Avis sur la notification d'un contrôle préalable adressée par la déléguée à la protection des données de l'Office européen de lutte antifraude (OLAF) concernant un système de contrôle d'accès et d'identité

Bruxelles, le 7 avril 2008 (Dossier 2007-635)

1. Procédure

Le 17 octobre 2007, le contrôleur européen de la protection des données (ci-après dénommé "le CEPD") a reçu de la déléguée à la protection des données de l'Office européen de lutte antifraude (ci-après dénommé "l'OLAF") une notification en vue d'un contrôle préalable (ci-après dénommée "la notification") concernant les traitements de données liés à l'exploitation d'un système de contrôle d'accès et d'identité.

Le 6 décembre 2007, le CEPD a demandé des informations complémentaires, que la déléguée à la protection des données de l'OLAF (ci après dénommée "la DPD") lui a envoyées le 17 mars 2008.

Le 27 mars 2008, le CEPD a transmis son projet d'avis à la DPD pour observations, lesquelles lui sont parvenues le 4 avril 2008.

2. Examen du dossier

2.1. Les faits

Toile de fond

Le système de contrôle d'accès et d'identité fait partie de l'infrastructure de sécurité qui protège les locaux de l'OLAF et ses systèmes informatiques, lesquels viennent appuyer les enquêtes et l'ensemble des autres activités de l'OLAF visant à protéger les intérêts financiers de l'Union européenne.

Les données opérationnelles de l'OLAF sont soumises aux exigences de sécurité visées dans le règlement (CE) n° 45/2001. En outre, dans certains cas, ces données peuvent être classifiées et les mesures de sécurité complémentaires applicables en matière d'informations classifiées de l'UE doivent être mises en œuvre. L'OLAF souhaite traiter les informations classifiées de l'UE jusqu'au niveau SECRET UE. Des exigences de confidentialité et de sécurité très strictes s'appliquent au traitement de ces données dans ce contexte.

La politique de l'OLAF en matière de sécurité de l'information, élaborée afin de mettre en œuvre ces exigences de sécurité au sein de l'OLAF, exige une application rigoureuse du principe du besoin d'en connaître ("need to know"). Cela suppose une identification sans équivoque, c'est-à-dire une authentification forte, de tout utilisateur des systèmes de traitement des données opérationnelles de l'OLAF.

La politique de la Commission en matière de sécurité des systèmes d'information définit trois facteurs d'authentification: l'authentification par la connaissance, par la possession et par les

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

caractéristiques personnelles. L'OLAF a décidé de mettre en œuvre un système d'authentification combinant deux facteurs d'authentification, à savoir la possession et les caractéristiques personnelles. Conformément au document fourni au CEPD, l'OLAF a adopté les empreintes digitales comme facteur d'authentification par les caractéristiques personnelles, étant donné qu'il s'agit du meilleur compromis disponible en termes de convivialité, de fiabilité et de coût. D'autres systèmes, tels que la géométrie de la main et les caractéristiques de l'iris et de la rétine, ont été jugés plus intrusifs et/ou plus onéreux. En ce qui concerne l'authentification par la possession, l'OLAF a recours à une carte à puce. Les données biométriques relatives aux utilisateurs sont uniquement stockées sur cette carte à puce et ne peuvent être utilisées à d'autres fins.

Finalité
Le traitement des données dans le cadre du système de contrôle d'accès et d'identité a pour but de veiller à ce que seules les personnes autorisées aient accès aux locaux de l'OLAF.

Responsable du traitement
Le traitement des données relève essentiellement de la responsabilité de l'OLAF, en particulier de celle de l'Unité Services de l'information, qui fournit l'ensemble des systèmes de traitement des données.

Traitement
Ce système est destiné à contrôler l'identité des personnes entrant et sortant des locaux de l'OLAF en dehors des heures de service, ainsi que des zones spéciales sécurisées, et à leur en autoriser ou refuser l'accès. Ce système autorise ou refuse l'accès à toutes les entrées et sorties du périmètre de sécurité physique de l'OLAF au sein du bâtiment de l'Office, ainsi que des zones spéciales sécurisées telles que les locaux informatiques et le centre de gestion des documents de l'OLAF, où les informations opérationnelles sont traitées, conservées et archivées.

L'accès à l'OLAF par les portes d'accès automatiques réservées au personnel, situées dans le hall surveillé, ne nécessitera pas d'authentification biométrique. Une authentification par les empreintes digitales sera requise aux points d'accès non surveillés de l'OLAF, en dehors des horaires normaux de service, soit de 20h00 à 7h00, et pendant les week-ends. Une porte vitrée, située au-delà des portes d'accès automatiques réservées au personnel, sera fermée en dehors des horaires normaux de service, empêchant ainsi tout accès non autorisé aux ascenseurs de l'OLAF. L'ouverture de cette porte, ainsi que de toutes les portes permettant d'accéder à l'OLAF à partir des cages d'escalier, est soumise à un contrôle d'accès biométrique.

Le système de contrôle d'accès est composé de cartes d'accès personnelles, délivrées à chaque membre du personnel de l'OLAF, d'un certain nombre de lecteurs de cartes, de points d'accès, d'un serveur de base de données central où sont stockées les informations concernant les droits d'accès et le protocole des accès, ainsi que de plusieurs postes de travail administratifs.

Les visiteurs se voient délivrés une carte visiteur (générique), les données à caractère personnel les concernant n'étant donc pas enregistrées dans le système.

* L'enrôlement d'un utilisateur consiste en deux procédures indépendantes:
a) le numéro d'identification unique de la carte est enregistré dans le système de contrôle d'accès et est associé à une personne dans la base de données;
b) les empreintes de trois doigts de la personne concernée sont numérisées par le système, qui calcule un modèle numérique de ces empreintes, lequel est stocké uniquement sur la carte, et non dans la base de données. L'OLAF ne prévoit pas d'utiliser cette carte à d'autres fins que le contrôle d'accès physique et informatique.

