avec ses partenaires internationaux dans le cadre d'enquêtes externes. Elle peut donc être considérée comme justifiée par la disposition légale susvisée, en tant qu'infrastructure développée en lien avec la lutte contre la fraude et garantissant la collecte et l'analyse d'informations.

Néanmoins, dans un souci de sécurité juridique, le CEPD recommande que la base légale soit renforcée et que l'OLAF conclue à cette fin des accords spécifiques avec les partenaires IDCP par un échange de correspondance, comme prévu dans l'accord de coopération basé sur l'accord de coopération type approuvé par le CEPD, énonçant les principaux éléments du traitement et ses limites externes. Ceci constituerait une garantie nécessaire, non seulement pour les personnes concernées, mais aussi pour l'OLAF lui-même, puisque cela donnerait à la plateforme IDCP une base légale plus solide.

*3.2.2.3. Nécessité*

L'OLAF a avancé divers arguments pour justifier la nécessité de la nouvelle plateforme, tant par écrit que de manière orale, lors de la réunion opérationnelle avec le CEPD.

L'OLAF a souligné que la coopération avec des États membres, des autorités de pays tiers et des organisations internationales est un élément essentiel de ses activités. Dans l'exercice de sa mission de protection du budget de l'Union européenne, l'OLAF entend se baser sur un réseau de services et d'organisations de partenaires d'enquête, administratifs et judiciaires. L'OLAF relève que ces partenaires ont souvent des responsabilités convergentes dans l'exercice d'un contrôle lors de divers projets financés par l'Union européenne et qui se déroulent en dehors de son territoire. L'OLAF déclare qu'il n'a probablement pas les pouvoirs suffisants en matière d'enquête ou de collecte d'informations à l'égard de tels projets et qu'il aura donc besoin de se reposer sur la coopération de ses partenaires. Le partage d'informations concernant la mise en œuvre de tels projets est donc considéré par l'OLAF comme un élément essentiel de sa mission d'enquête.

L'OLAF insiste sur le fait qu'il doit savoir si des informations pertinentes existent et quel partenaire les détient, afin de pouvoir partager efficacement les données d'enquête avec ses partenaires. En particulier, l'OLAF a souligné le besoin de collecter des informations sur des affaires de double financement non déclaré pour le même projet et des enquêtes parallèles concernant le même projet. Il a expliqué que l'absence de coordination entre les donateurs aboutit à des situations dans lesquelles des fonds pour un même projet sont versés deux ou plusieurs fois par différents donateurs du fait de l'absence générale de coordination. L'OLAF maintient que ces défauts seraient considérablement atténués s'il existait un système permettant l'échange d'informations sur des enquêtes parallèles. L'OLAF soutient que la plateforme IDCP permettrait de combler cette absence d'informations dans le sens où elle lui permettrait de vérifier qu'un partenaire a enquêté ou enquête sur une affaire parallèle ou liée, ou peut détenir de toute autre façon des informations pertinentes sur une affaire particulière.

Le CEPD a pris bonne note de ces arguments. L'OLAF a fourni des éléments suffisants pour justifier le besoin d'une coopération plus structurée dans la lutte contre la fraude dans le secteur des dépenses externes. La coopération et l'échange d'informations sont en effet essentiels pour

[11] Décision n° 352/1999 de la Commission, précitée.

combattre efficacement la fraude au niveau international. Les affaires de double financement sont un bon exemple du besoin d'une coordination renforcée, compte tenu de leur impact financier considérable. Les fonds doivent être gérés efficacement, en particulier en période de crise économique.

La coopération pourrait être plus efficace si elle n'était pas unilatérale mais réciproque. L'OLAF a fourni des arguments suffisants pour démontrer qu'il ne peut obtenir les informations dont il a besoin de la part de ses partenaires que s'il accepte en échange de partager des informations avec eux. La nécessité de ce type de transfert devra donc être appréciée dans le cadre d'une réciprocité assurée. À cet égard, la contribution de l'OLAF à la plateforme IDCP pourrait être perçue comme une condition préalable à l'adhésion à celle-ci et à la volonté des partenaires d'y contribuer.

