LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

GIOVANNI BUTTARELLI
CONTRÔLEUR ADJOINT

M^me^ Laraine LAUDATI
Déléguée à la protection des données
Commission européenne
Office européen de lutte antifraude
(OLAF)
1049 Bruxelles

Bruxelles, le 10 août 2012
Notre réf.: D(2012)1681 **C 2012-0279**
Veuillez utiliser l'adresse edps@edps.europa.eu pour toute correspondance

Objet: Notification en vue d'un contrôle préalable reçue de la déléguée à la protection des données de l'Office européen de lutte antifraude (OLAF) concernant le traitement de données à caractère personnel en rapport avec la fonction de recherche

Madame,

J'ai l'honneur de vous écrire au sujet de la notification d'un contrôle préalable concernant la fonction de recherche que vous m'avez fait parvenir le 23 mars 2012. La notification a été déclenchée par une recommandation du CEPD dans le cadre de son avis du 3 février 2012 sur un contrôle préalable concernant les nouvelles procédures d'enquête de l'OLAF. En effet, la fonction de recherche («Search Facility») a été notifiée à l'origine dans le contexte de cette procédure de contrôle préalable. Dans son avis, le CEPD a conclu qu'il ne disposait pas d'éléments d'information suffisants pour procéder à une analyse de la nouvelle base de données explorée par la fonction de recherche et a dès lors invité l'OLAF à lui présenter une notification distincte.

Dans la lettre accompagnant cette notification, vous avez souligné qu'après avoir mûrement réfléchi lors la rédaction de la notification, l'OLAF estimait qu'un contrôle préalable n'était plus nécessaire pour ce traitement dans la mesure où il relevait de la notification concernant les bases de données de renseignements de l'OLAF (ci-après, les «notifications de 2007») (voir l'avis du CEPD du 21 novembre 2007 dans les dossiers joints 2007-0027 et 2007-0028, ci-après, l'«avis de 2007»).

La fonction de recherche est une nouvelle base de données iBase dont la principale finalité est de permettre au personnel habilité de l'unité Enquête – Sélection & Révision (unité 01), chargé de la sélection des dossiers, d'effectuer des recherches électroniques parmi un sous-ensemble de données dans le système de gestion des dossiers de l'OLAF (CMS) afin de

vérifier si les nouvelles informations ne se rapportent pas à un dossier existant et d'éviter l'ouverture de dossiers redondants sur des affaires identiques. La fonction recherchera les correspondances croisées dans les champs de données suivants extraits des onglets «Organisation» et «Personne» du CMS: nom, observation sur l'implication, observation sur l'organisation, adresse(s), contact(s), fonction(s), type de personnes concernées, autre nom, date de naissance, lieu de naissance, observation sur la personne, pays, programme. Les résultats de la recherche indiqueront les documents où les données recherchées apparaissent.

La base de données contiendra les documents suivants: avis sur la décision d'ouverture (évaluation initiale avant le 1er février 2012), rapports à neuf mois, rapports intermédiaires et rapports finaux. La fonction en question est liée aux nouvelles procédures d'enquête, qui ont introduit une procédure de sélection en vue de l'évaluation des nouvelles informations présentant un intérêt potentiel dans le cadre d'enquêtes (voir l'avis du CEPD du 3 février 2012 sur les notifications en vue d'un contrôle préalable concernant les dossiers 2011-1127, 2011-1129, 2011-1130, 2011-1131 et 2011-1132). Comme toute autre base de données de renseignements, la fonction de recherche peut également être utilisée par les analystes de l'OLAF pour les finalités et dans les conditions énoncées dans les notifications de 2007 et l'avis qui leur est lié. Contrairement à d'autres bases de données de renseignements, l'accès à la base de données explorée par la fonction de recherche est également accordé aux membres de l'unité 01 à des fins de sélection des dossiers.

Les notifications de 2007 énoncent les conditions dans lesquelles l'OLAF peut traiter des données pour la finalité du renseignement/analyse et des activités opérationnelles et, pour soutenir des demandes de dossiers spécifiques, des opérations et des enquêtes visant à garantir l'exactitude et la pertinence optimales des informations reçues, diffusées ou traitées à des fins financières, administratives, disciplinaires, judiciaires et de renseignement. Les bases de données de renseignement (iBase) ont été décrites comme un des outils utilisés par le pool de données en matière d'information et de renseignement. Par conséquent, l'outil informatique utilisé (la base de données iBase) dans le traitement décrit dans les dossiers joints 2007-0027 et 2007-0028 est le même que celui décrit dans la notification actuelle. Il existe cependant quelques différences. Les dossiers joints 2007-0027 et 2007-0028 couvrent un scénario plus large, tandis que la fonction de recherche se borne essentiellement à vérifier si les nouvelles informations ne se rapportent pas à un dossier existant et à éviter l'ouverture de dossiers redondants sur des affaires identiques. Son contenu est expressément défini (avis sur la décision d'ouverture (évaluation initiale avant le 1er février 2012), rapports à neuf mois, rapports intermédiaires et rapports finaux).