* Spécificités techniques: les cartes personnelles utilisent la technologie Mifare et un dispositif passif (le modèle utilisé est la carte Mifare classique 4 K, qui est le modèle que la direction de la sécurité de la Commission a recommandé au moment où le projet de l'OLAF en matière de sécurité a été lancé). Ces cartes contiennent un numéro d'identification unique et trois modèles d'empreintes digitales permettant une authentification biométrique par vérification de la concordance entre les empreintes de l'utilisateur et les données contenues dans la carte (technologie "*match-on-card*"). Le stockage de trois modèles d'empreintes permet de procéder à l'authentification en utilisant l'un des trois modèles contenus dans la carte.

Par modèle biométrique, on entend les données qui représentent l'empreinte enregistrée. Il se compose de deux éléments: l'en-tête biométrique, qui contient des données relatives au type et à la version de l'algorithme biométrique utilisé, et les données de référence, qui présentent les caractéristiques des empreintes à proprement parler. Les données de référence sont calculées et stockées sur la carte au moment de l'enrôlement de l'utilisateur. L'algorithme biométrique ne fonctionne que dans un sens; en d'autres termes, il n'est pas possible de reconstituer les empreintes numérisées à partir des données de référence.

Il existe deux types de lecteurs de cartes: le lecteur classique, qui lit le numéro de la carte, lequel est vérifié par le contrôleur d'accès, et le lecteur de type biométrique, qui est capable de numériser l'empreinte digitale d'une personne et de vérifier sa concordance avec l'une de celles qui sont stockées sur la carte. En cas de concordance, le lecteur transmet le numéro d'indentification de la carte au système de contrôle d'accès. L'accès est autorisé ou refusé en fonction des autorisations programmées dans le système pour la carte en question.

Le taux de faux rejets pour toutes les parties du bâtiment est fixé à 1 %. En outre, le système autorise dix essais par doigt dont l'empreinte a été enregistrée avant de bloquer la carte.

Les contrôleurs d'accès contiennent la liste des numéros des cartes autorisées pour les zones définies dans le système, et autorisent ou refusent l'accès en fonction de cette liste. Par ailleurs, ils enregistrent le protocole des accès et le transmettent au serveur de base de données central.

Le serveur de base de données central constitue l'interface administrative avec le système. Il conserve les informations concernant les utilisateurs et leurs droits d'accès. Il conserve également la trace de toutes les tentatives d'accès, fructueuses ou non.

Personnes concernées

D'après le formulaire de notification, les personnes concernées sont les suivantes: chacun des membres du personnel de l'OLAF, y compris le personnel statutaire, les experts nationaux détachés et le personnel intra-muros travaillant pendant une période continue dans les locaux de l'OLAF.

Les visiteurs et les autres membres du personnel de la Commission se verront délivrés une carte temporaire - ils ne sont pas enregistrés dans le système.

Catégories de données concernées

Les catégories de données concernées sont les suivantes:

- données personnelles d'identification (nom, numéro personnel, photo);
- numéro de la carte;
- informations relatives à la procédure d'habilitation;
- empreintes digitales (sur la carte d'identification personnelle uniquement);
- droits d'accès.

Plus précisément, les données ci-après sont journalisées par le système de contrôle d'accès à chaque fois qu'une carte est présentée à un lecteur. Lorsqu'une authentification de l'utilisateur (par ses empreintes digitales) est requise, ces informations ne sont journalisées que pour les tentatives fructueuses: date, heure, nom, autorisation ou refus de l'accès, nom du groupe d'accès et numéro et description du lecteur de cartes.

En ce qui concerne les droits d'accès, le périmètre de sécurité de l'OLAF est divisé en plusieurs zones. Le système de contrôle d'accès permet de définir différentes "familles". Une famille contient la liste des zones sécurisées et des heures auxquelles le système en autorise l'accès. Les droits d'accès aux locaux sécurisés de l'OLAF, et en leur sein, sont définis par l'appartenance des utilisateurs à une famille. L'appartenance à une famille est décidée par l'OLAF, selon la catégorie de fonction des membres du personnel concernés.

Destinataires des données
Conformément à la notification et à la déclaration de confidentialité, les informations relatives au contrôle d'accès ne sont accessibles qu'aux gestionnaires de sécurité de l'OLAF. En cas d'incident de sécurité, ces informations peuvent être communiquées à la direction de la sécurité de la Commission et/ou à l'Office d'investigation et de discipline (IDOC).

Information des personnes concernées
Une déclaration de confidentialité sera disponible sur l'Intranet et sur le site Internet de l'OLAF, ainsi qu'auprès du poste de garde à l'entrée du bâtiment de l'OLAF, sur demande.

La déclaration de confidentialité comprend les éléments suivants: une explication du système de contrôle d'accès de l'OLAF, les informations à caractère personnel collectées, ainsi que la fin à laquelle ces informations sont collectées et les moyens techniques utilisés pour cette collecte, les destinataires des informations et les personnes à qui elles sont communiquées, les modalités de protection des informations, la période de conservation des données, la présentation des droits des personnes concernées (en termes d'accès, de modification et de suppression) et la mention du droit de saisir le CEPD. La DPD a joint un projet de déclaration de confidentialité à la notification.