S'agissant de l'outil spécifique choisi, il appartient à l'institution européenne de déterminer quels mécanismes sont les plus appropriés pour atteindre l'objectif sous-jacent, pour autant que ces moyens ne soient pas manifestement disproportionnés. En l'espèce, il semble qu'un système manuel de partage d'informations ne soit pas une solution de substitution efficace, pour plusieurs raisons. D'une part, la plateforme IDCP permettra à l'OLAF de consulter tous ses partenaires à la fois, plutôt qu'un par un. D'autre part, la consultation sera menée de façon automatisée, ce qui implique des réponses immédiates et plus précises.

Le traitement notifié peut donc être basé sur l'article 5, point a), du règlement. Ceci étant, la légalité de la plateforme IDCP dépendra de sa conformité à l'ensemble des exigences du règlement, y compris la proportionnalité et la qualité des données, qui seront examinées dans les parties ci-après.

### 3.3. Identification du responsable du traitement

Aux termes de l'article 2, point d), du règlement, le «responsable du traitement» est défini comme «*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*». À l'opposé de la notion de responsable du traitement se trouve celle de «sous-traitant», définie par l'article 2, point e), comme «*la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel* <u>*pour le compte*</u> *du responsable du traitement*» (mis en exergue par l'auteur).

L'identification du responsable du traitement dans le contexte des opérations de traitement des données vise à déterminer l'entité qui sera responsable de la conformité aux règles en matière de protection des données, de la façon dont les personnes concernées peuvent exercer leurs droits, de la législation relative à la protection des données qui est applicable, ainsi que des questions juridictionnelles. La clarification des rôles et responsabilités prend encore plus d'importance quand plusieurs entités sont potentiellement impliquées dans le traitement de données à caractère personnel, comme c'est le cas en l'espèce.

L'OLAF indique dans la notification qu'il traitera les ensembles de données reçus des partenaires IDCP «pour le compte du partenaire». Ceci ne permet pas de dire avec précision si l'OLAF se considère comme un sous-traitant, par opposition à un responsable du traitement, à l'égard des ensembles de données transmis par des partenaires IDCP. Il ressort toutefois de la description des missions figurant dans la nouvelle notification et des autres documents fournis que l'OLAF jouera un rôle fondamental dans la gestion de la base de données. Celle-ci sera située physiquement dans les locaux de l'OLAF et hébergée sur un serveur de l'OLAF. Des

analystes de l'OLAF seront responsables de la gestion de l'infrastructure physique. L'OLAF gèrera l'authentification, les comptes utilisateurs, les téléchargements, l'accès sécurisé et les utilisateurs authentifiés au moyen de certificats valables provenant de l'organisation partenaire.

Compte tenu de l'étendue et de l'importance de ses missions, telles que décrites dans la notification, le rôle de l'OLAF à l'égard de l'ensemble de données transmis par les partenaires IDCP ne peut être celui d'un simple sous-traitant. L'OLAF jouera un rôle essentiel dans la gestion du système. Selon le niveau de contrôle exercé par les partenaires IDCP sur la gestion de la base de données, l'OLAF pourra être qualifié de responsable unique du traitement ou de responsable commun du traitement, avec une responsabilité principale, mais pas de simple sous-traitant.

Compte tenu de ce qui précède, le CEPD recommande à l'OLAF d'indiquer clairement, dans un manuel technique spécifique, les responsabilités des différents acteurs dans la mise en œuvre de la plateforme IDCP. Le CEPD recommande notamment à l'OLAF de prévoir les points principaux suivants:

- Les partenaires IDCP et l'OLAF seront les responsables du traitement à l'égard de leurs propres activités de traitement des données en tant que partenaires du système et contributeurs à celui-ci. Chaque partenaire IDCP sera chargé de veiller à la qualité des données et à la légalité des données intégrées au système.
- L'OLAF sera l'opérateur du système, responsable, principalement et avant tout, du fonctionnement technique, de la maintenance, et de la garantie de la sécurité globale.
- Les partenaires IDCP et l'OLAF partageront la responsabilité de l'obligation de notification et de l'octroi de droits d'accès, d'objection et de rectification.