Malgré sa portée plus limitée et d'autres différences (par exemple, l'accès accordé à l'unité 01), il ressort néanmoins des informations disponibles que la fonction de recherche reproduirait effectivement les caractéristiques habituelles des bases de données de renseignement et qu'elle relèverait dès lors des notifications correspondantes. La notification de 2007 a décrit la structure standard, la conception, le suivi d'audit, le contrôle de gestion et les droits d'accès à des bases de données dans l'environnement iBase plutôt que dans celui d'une base de données particulière. Tant qu'une nouvelle base de données correspond aux caractéristiques énoncées dans cette notification, elle sera couverte par la notification de 2007, ce qui rend superflue une notification distincte. En réponse à une question spécifique, l'OLAF a confirmé que la fonction de recherche répondait à ces caractéristiques habituelles. En conséquence, les observations et recommandations formulées dans l'avis du CEPD de 2007 s'appliquent également en l'occurrence, selon le cas.

Il convient en outre de considérer que le traitement réalisé au moyen de la base de données iBase explorée par la fonction de recherche s'inscrit dans le traitement général décrit dans les dossiers 2011-1127, 2011-1129, 2011-1130, 2011-1131 et 2011-1132 (plus précisément, la

«phase de sélection»). Par conséquent, ce traitement doit également se conformer aux observations et recommandations formulées dans le contexte de l'avis du CEPD du 3 février 2012, dans la mesure où elles sont applicables.

Eu égard à ce qui précède, nous considérons que le présent traitement ne nécessite pas de contrôle préalable complet, étant donné qu'il est déjà couvert par les notifications concernant le pool de données en matière d'information et de renseignement et les bases de données de renseignement de l'OLAF, dossiers 2007-0027 et 2007-0028, et les nouvelles procédures d'enquête de l'OLAF (enquêtes internes, enquêtes externes, plaintes rejetées et informations entrantes ne présentant aucun intérêt dans le cadre d'enquêtes, d'enquêtes de coordination et de mise en œuvre des recommandations de l'OLAF), dossiers 2011-1127, 2011-1129, 2011-1130, 2011-1131 et 2011-1132. Nous vous renvoyons aux recommandations formulées dans les avis finaux du CEPD dans ces dossiers, qui s'appliquent également, de manière générale, à la base de données en question. En particulier, nous rappelons qu'il importe de garantir les principes de qualité des données, de nécessité et de proportionnalité lors de l'utilisation de la base de données au cas par cas, en rapport avec les besoins spécifiques de chaque enquête.

Quant aux mesures de sécurité spécifiques applicables à la base de données, le CEPD souhaite attirer l'attention de l'OLAF sur plusieurs éléments:

- Les contrôles de sécurité doivent découler d'une analyse du risque de l'information. Dans l'idéal, un système de gestion de la sécurité de l'information (SGSI) s'appuierait sur la création d'un nouveau système et nécessiterait la réalisation d'une analyse du risque, ce qui aiderait l'OLAF à définir tous les contrôles de sécurité devant être effectués sur le plan technique et organisationnel.

- Pour ce qui est de la gestion des utilisateurs:
    - le CEPD comprend qu'un service d'annuaire sera utilisé afin de permettre l'authentification des utilisateurs et que les comptes d'utilisateur seront passés en revue une fois par an. La révision de ces comptes d'utilisateur est essentielle pour garantir que seul le personnel habilité a accès au système. Par conséquent, elle doit être planifiée et gérée minutieusement;
    - enfin, les procédures d'octroi, de modification et de retrait de l'accès à ce système doivent être clairement documentées et communiquées; les révisions de ces procédures doivent avoir lieu régulièrement afin de garantir la mise en œuvre et l'efficacité de contrôles de sécurité suffisants.

- Pour ce qui est de la journalisation et de la surveillance:
    - des révisions régulières des journaux du service d'annuaire doivent être effectuées pour détecter les tentatives d'attaque. D'autres contrôles de sécurité [tels que des systèmes de détection ou de prévention d'intrusion (IDS/IPS)] pourraient également être envisagés;
    - les bases de données d'audit et de sécurité iBase doivent être protégées contre toute perte de confidentialité et d'intégrité, même de la part des administrateurs;
    - la base de données d'audit iBase doit être gérée de telle manière que si elle tombe en panne, aucune information relative aux journaux ne soit perdue;
    - une procédure documentée doit être mise en place pour garantir le respect de la période de conservation de trois ans pour les journaux, idéalement par des moyens automatiques (autrement dit, le système devrait supprimer automatiquement les journaux de plus de trois ans). Des exceptions peuvent être prévues aux fins d'enquêtes internes et conformément à une procédure dûment documentée.

- Pour ce qui est de l'extrait historique initial des données nécessaires pour créer la base de données iBase, mentionné dans votre notification, et les importations ultérieures de données dans ladite base de données:
    - il convient de veiller à ce que toute opération, notamment manuelle, soit suffisamment contrôlée pour détecter les erreurs (garantie de la qualité des données);
    - toute copie temporaire des données (même partielle) doit être protégée contre la perte de confidentialité et d'intégrité et détruite dès qu'elle n'est plus utile.

Si vous avez besoin de plus amples informations concernant le présent traitement, le personnel du CEPD se tient à votre disposition pour vous fournir une aide supplémentaire.

Je vous prie d'agréer, Madame, l'expression de mes salutations distinguées.

(**signé**)

Giovanni BUTTARELLI