Droits des personnes concernées
Dans la déclaration de confidentialité, les droits des personnes concernés sont décrits comme suit: "*Vous avez le droit d'accéder aux données à caractère personnel que détient l'OLAF vous concernant, de les corriger et de les compléter. Toute demande d'accès, de rectification, de verrouillage et/ou d'effacement des données à caractère personnel vous concernant doit être adressée à M. [...], chef de l'unité D8 [adresse électronique]. Vous pouvez également contacter M. [...] en cas de problème ou pour toute question liée au traitement des données à caractère personnel vous concernant. Les exceptions prévues à l'article 20, paragraphe 1, points a) et b) du règlement (CE) nº 45/2001, pourraient s'appliquer.*"

En outre, le délai de verrouillage des données, sur demande légitime et motivée de la personne concernée, est fixé à un mois.

Durée de conservation des données
D'après la notification et la déclaration de confidentialité, les données enregistrées (soit les informations relatives au contrôle d'accès) ne seront pas conservées plus d'un an. Cette période de conservation est nécessaire car tous les incidents de sécurité ne sont pas détectés immédiatement. L'OLAF estime qu'une période de conservation totale d'un an est raisonnable pour ce qui le concerne, compte tenu du caractère sensible de ses activités opérationnelles.

Traitement automatisé/manuel
Le traitement automatisé comprend ce qui suit: la lecture d'une carte d'accès personnelle par un lecteur de cartes classique/biométrique, la transmission des données du lecteur au contrôleur d'accès, l'enregistrement du protocole des accès par le contrôleur et la transmission par ce dernier du protocole au serveur de base de données central, ainsi que la conservation d'informations par ce serveur.

Le traitement manuel, quant à lui, n'interviendra qu'en cas d'incident de sécurité, auquel cas le responsable de la sécurité se connectera à la base de données de contrôle d'accès afin d'en extraire les informations relatives aux personnes qui sont entrées dans les locaux de l'OLAF ou qui en sont sorties à une heure donnée.

Stockage
Les données sont enregistrées dans une base de données sur un disque dur et un support de sauvegarde. Les empreintes digitales sont stockées sur les cartes d'identification personnelles.

Mesures de sécurité
Des mesures de sécurité sont appliquées. En particulier, les empreintes digitales sont stockées sur les cartes d'identification personnelles. (...).

En outre, des mesures de sécurité sont également prises pendant la phase d'enrôlement, qui a lieu au sein de l'Unité Administration et ressources humaines. (...).

2.2. Aspects juridiques

2.2.1. Contrôle préalable

Le présent avis en vue d'un contrôle préalable porte sur le traitement d'informations à caractère personnel auquel procède l'OLAF, en particulier l'Unité Services de l'information, pour contrôler l'identité des personnes entrant et sortant des locaux de l'OLAF, ainsi que des zones spéciales sécurisées, et leur en autoriser ou refuser l'accès.

Le règlement (CE) n° 45/2001[1] 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 dans un fichier"* ainsi qu'au traitement de données *"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*".[2] Pour les raisons exposées ci-dessous, tous les éléments justifiant l'application du règlement (CE) nº 45/2001 sont réunis en l'espèce.

Premièrement, les *données à caractère personnel* telles que définies à l'article 2, point a), du règlement (CE) n° 45/2001 sont collectées et traitées ultérieurement. Deuxièmement, les données à caractère personnel collectées font l'objet de *traitements automatisés*, tels que définis à l'article 2, point b), du règlement (CE) n° 45/2001, ainsi que de traitements manuels. En effet, les données à caractère personnel, telles que les données personnelles d'identification et les empreintes digitales, sont collectées et font l'objet d'un traitement automatisé, par exemple lorsque l'Unité Services de l'information établit les modèles d'empreintes. Enfin, le traitement est

[1] Règlement (CE) n° 45/2001 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 (ci-après dénommé "le règlement (CE) n° 45/2001").

[2] Voir l'article 3 du règlement (CE) n° 45/2001.

effectué par un organe communautaire, ici l'Office européen de lutte antifraude, dans le cadre du droit communautaire (article 3, paragraphe 1, du règlement (CE) n° 45/2001). Par conséquent, tous les éléments justifiant l'application du règlement (CE) nº 45/2001 sont réunis en l'espèce.

L'article 27, paragraphe 1, du règlement (CE) n° 45/2001 soumet au contrôle préalable du CEPD *"les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités"*. Le CEPD estime que la présence de certaines données biométriques autres que les seules photographies, comme c'est le cas en l'espèce, où des empreintes digitales biométriques sont collectées, présente des risques particuliers au regard des droits et libertés des personnes concernées. Ce point de vue se fonde principalement sur la nature des données biométriques, qui sont extrêmement sensibles en raison de certaines des caractéristiques qui leur sont inhérentes. Ainsi, les données biométriques modifient irrévocablement la relation entre le corps et l'identité en ce sens qu'elles rendent les caractéristiques du corps humain "lisibles par une machine" et susceptibles d'être utilisées ultérieurement. Outre la nature extrêmement sensible de ces données, le CEPD note également les possibilités d'interconnexions et la situation actuelle en termes d'outils technologiques, qui peuvent avoir des conséquences inattendues et/ou fâcheuses pour les personnes concernées. Ces risques justifient la nécessité de soumettre le traitement des données à un contrôle préalable du CEPD afin de vérifier que des mesures de protection strictes ont été mises en œuvre.

Étant donné que le contrôle préalable vise à examiner des situations susceptibles de présenter certains risques, le CEPD devrait rendre son avis avant le début du traitement. Le présent avis constitue un **contrôle préalable à proprement parler**. En conséquence, le traitement en question ne devrait pas être mis en œuvre avant d'avoir été officiellement approuvé par le CEPD.

La notification a été reçue le 17 octobre 2007. Conformément à l'article 27, paragraphe 4, du règlement (CE) n° 45/2001, le délai de deux mois dans lequel le CEPD doit rendre son avis a été suspendu pendant 102 jours au total afin d'obtenir des informations complémentaires, plus 8 jours pour permettre la présentation d'observations sur le projet d'avis. Le présent avis doit donc être adopté au plus tard le 7 avril 2008 (le 6 avril étant un dimanche).