### 3.4. Qualité des données

Conformément à l'article 4, paragraphe 1, points a), c) et d), du règlement 45/2001, les données à caractère personnel doivent être traitées loyalement et licitement, être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement, et être exactes. La licéité du traitement des données a déjà été évoquée (cf. point 3.2), tandis que sa loyauté doit être appréciée dans le contexte des informations fournies aux personnes concernées (cf. point 3.9).

La mise en œuvre de la plateforme IDCP sera basée sur un concept «pull». Les partenaires IDCP pourront accéder directement aux informations relatives aux enquêtes de l'OLAF depuis la base de données, sans aucune interaction avec l'OLAF. L'accès «pull» présente le risque spécifique que des données non pertinentes soient fournies en réponse à une recherche. Pour minimiser ce risque, les données figurant sur la plateforme IDCP devront être limitées autant que possible. Par exemple, une recherche sur un nom particulier peut révéler des informations concernant plusieurs affaires indépendantes dans différents pays, alors même que l'autorité de vérification ne s'intéresse qu'à l'une de ces affaires dans un pays donné. L'octroi d'un accès direct augmenterait donc le risque d'une collecte dénuée de pertinence ou de «fishing expeditions». De manière générale, tout échange de données à caractère personnel doit respecter les principes de nécessité et de proportionnalité. Il convient donc d'éviter ou de minimiser l'échange de données non pertinentes aux fins de l'enquête en question.

Au cours de la procédure, le CEPD a cherché à savoir s'il serait possible d'utiliser en l'espèce un système pur de concordance/non-concordance («*hit/no hit*»), montrant uniquement si une entité donnée (par exemple un nom, une entreprise, une adresse) est liée à une enquête.

L'OLAF a répondu avec fermeté qu'un tel système ne servirait pas l'objectif sous-jacent pour un certain nombre de raisons:

- un modèle de concordance/non-concordance est idéal pour les systèmes dans lesquels les informations sont décrites de façon complète par une réponse positive ou négative et pourraient donc être exprimées de façon exhaustive par une concordance (ou un nombre limité de concordances) ou une non-concordance. Ceci est en particulier le cas des systèmes qui reposent sur une logique binaire (concordance/non-concordance), mais ce n'est pas le cas des informations qui figurent dans la base de données actuelle;
- les données d'enquête sont liées entre elles par des rapports logiques et complexes, et ne deviennent intelligibles qu'une fois ces rapports compris. Cela tient au fait que les enquêteurs ne travaillent pas sur des informations complètes sur leur affaire (puisqu'ils enquêtent à ce sujet) et doivent vérifier si un élément de leur enquête a un rapport direct ou indirect avec des informations collectées dans une autre affaire. Comprendre les rapports entre les différentes entités est l'une des analyses essentielles que les enquêteurs effectuent dans le cadre de leurs obligations et cela serait impossible sur la seule base d'un système de concordance/non-concordance. Pour obtenir un résultat porteur de sens, les enquêteurs doivent identifier les affaires qui ne présentent que des similitudes limitées avec l'objet de leur enquête et confirmer un possible rapport direct ou indirect avec leur affaire, en étudiant les cas connus et la façon dont ils interagissent;
- il peut arriver que des noms soient mal orthographiés; certains termes ou noms peuvent être trop répandus et donner lieu à des concordances excessives ou être classés de façon erronée ou inexacte. Pour obtenir un résultat porteur de sens, l'OLAF peut donc avoir besoin d'établir des liens avec les autres données à sa disposition et de les mettre en rapport avec les données des autres partenaires;
- l'OLAF considère que ce système représenterait une charge administrative dissuasive pour l'utilisation du système.

Le CEPD prend note des arguments ci-dessus. Cependant, il est important d'introduire certaines garanties appropriées quant à l'étendue de l'accès, afin de minimiser les inquiétudes concernant la qualité des données. En particulier, il recommande à l'OLAF de définir plus précisément les modalités d'accès comme suit:

1. chaque accès à la plateforme IDCP doit être dûment motivé et validé dans le cadre d'une procédure interne mise en place par chaque partenaire, spécifiée dans le manuel utilisateur, que chaque partenaire devrait s'engager à respecter. Cela permettrait un contrôle préalable de la nécessité de l'accès aux données. La demande et la motivation par le partenaire devraient être enregistrées et pouvoir être contrôlées a posteriori. Cette procédure devrait aussi être reflétée dans les fonctionnalités de la base de données. En particulier, l'OLAF devrait inclure un champ obligatoire demandant au partenaire, lors de chaque session de recherche, d'indiquer l'enquête concernée (ou le fichier opérationnel de l'affaire en question) et de motiver brièvement la nécessité sur ce fondement. Si l'intégration de cette fonctionnalité dans la base de données est impossible, l'OLAF devrait mettre en place une base de données distincte dans le seul but d'enregistrer les justifications fournies par les utilisateurs. Cette base de données pourrait être située dans un environnement distinct sous contrôle strict de l'OLAF;

2. mettre en œuvre une approche en deux étapes dans laquelle tous les partenaires auront accès à une première couche de données et pourront accéder aux extensions graphiques du résultat (deuxième couche), sur demande motivée devant être validée électroniquement par l'OLAF, pour autant que les données de l'OLAF sont concernées. Sinon, l'OLAF peut aussi envisager un système mixte avec accès intégral aux données

sans caractère personnel (données relatives à des sociétés qui n'identifient pas des personnes physiques, par exemple) et une concordance/non-concordance pour les noms et autres données à caractère personnel; le système devrait fixer un seuil pour le nombre de résultats affichés pour chaque recherche. Si une recherche donne trop de résultats, l'utilisateur pourrait n'obtenir que les résultats les plus pertinents (les concordances exactes en premier), jusqu'à ce que le seuil soit atteint, et l'utilisateur devrait être informé du fait que sa recherche a généré trop de résultats. Un tel seuil devrait être déterminé sur la base des besoins professionnels et en tenant compte de la protection des données;

3. l'OLAF devrait limiter le recours aux champs ouverts. En particulier, l'OLAF devrait restreindre le contenu des champs ouverts en fonction de critères spécifiques (par exemple en limitant la longueur de la chaîne de texte);

4. l'OLAF devrait limiter l'étendue de l'entité de données «personne» aux seules personnes ou entités qui font l'objet d'une enquête.

S'agissant de l'exactitude des données, les données devraient être soumises à des contrôles fréquents par chaque partenaire (au moins annuellement) afin d'en vérifier l'exactitude et l'actualité. Il est également possible que les données doivent être mises à jour en fonction de l'avancée de l'enquête, par exemple quand des personnes sont lavées de tous soupçons. L'OLAF devrait aussi recommander et vérifier que des politiques et des garanties adéquates soient mises en œuvre par ses partenaires à cet égard. Les données qui doivent être supprimées des fichiers de l'OLAF selon sa politique de conservation doivent aussi l'être de la plateforme IDCP. Sur ce point, se reporter aux parties 3.6, 3.8 et 3.10 ci-dessous.

### 3.5. Catégories spéciales de données

L'article 10, paragraphe 5, du règlement dispose: *«le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que s'il est autorisé par les traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités ou, si cela s'avère nécessaire, par le contrôleur européen de la protection des données»*. En l'espèce, il y a lieu de considérer que le traitement des données visées par l'OLAF est autorisé par les dispositions pertinentes du règlement n° 1073/1999 et par l'article 2 de la décision 1999/352 de la Commission établissant la compétence de l'OLAF concernant la conduite d'enquêtes antifraude.