2.2.2. Licéité du traitement

Le traitement de données à caractère personnel ne peut être effectué que s'il est justifié par des motifs visés à l'article 5 du règlement (CE) n° 45/2001.

Parmi les différents motifs énumérés à l'article 5 du règlement (CE) n° 45/2001, le traitement notifié en vue d'un contrôle préalable relève de l'article 5, point a), qui prévoit que le traitement de données peut être effectué s'il "*est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités ou relevant de l'exercice légitime de l'autorité publique dont est investi l'institution ou l'organe communautaire ou le tiers auquel les données sont communiquées*".

Afin de déterminer si le traitement est conforme à l'article 5, point a), du règlement (CE) n° 45/2001, il convient de répondre aux trois questions ci-après. Premièrement, le traité ou d'autres actes législatifs prévoient-ils ce traitement? Deuxièmement, le traitement est-il effectué dans l'intérêt public? Troisièmement, le traitement est-il effectivement nécessaire à l'exécution de cette mission (critère de la nécessité)? Bien évidemment, ces trois exigences sont étroitement liées.

* La **base juridique** du traitement comprend:

- l'article 297 du traité CE et l'article 17 du statut des fonctionnaires;
- le règlement (CE) n° 1073/1999: considérants 4, 17 et 18 et article 8, article 11, paragraphe 1, et article 12, paragraphe 3;
- la décision 1999/352/CE de la Commission: considérants 4 et 5 et article 3;
- la décision 2001/844/CE, CECA, Euratom de la Commission (dispositions en matière de sécurité);
- la décision 2006/3602/CE de la Commission concernant la sécurité des systèmes d'information;
- la politique de la Commission en matière de sécurité des systèmes d'information; et
- la politique de l'OLAF en matière de sécurité de l'information (point 4.5 du manuel de l'OLAF).

* Le traitement est effectué **dans l'exercice légitime de l'autorité publique**. Le CEPD note que la Commission met en œuvre le traitement dans l'exercice légitime de son autorité publique. En effet, le traitement s'inscrit dans le cadre d'une mission effectuée dans l'intérêt public sur la base du statut des fonctionnaires des Communautés européennes et du régime applicable aux autres agents des Communautés, ainsi que de la politique de l'OLAF en matière de sécurité de l'information. Le critère d'admissibilité du traitement est donc respecté.

* En ce qui concerne la nécessité du traitement (**critère de la nécessité**), selon l'article 5, point a), du règlement (CE) n° 45/2001, le traitement des données doit être "*nécessaire à l'exécution d'une mission*", comme indiqué ci-dessus. À cet égard, le considérant 27 précise que: "*le traitement de données à caractère personnel effectué pour l'exécution de missions d'intérêt public par les institutions et les organes communautaires comprend le traitement de données à caractère personnel nécessaires pour la gestion et le fonctionnement de ces institutions et organes*".

La mission de l'OLAF consiste à protéger les intérêts financiers et les autres intérêts de la Communauté contre la fraude et des comportements irréguliers susceptibles de poursuites administratives ou pénales. En outre, l'OLAF exerce les compétences de la Commission en vue de renforcer la lutte contre la fraude, la corruption et toute autre activité illégale portant atteinte aux intérêts financiers de la Communauté[3].

Compte tenu de l'importance de ces intérêts et afin d'empêcher tout accès non autorisé à ces informations sensibles ou toute diffusion non autorisée de celles-ci, l'OLAF pourrait en effet devoir adopter des mesures de sécurité spécifiques, y compris en mettant en place des systèmes de contrôle d'accès stricts à des zones données de l'OLAF. En conséquence, de l'avis du CEPD, la mise en œuvre de systèmes de contrôle d'accès rigoureux donnant lieu au traitement de données à caractère personnel peut, en l'espèce, être raisonnablement considérée comme une mesure de contrôle interne nécessaire à la protection des informations financières et des autres intérêts de la Communauté.

2.2.3. Traitements portant sur des catégories particulières de données

Le traitement de données notifié ne concerne pas des données relevant des catégories de données visées à l'article 10, paragraphe 1, du règlement (CE) n° 45/2001.

2.2.4. Qualité des données

Adéquation, pertinence et proportionnalité. En vertu de l'article 4, paragraphe 1, point c), du règlement (CE) n° 45/2001, les données doivent être adéquates, pertinentes et non excessives au

[3] Manuel de l'OLAF, p. 13.

regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement. Ce principe est appelé "principe de la qualité des données". En analysant la conformité du traitement en l'espèce, qui consiste essentiellement à traiter des données biométriques, avec ce principe, le CEPD a noté ce qui suit.

Ainsi qu'il est indiqué dans la notification, chaque membre du personnel de l'OLAF est considéré comme une personne concernée. En outre, la notification précise que le système en question est destiné à contrôler les identités et à autoriser ou refuser l'accès à toutes les entrées et sorties du périmètre de sécurité physique de l'OLAF au sein du bâtiment de l'Office en dehors des heures de service, ainsi que des zones spéciales sécurisées. En conséquence, chaque membre du personnel de l'OLAF doit disposer d'une carte de l'OLAF afin d'être autorisé à accéder aux locaux sécurisés de l'Office. Néanmoins, le CEPD ne juge pas nécessaire de relever les empreintes digitales de chacun des membres du personnel de l'OLAF. En effet, seuls ceux qui peuvent être amenés à travailler en dehors des heures de service et ceux qui doivent accéder aux zones spéciales sécurisées du bâtiment de l'OLAF devraient voir leurs empreintes enregistrées sur leur carte.Par ailleurs, l'OLAF a informé le CEPD des raisons qui ont justifié l'utilisation d'éléments biométriques dans ses systèmes de sécurité spécifiques. La politique de l'OLAF en matière de sécurité de l'information, élaborée afin de mettre en œuvre les exigences de sécurité applicables au sein de l'OLAF, exige une application rigoureuse du principe du besoin d'en connaître.