Conformément à l'article 10, paragraphe 1, du règlement, le traitement de catégories spéciales de données (à savoir des *données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la santé ou à la vie sexuelle*) est interdit. Le règlement prévoit certaines exceptions à l'article 10, paragraphe 2. Il semble toutefois plus probable que la seule exception applicable soit celle visée au point d). Ceci étant, puisqu'il s'agit d'une exception, cette disposition doit être interprétée de façon restrictive.
Dans la nouvelle notification, l'OLAF indique, en qualité de responsable du traitement, qu'aucune catégorie spéciale de données ne sera transférée par l'intermédiaire de la plateforme IDCP. Dans le contexte de la garantie de l'échange de données à caractère personnel, il semble que le traitement de catégories spéciales de données ne puisse être totalement exclu, mais qu'il soit exceptionnel. En tout état de cause, le personnel de l'OLAF en charge des fichiers doit avoir conscience de cette règle et éviter d'inclure des catégories spéciales de données, à moins que l'une des circonstances prévues à l'article 10, paragraphe 2 (dans un sens restreint, comme indiqué ci-dessus), ne soit présente dans l'affaire en cours d'investigation ou à moins que l'article 10, paragraphe 4, ne puisse s'appliquer.

### 3.6. Conservation des données

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. L'institution ou l'organe communautaire prévoit, pour les données à caractère personnel qui doivent être conservées au-delà de la période précitée à des fins historiques, statistiques ou scientifiques, soit qu'elles ne seront conservées que sous une forme qui les rend anonymes, soit, si cela est impossible, qu'elles ne seront stockées qu'à condition que l'identité de la personne concernée soit cryptée. Les données ne doivent en tout cas pas être utilisées à des fins autres qu'historiques, statistiques ou scientifiques»* (article 4, paragraphe 1, point e), du règlement).

Selon la nouvelle notification, les données à caractère personnel concernées par le présent traitement seront sauvegardées pendant dix ans. Les données feront l'objet d'examens annuels dans le cadre de contrôles automatisés et manuels dès lors qu'elles auront été conservées depuis trois ans, afin de garantir qu'elles sont détenues conformément à la période de conservation fixée. L'OLAF déclare que des données à caractère personnel pertinentes pourront être conservées dans ses fichiers d'enquête pour une durée maximale de 15 ans, conformément aux règles applicables à de telles enquêtes[12]. Les données reçues de partenaires internationaux seront conservées par l'OLAF selon la période demandée par le partenaire transmettant les données. En tout état de cause, la période de conservation fondamentale dans ces situations sera aussi de dix ans.

Le CEPD n'a pas reçu de justification convaincante quant à la nécessité d'une période de conservation aussi longue. De prime abord, rien ne démontre qu'une période de conservation plus courte (5 ans par exemple) ne soit pas suffisante. Il recommande donc à l'OLAF de réduire sa période de conservation pour les données IDCP. En outre, il est recommandé à l'OLAF de garantir la suppression de la plateforme IDCP de toutes les données à caractère personnel qui, aux termes de sa politique de conservation, doivent être supprimées de ses fichiers (c'est-à-dire les données datant de plus de 15 ans), peu importe qu'elles soient conservées sur la plateforme IDCP depuis une période moins longue que la période de conservation.

### 3.7. Transferts de données

Conformément à l'article 9, paragraphe 1, du règlement, les transferts de données à caractère personnel à des destinataires autres que les institutions et organes communautaires, et qui ne sont pas soumis à la législation nationale adoptée en application de la directive 95/46/CE, ne peuvent avoir lieu que pour autant qu'un niveau de protection adéquat soit assuré dans le pays du destinataire ou au sein de l'organisation internationale destinataire, et que ce transfert vise exclusivement à permettre l'exécution des missions qui relèvent de la compétence du responsable du traitement[13]. Cette règle est particulièrement pertinente pour l'OLAF dans la mesure où la plupart des pays tiers ou des organisations internationales auxquels l'OLAF transfèrerait des données à caractère personnel ne seraient généralement pas reconnus comme assurant un niveau de protection adéquat.

---

[12] Avis du CEPD sur les procédures d'enquête révisées de l'OLAF, du 3 février 2012, disponible sur le site Internet du CEPD dans la rubrique Supervision/Contrôles préalables/Avis.

[13] Parallèlement au présent contrôle préalable, le CEPD élabore actuellement un document de synthèse sur les transferts de données transfrontaliers, qui couvrira également le type d'échanges faisant l'objet du présent contrôle préalable.

Par dérogation à la règle générale, une institution ou un organe communautaire peut transférer des données à caractère personnel aux destinataires susvisés si l'une des exceptions énoncées à l'article 9, paragraphe 6, du règlement s'applique. L'intérêt particulier pour l'OLAF fait partie des diverses exceptions visées à l'article 9, paragraphe 6, point d), concernant les transferts nécessaires ou légalement requis pour des raisons d'intérêt public, puisqu'il est probable que nombre des transferts internationaux effectués par l'OLAF relèvent de son champ d'application. Cependant, un recours systématique aux dérogations est inacceptable du point de vue de la protection des données. En principe, les transferts basés sur les exceptions susvisées ne devraient pas être volumineux, systématiques ou structurels[14].

La plateforme IDCP introduit un outil de partage d'informations qui est permanent, structurel et systématique. Par conséquent, il ne remplit pas fondamentalement les conditions d'une exception sur le fondement de l'article 9, paragraphe 6, point d), du règlement. Il convient donc de tenir compte de l'article 9, paragraphe 7, du règlement, selon lequel le CEPD «*peut autoriser un transfert ou un ensemble de transferts de données à caractère personnel vers un pays tiers ou une organisation internationale n'assurant pas un niveau de protection adéquat [...] lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants; ces garanties peuvent notamment résulter de clauses contractuelles appropriées*».

Pour déterminer si la plateforme IDCP réunit les conditions relatives à l'application de l'article 9, paragraphe 7, du règlement, le CEPD doit donc vérifier si elle offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants.

Sur ce point, il convient de tenir compte des éléments suivants:

- L'OLAF a défini un ensemble de clauses pour l'échange d'informations qui doivent être conclues avec des pays tiers et des organisations internationales dans le cadre d'un accord de coopération administrative («accord de coopération»). L'OLAF accordera un accès à la plateforme IDCP aux seuls partenaires internationaux avec lesquels il aura conclu un accord de coopération comprenant en annexe des clauses relatives à la protection des données.
- Le CEPD a analysé ces garanties[15] et considère qu'elles sont essentielles en ce qui concerne les exceptions prévues à l'article 9, paragraphe 6, du règlement. Compte tenu du nombre limité de transferts prévus par l'OLAF, le CEPD invite l'OLAF à utiliser de telles clauses dans le contexte de transferts exceptionnels. Si la fréquence et l'étendue des échanges devaient augmenter significativement à l'avenir, l'OLAF devrait demander une autorisation spéciale, conformément à l'article 9, paragraphe 7, du règlement.
- L'OLAF ne prévoit de conclure un partenariat IDCP qu'avec des partenaires sélectionnés dont il juge qu'ils offrent des garanties de fiabilité suffisantes. Dans son avis sur les accords de coopération, le CEPD a notamment recommandé à l'OLAF de

[14] Voir document de travail du groupe de travail Article 29, Transferts de données personnelles vers des pays tiers: application des articles 25 et 26 de la directive relative à la protection des données, 24 juin 1998, disponible sur le site Internet du groupe de travail.

[15] Les clauses sont essentiellement inspirées (avec certains ajustements) de l'ensemble alternatif de clauses contractuelles de la Commission de 2004. Voir décision de la Commission du 27 décembre 2004 modifiant la décision n° 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers, JO L 385 du 29.12.2004, p. 74.

*«sélectionner ses partenaires avec soin, en réalisant une évaluation préalable de leur capacité et de leur volonté à respecter les clauses de l'accord de coopération et ses annexes»*.