Cela suppose une identification sans équivoque, c'est-à-dire une authentification forte, de tout utilisateur des systèmes de traitement des données opérationnelles de l'OLAF. S'agissant du contrôle d'accès de l'OLAF, le CEPD interprète le principe du besoin d'en connaître comme exigeant que seules les personnes qui ont besoin d'un accès spécial soient enregistrées dans le système et, par conséquent, fassent l'objet d'un relevé d'empreintes. Ainsi, compte tenu de ce qui précède, le CEPD recommande que l'OLAF réexamine la question et envisage la possibilité de limiter la liste des personnes dont les empreintes devront être enregistrées, au vu des besoins réels en termes d'accès à l'OLAF en dehors des heures normales de service, ou d'accès aux zones sécurisées au sein de l'OLAF, ou encore d'utilisation des points d'accès non surveillés (cages d'escalier) aux locaux sécurisés de l'OLAF.

Le type de données collectées, essentiellement des modèles d'empreinte de trois doigts et des données d'identification associées, correspond aux données que requiert l'exploitation d'un système de contrôle d'accès fondé sur la biométrie. De ce point de vue, le CEPD estime que les données collectées sont adéquates et pertinentes au regard des finalités du traitement.

L'OLAF a opté pour une combinaison de deux des trois[4] facteurs d'authentification définis par la politique de la Commission en matière de sécurité des systèmes d'information (authentification par la possession et par les caractéristiques personnelles). L'OLAF a par ailleurs indiqué que les garanties de sécurité fournies par la combinaison de ces deux facteurs d'authentification étaient jugées suffisantes pour satisfaire aux exigences de la politique de l'OLAF en matière de sécurité de l'information.

Le CEPD se félicite de cette pratique, ainsi que du raisonnement de l'OLAF. En effet, compte tenu de la nature extrêmement sensible des données biométriques, de manière à évaluer comme il se doit le caractère adéquat du recours à ces données à des fins de contrôle d'accès, il est nécessaire de procéder à une ***analyse d'impact ciblée*** qui examine les raisons ayant justifié le recours à cette technologie et détermine si d'autres solutions, portant moins atteinte à la vie privée, ont été envisagées. Néanmoins, dans une perspective d'avenir et plus particulièrement dans le cadre d'éventuelles actualisations du système, l'OLAF, outre des aspects techniques et de sécurité, devrait également tenir compte de

[4] Le troisième facteur d'authentification (par la connaissance, c'est-à-dire par un mot de passe ou un code PIN) a été jugé inadapté aux exigences de sécurité auxquelles sont soumises les données opérationnelles de l'OLAF, étant trop dépendant de l'utilisateur.

considérations liées à la protection des données et de la vie privée lorsqu'il procède à une analyse d'impact.

Loyauté et licéité. L'article 4, paragraphe 1, point a), du règlement (CE) n° 45/2001 exige que les données soient traitées loyalement et licitement. La question de la licéité a été analysée ci-dessus (voir point 2.2.2). Celle de la loyauté est étroitement liée à l'objet du point 2.2.8, à savoir les informations fournies aux personnes concernées.

Exactitude. Conformément à l'article 4, paragraphe 1, point d), du règlement (CE) n° 45/2001, les données à caractère personnel doivent être "exactes et, si nécessaire, mises à jour" et "toutes les mesures raisonnables sont prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées".

En l'espèce, les données à caractère personnel sont principalement constituées de données biométriques, utilisées à des fins de contrôle d'accès. Certaines caractéristiques essentielles des systèmes biométriques ont une incidence directe sur le niveau d'exactitude des données générées pendant les phases soit d'enrôlement soit d'identification inhérentes à ce type de système. La question de l'exactitude des données se posera dans la mesure où le système biométrique mis en place intègre ces caractéristiques essentielles. Nous décrivons ci-après ces caractéristiques essentielles et analysons la mesure dans laquelle elles ont été prises en compte dans le système biométrique examiné.

Premièrement, toute phase d'enrôlement doit prévoir des solutions de remplacement permettant d'identifier des personnes qui ne peuvent pas être enregistrées, ne serait-ce que temporairement, par exemple en raison d'empreintes digitales endommagées. C'est ce qu'on appelle habituellement des ***procédures de secours***[5]**.** D'après les informations complémentaires reçues, l'OLAF n'a pas prévu de taux d'enregistrements impossibles, puisqu'il part du principe que l'ensemble du personnel pourra être enregistré. En outre, si un membre du personnel, pour quelque raison que ce soit, ne peut ou ne veut pas être enregistré, temporairement ou de manière permanente, en vertu de la procédure prévue par l'OLAF, il ne pourra accéder à l'OLAF que pendant les plages horaires fixes et par les portes d'accès automatiques réservées au personnel, situées dans le hall surveillé, qui régulent l'accès aux ascenseurs de l'OLAF. Il ne pourra pas utiliser les escaliers pour accéder au périmètre de sécurité de l'OLAF.