Les garanties générales fournies par les accords de coopération, dans la mesure où elles ont été développées en lien avec des transferts exceptionnels, ne peuvent pas être utilisées de façon automatique pour la plateforme IDCP et doivent donc être renforcées pour établir des garanties adéquates aux fins d'une autorisation en vertu de l'article 9, paragraphe 7, du règlement. La demande d'autorisation sera analysée par le CEPD dans une procédure distincte.

### 3.8. Droits d'accès et de rectification

L'article 13 du règlement prévoit un droit d'accès pour les personnes concernées, et l'article 14 accorde un droit de rectification des données à caractère personnel.

Le droit d'accès permet aux personnes physiques de découvrir si des informations les concernant font l'objet d'un traitement et, dans l'affirmative, quels types d'informations. Le droit d'accès est souvent un préalable au droit de rectification. Dès lors qu'une personne physique a pu accéder à ses données et vérifier l'exactitude et la licéité du traitement, le droit de rectification lui permet de corriger des données inexactes ou incomplètes. Le respect des droits d'accès et de rectification est directement lié au principe de la qualité des données et, dans le contexte d'enquêtes, il coïncide dans une large mesure avec le droit de défense. Garantir le droit d'accès à la personne concernée par l'enquête externe est donc de la plus haute importance.

Le CEPD relève que l'OLAF, en qualité de gérant de la plateforme IDCP et de responsable du traitement des données, est tenu de fournir un accès aux données IDCP, peu importe que ces données proviennent de ses propres fichiers ou des fichiers d'un partenaire. L'OLAF devra fournir un tel accès, à moins qu'une restriction ne s'applique en vertu de l'article 20 du règlement. Le CEPD reconnaît que l'OLAF pourrait avoir besoin de consulter ses partenaires dans le cadre d'une décision relative à l'application d'une restriction aux données à caractère personnel provenant d'un pays tiers. En tout état de cause, le CEPD souligne que de telles restrictions doivent être interprétées de façon restrictive et ne sauraient s'appliquer de façon systématique.

Dans la nouvelle notification, l'OLAF fait référence aux principes et procédures utilisés dans le cadre d'enquêtes externes, qui s'appliqueraient également en l'espèce. Par conséquent, les orientations données par le CEPD dans l'avis relatif aux enquêtes externes de l'OLAF (voir partie 3.7) et aux procédures d'enquête révisées de l'OLAF s'appliquent de manière générale dans ce contexte[16]. Le CEPD renvoie l'OLAF aux observations et recommandations formulées dans ces avis, et au suivi en cours à cet égard.

### 3.9. Information des personnes concernées

Le règlement dispose que les personnes concernées doivent être informées lorsque des données à caractère personnel les concernant sont collectées, et il énumère un certain nombre d'éléments qui doivent impérativement figurer dans l'information afin de garantir le caractère équitable du traitement des données à caractère personnel. En l'espèce, les données traitées par l'OLAF sont soit déjà en sa possession (les propres données de l'OLAF), soit collectées auprès d'autres partenaires IDCP.

[16] Voir supra.

Dans la notification, l'OLAF fait référence aux principes et procédures utilisés dans le cadre d'enquêtes externes. Le CEPD souligne que cette approche n'est que partiellement acceptable. En particulier, elle s'applique uniquement à la première catégorie de données à caractère personnel (données déjà sauvegardées dans les fichiers de l'OLAF). Dans la mesure où ces données sont déjà enregistrées dans le CMS dans le cadre d'une enquête externe en cours, il est vrai que les personnes concernées ont en principe déjà été informées du traitement de leurs données à caractère personnel aux fins des articles 11 et 12 du règlement[17]. Sur ce point, le CEPD tient à renvoyer aux avis de contrôle préalable sur les enquêtes externes de l'OLAF et aux procédures d'enquête révisées de l'OLAF.