Au terme de son analyse, le CEPD conclut que bien que l'OLAF prévoie que l'ensemble de son personnel pourra être enregistré, il a mis en œuvre une procédure de secours, étant donné que trois modèles d'empreinte, et non un seul, sont relevés pendant la phase d'enrôlement. Au cours du processus d'authentification biométrique, l'utilisateur présente l'un des trois doigts qu'il a choisis lors de la phase d'enrôlement. Bien que cette solution réduise le risque d'enregistrements impossibles, il est toujours possible que, de manière temporaire, certaines personnes ne puissent pas être enregistrées dans le système de reconnaissance des empreintes digitales. Dans ce cas, le CEPD suggère que l'OLAF mette en œuvre une solution de remplacement. Celle-ci pourrait prévoir qu'une personne habilitée accompagne dans ses déplacements la personne qui accède aux zones sécurisées du bâtiment de l'OLAF. Par ailleurs, en cas d'impossibilité permanente de procéder à l'enregistrement, l'OLAF devrait mettre au point une solution de remplacement réaliste.

---

5 Pour une description des principes en matière de protection des données applicables dans le cadre des procédures de secours, voir l'avis du 13 octobre 2006 sur le projet de règlement du Conseil (CE) portant fixation de la forme des laissez-passer délivrés aux membres et aux agents des institutions (JO C 313 du 20.12.2006, p. 36).

Deuxièmement, des mesures semblables doivent être prévues pour les personnes qui ont été correctement enregistrées, mais qui ne peuvent pas être identifiées (ce que l'on appelle généralement les "***faux rejets***"). Si ces mesures ne sont pas intégrées dans l'architecture du système, l'exactitude des informations générées par le système pourrait être compromise. En particulier, en cas de faux rejet, le système gardera trace du fait qu'une personne donnée, ne disposant pas des droits d'accès requis, a tenté d'accéder à une zone sécurisée, alors même que cette personne disposait des droits correspondants. Dans le même temps, puisque cette personne n'aura pas pu être identifiée, elle se verra refuser un droit (droit d'accès à des zones données de l'OLAF ou droit d'accès à certaines heures) dont elle bénéficie.

En ce qui concerne le système de contrôle d'accès de l'OLAF, le taux de faux rejets pour l'ensemble du bâtiment est fixé à 1 %, ce qui correspond au niveau de sécurité auquel devraient satisfaire les bâtiments de l'OLAF. En outre, le système autorise dix essais par doigt dont l'empreinte a été enregistrée avant de bloquer la carte. Le CEPD estime que cette solution devrait limiter le risque de rejets. Néanmoins, s'agissant des faux rejets, le CEPS suggère que l'OLAF mette en place une mesure de remplacement semblable à celle applicable aux enregistrements impossibles. Cette procédure devrait résoudre le problème sans être trop contraignante pour les personnes concernées. En d'autres termes, les procédures de remplacement devraient fournir des solutions suffisamment simples au problème de non-identification et de rejet.

Troisièmement, le système de contrôle d'accès physique de l'OLAF se fonde sur des modèles d'empreintes stockés sur des cartes, associés à l'utilisation de lecteurs. Ce système de contrôle d'accès physique n'utilise pas un dispositif d'authentification fondé sur une concordance à 100 % avec les informations contenues dans la carte (technologie "*match-on-card*"). L'OLAF a mis en œuvre un mode de recherche fondé sur la comparaison de deux empreintes ("*one-to-one*"), qui consiste à comparer les données biométriques à un seul modèle d'empreinte, et non à plusieurs. Le CEPD se félicite de la mise en place de ce système, qui évite toute autre utilisation illicite et tout recours à l'hameçonnage ("*phishing*"), auxquels l'utilisation de base des données donne souvent lieu[6].

Enfin, le CEPD souhaite mettre l'accent sur un dernier élément relatif à la qualité des données. Les éléments biométriques, en particulier les empreintes digitales, peuvent évoluer au cours de la vie d'une personne concernée. Afin de garantir un niveau élevé d'exactitude des données, le CEPD suggère à l'OLAF de mettre en place une procédure prévoyant que les membres du personnel de l'OLAF doivent renouveler leur enregistrement à intervalles réguliers. La périodicité appropriée sera déterminée en fonction du type de population qui doit renouveler son enregistrement (c'est-à-dire de la qualité des données spécifiques fournies par la personne concernée), ainsi que de la fréquence d'utilisation du système.

2.2.5. Conservation des données

L'article 4, paragraphe 1, point e), du règlement (CE) n° 45/2001 pose le principe que les données à caractère personnel doivent être "*conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement*". *"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 […] statistiques*

[6] Voir l'avis du 14 février 2008 rendu à la suite d'une notification adressée par le délégué à la protection des données de la Banque centrale européenne concernant l'intégration dans un système de contrôle d'accès préexistant d'une technologie d'analyse de l'iris pour les zones hautement sécurisées de la BCE (dossier 2007-501).

[…], 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."

D'après la notification, les données enregistrées (soit les informations relatives au contrôle d'accès) ne seront pas conservées plus d'un an. Ces données sont nécessaires pour enquêter sur les incidents de sécurité. Pour justifier cette période de conservation, l'OLAF indique qu'elle est nécessaire car tous les incidents en matière de sécurité ne sont pas détectés immédiatement. Ainsi, certaines enquêtes de sécurité ont été lancées deux ou trois ans après la divulgation d'un document sensible relatif aux activités de l'OLAF. L'OLAF estime donc qu'une période de conservation totale d'un an est raisonnable pour ce qui le concerne, compte tenu du caractère sensible de ses activités opérationnelles.