La situation est différente pour les données à caractère personnel collectées par l'OLAF auprès de partenaires IDCP. Dans ce cas, rien ne garantit que les personnes concernées ont été informées par l'autorité de transfert. Il convient également de garder à l'esprit que des données peuvent être collectées auprès de pays ou d'organisations ne disposant pas de règles relatives à la protection des données. Ceci implique que l'information prévue à l'article 12 doit en principe être fournie par l'OLAF, à moins que, conformément à l'article 12, paragraphe 2, du règlement, «*l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés*».

En l'espèce, le CEPD reconnaît que la remise par l'OLAF d'une information aussi générale à chaque personne dont le nom est fourni par des partenaires de l'OLAF impliquerait des efforts disproportionnés. Par conséquent, d'autres moyens devront être utilisés, à titre de deuxième choix, pour garantir la plus grande transparence possible du traitement. Par exemple, l'OLAF pourrait publier sur son site Internet une déclaration spécifique relative à la vie privée concernant la plateforme IDCP et demander à ses partenaires d'en faire autant. Les accords de coopération et l'annexe relative à la protection des données devraient aussi faire l'objet d'une publication adéquate.

### 3.10. Mesures de sécurité

[...]

## 4. CONCLUSIONS

L'opération de traitement proposée doit être mise en œuvre à la lumière des dispositions du règlement (CE) n° 45/2001 à condition de tenir pleinement compte des recommandations formulées ci-dessus. En particulier, l'OLAF doit:

- conclure les accords pertinents pour le présent traitement avec les organisations partenaires IDCP, en énonçant les principaux éléments du traitement et ses limites externes;
- préciser clairement l'affectation des responsabilités entre l'OLAF et les autres partenaires IDCP concernant le respect des exigences du règlement (voir partie 3.3 ci-dessus);
- limiter les modalités d'accès comme indiqué dans la partie 3.4 ci-dessus;
- garantir des contrôles suffisamment fréquents (au moins annuels) de l'exactitude, de l'exhaustivité et de l'actualité des données à caractère personnel figurant sur la plateforme IDCP;
- réduire la durée de la période de conservation;

[17] Sauf dans les cas où une exception s'applique en vertu de l'article 20.

- garantir la suppression de la plateforme IDCP de toutes les données à caractère personnel qui, aux termes de sa politique de conservation, doivent être supprimées de ses fichiers (à savoir des données datant de plus de 15 ans), peu importe qu'elles soient conservées sur la plateforme IDCP depuis moins de dix ans;
- fournir des garanties supplémentaires dans le contexte du partenariat IDCP pour pouvoir obtenir une autorisation au titre de l'article 9, paragraphe 7, du règlement. De telles garanties supplémentaires seront traitées dans le cadre de la procédure distincte relative à l'octroi de l'autorisation visée à l'article 9, paragraphe 7, du règlement;
- fournir un véritable droit d'accès aux données IDCP (ou garantir que le partenaire dont proviennent les données fournisse un tel accès), peu importe que ces données proviennent de fichiers de l'OLAF ou des fichiers d'un partenaire, à moins qu'une restriction ne s'applique au sens de l'article 20 du règlement;
- mettre en place des mécanismes adéquats afin d'améliorer la transparence du traitement vis-à-vis des personnes concernées à l'égard des données transmises par des pays tiers conformément à l'article 12 du règlement, comme indiqué dans la partie 3.9;
- réaliser une analyse exhaustive des risques et définir en détail les contrôles de sécurité spécifiques qui doivent être mis en œuvre pour réduire les risques à un niveau acceptable par la direction de l'OLAF; ceci inclut un examen des contrôles de sécurité existants tenant compte de la partie 3.10 ci-dessus.

Conformément à la législation, la mise en œuvre de la plateforme IDCP est soumise à une autorisation spécifique du CEPD aux termes de l'article 9, paragraphe 7, du règlement. La demande d'autorisation sera analysée par le CEPD dans un avis distinct. L'OLAF devrait s'abstenir d'activer la plateforme IDCP avant que le CEPD ne délivre une telle autorisation.

Fait à Bruxelles, le 18 juillet 2013

(**signè**)

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données