LE CEPD estime que la rapidité de la détection des incidents de sécurité est essentielle. En effet, plus un système est sensible, plus précoce doit être la détection des incidents de sécurité. Le CEPD reconnaît qu'il peut être nécessaire de conserver une piste de vérification de l'enregistrement des données pendant une période qui permette de reconstituer les événements intervenus pendant les incidents de sécurité et que, dans le cas de l'OLAF, une période très courte pourrait créer des difficultés pratiques. Le CEPD part du principe que l'OLAF a mis en place, ou, si ce n'est pas le cas, qu'il devrait mettre au point, une procédure d'identification des incidents et de réaction à ceux-ci, afin qu'ils soient détectés et signalés dès que possible. On peut supposer que l'OLAF a pour objectif de détecter les incidents immédiatement après qu'ils ont eu lieu et, en tout état de cause, au plus tard quelques mois après cette date. Compte tenu de ce qui précède, le CEPD est d'avis qu'une période de conservation d'un an est trop longue et invite l'OLAF à réexaminer la période qu'il a fixée en réexaminant la nécessité de raccourcir cette période sur la base de statistiques relatives aux incidents. En conséquence, la période de conservation devrait être déterminée en fonction du laps du temps qui s'écoule habituellement entre le moment où l'incident de sécurité a lieu et celui où l'OLAF le détecte. Le CEPD est conscient que l'OLAF ne dispose pas de telles statistiques sur les incidents, mais estime qu'il sera en mesure de réexaminer la période de conservation initiale un an après le début de l'exploitation de son nouveau système. Ainsi, le CEPD est d'accord pour que l'OLAF propose une nouvelle période de conservation sur la base des statistiques dont il disposera alors.

Le délai de verrouillage ou d'effacement des données, sur demande légitime et motivée de la personne concernée, est, quant à lui, fixé à un mois. Le CEPD estime que cette période de conservation est conforme aux exigences fixées à l'article 4, paragraphe 1, point e), du règlement (CE) n° 45/2001.

À la lecture de la notification, le CEPD conclut que l'établissement de statistiques relatives aux données à caractère personnel n'est pas autorisé au-delà de la période de conservation. Néanmoins, le CEPD tient à souligner que, en cas d'utilisation de ces données au-delà de la période de conservation, il est nécessaire que ces données soient rendues anonymes (article 4, paragraphe 1, point e), du règlement (CE) n° 45/2001).

2.2.6. Transfert des données

D'après la notification, les informations relatives au contrôle d'accès ne sont accessibles qu'aux gestionnaires de sécurité de l'OLAF. En cas d'incident de sécurité, ces informations peuvent être communiquées à la direction de la sécurité de la Commission et/ou à l'Office d'investigation et de discipline (IDOC). Ces informations peuvent donc être transférées au sein de la Commission dans le cadre d'une enquête de sécurité, mais elles ne seront en aucun cas transférées à l'extérieur de la Commission. L'article 7 du règlement (CE) n° 45/2001, qui prévoit certaines obligations

dans le cas où les responsables du traitement transfèrent des données à caractère personnel, aux institutions ou organes communautaires, s'appliquera par conséquent.

Le CEPD rappelle que cet article prévoit que les données à caractère personnel ne sont transférées "*que si elles sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire*". Pour respecter cette disposition, l'OLAF doit s'assurer, lorsqu'il communique des données à caractère personnel, que i) le destinataire a les compétences requises et ii) le transfert est nécessaire. Il convient d'apprécier au cas par cas si un transfert donné satisfait à ces exigences. En outre, conformément à l'article 7 du règlement (CE) n° 45/2001, il convient d'informer le destinataire que les données à caractère personnel peuvent uniquement être traitées aux fins qui ont motivé leur transmission.

2.2.7. Traitement d'un numéro personnel ou d'un identifiant unique

L'article 10, paragraphe 6, du règlement (CE) nº 45/2001 prévoit que "*le contrôleur européen de la protection des données détermine les conditions dans lesquelles un numéro personnel ou tout autre identifiant utilisé de manière générale peut faire l'objet d'un traitement par une institution ou un organe communautaire*." Le présent avis ne fixe pas les conditions générales d'utilisation d'un tel numéro personnel, mais examine les mesures particulières nécessaires à cet égard dans le cadre d'un système de contrôle d'accès.

LE CEPD a déjà précisé, dans un précédent avis en vue d'un contrôle préalable[7], le statut du numéro d'une puce RFID intégrée dans une carte. Le numéro d'identification associé à la puce RFID est une donnée à caractère personnel relevant du règlement (CE) n °45/2001. En effet, lorsque le numéro d'identification est utilisé pour enregistrer le comportement d'un membre du personnel et qu'il est associé à un numéro personnel (c'est-à-dire au nom d'une personne, comme c'est le cas ici), le traitement en question concerne des données à caractère personnel, ce qui impose le respect des principes applicables en matière de protection des données.

Le recours au numéro personnel est nécessaire dans la mesure où le numéro d'identification de la carte est communiqué au système de contrôle d'accès. Les contrôleurs d'accès contiennent la liste des numéros des cartes autorisées pour les zones définies dans le système, et accordent ou refusent l'accès en fonction de cette liste. Par ailleurs, ils enregistrent le protocole des accès et le transmettent au serveur de base de données central.

En l'espèce, l'utilisation du numéro personnel à des fins de vérification des données relatives au droit d'accès contenues dans le système est raisonnable dans la mesure où ce numéro est utilisé à des fins d'identification de la personne dans le système et où il contribue dès lors à garantir l'exactitude des données.

2.2.8. Droit d'accès et de rectification

Conformément à l'article 13 du règlement (CE) n° 45/2001, la personne concernée a le droit d'obtenir, sans contrainte, à tout moment dans un délai de trois mois à partir de la réception de la demande d'information et gratuitement, du responsable du traitement, la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données. L'article 14 du règlement (CE) n° 45/2001 confère à la personne concernée le droit de rectifier les données inexactes ou incomplètes.

---

[7] Voir l'avis du 19 octobre 2007 sur une notification en vue d'un contrôle préalable reçue du délégué à la protection des données de la Commission européenne à propos de la "mise en œuvre du Flexitime spécifique à la DG INFSO" (dossier 2007-218).

La notification en vue d'un contrôle préalable et les informations complémentaires fournies par le responsable du traitement décrivent la manière dont un membre du personnel peut accéder aux données à caractère personnel le concernant et mentionnent la possibilité qu'il a de les rectifier.

Conformément à la notification en vue d'un contrôle préalable et aux informations complémentaires fournies par le responsable du traitement, les droits d'accès et de rectification sont reconnus. La déclaration de confidentialité remise au CEPD pour examen indique le nom de la personne responsable de l'exécution de ces droits. Le CEPD rappelle que ces droits s'appliquent non seulement aux informations fournies par la personne concernée (données d'identification et modèles d'empreintes), mais également aux informations générées à chaque fois qu'une personne accède à une zone hautement sécurisée.

Le CEPD note que, d'après la notification, l'article 20 du règlement (CE) n° 45/2001 ne s'applique pas, en principe, dans le cadre du traitement de données examiné.

En conclusion, le CEPD estime que les conditions des articles 13 et 14 du règlement (CE) n° 45/2001 sont remplies.

2.2.9. Information de la personne concernée

Les articles 11 et 12 du règlement (CE) n° 45/2001 énumèrent les informations à fournir à la personne concernée. Ces articles présentent une liste d'informations obligatoires et une série d'autres informations.

Ces dernières doivent être fournies dans la mesure où, compte tenu des conditions particulières du traitement examiné, elles sont nécessaires pour garantir un traitement équitable des données à l'égard de la personne concernée. Dans ce cas, une partie des données est collectée directement auprès de la personne concernée et une autre partie auprès de tiers.

Dans le présent dossier, il y a lieu d'observer les dispositions de l'article 11 (*Informations à fournir lorsque les données sont collectées auprès de la personne concernée*). Étant donné que les membres du personnel pointeront personnellement dans le système, les personnes concernées fourniront elles-mêmes les données.

L'article 12 (*Informations à fournir lorsque les données n'ont pas été collectées auprès de la personne concernée*) devrait également s'appliquer, étant donné que la liste des données d'identification est extraite du SYSPER 2 en ce qui concerne les membres du personnel de l'OLAF.

Les personnes concernées sont informées au moyen d'une *déclaration de confidentialité concernant le contrôle d'accès à l'OLAF*. Afin d'établir le respect des articles ci-dessus, une copie de la déclaration de confidentialité a été communiquée au CEPD.

Cette déclaration contient des informations sur les finalités du traitement et sur la manière dont le traitement est effectué, sur les conditions d'exercice du droit d'accès et de rectification, sur les délais de conservation des données et sur la possibilité de saisir le CEPD. Le CEPD estime que cette déclaration de confidentialité contient la plupart des informations requises en vertu des articles 11 et 12 du règlement (CE) n° 45/2001. Néanmoins, il est d'avis que quelques modifications permettraient de garantir le plein respect de ces articles, en particulier:

- la mention de la base juridique du traitement auquel les données sont destinées;

- la mention du caractère obligatoire ou facultatif de la réponse aux questions ainsi que des conséquences éventuelles d'un défaut de réponse (par exemple des conséquences d'un enregistrement impossible). Par analogie avec un questionnaire, le personnel devrait être informé des conséquences concrètes d'un enregistrement ou d'un enregistrement impossible.

En outre, la déclaration de confidentialité est en principe fournie aux personnes qui sont soumises à une procédure d'enrôlement afin de pouvoir accéder au périmètre de sécurité physique de l'OLAF. Dans un autre avis en vue d'un contrôle préalable[8], le CEPD a pris acte de la procédure mise en œuvre au sein de la BCE (la déclaration de confidentialité "*sera fournie sur papier et les intéressés seront invités à la signer, précisant qu'ils l'ont lue et comprise*"). Le CEPD estime qu'il s'agit là d'un moyen approprié de communiquer les informations et suggère que les personnes concernées reçoivent une copie de la déclaration de confidentialité, de manière à pouvoir la consulter si elles souhaitent, par exemple, savoir comment exercer leurs droits ou comment s'effectue le traitement des données les concernant.

2.2.10. Mesures de sécurité

Conformément aux articles 22 et 23 du règlement (CE) n° 45/2001, le responsable du traitement et le sous-traitant doivent mettre en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à caractère personnel à protéger. Ces mesures de sécurité doivent notamment empêcher toute diffusion ou tout accès non autorisés, toute destruction accidentelle ou illicite, toute perte accidentelle ou toute altération, ainsi que toute autre forme de traitement illicite. Les mesures techniques et organisationnelles prévues semblent adéquates pour assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.

Le choix de la technologie utilisée pour le système mis en place par l'OLAF se fonde sur les recommandations de la direction de la sécurité. Un choix a donc dû être opéré concernant la technologie utilisée pour la connexion cartes/lecteurs dans le système mis en place. Le CEPD n'a pas été invité à participer aux discussions et aux choix ayant conduit à la sélection de la technologie utilisée[9].

Le CEPD regrette cet état de fait, estimant que d'autres solutions auraient pu être examinées en termes de sécurité et de cryptage, qui auraient renforcé le niveau de protection des données et de sécurité présentés par les cartes et les lecteurs. À cet égard, le CEPD recommande à l'OLAF de revenir sur sa décision concernant le choix technologique qu'il a opéré, en procédant à une nouvelle évaluation comprenant un calendrier réaliste de mise en œuvre d'un changement de technologie, compte tenu du choix des meilleures techniques disponibles[10] et des discussions actuellement menées sur les futurs systèmes de sécurité.

---

8 Voir l'avis sur le contrôle d'accès à la Banque centrale européenne (dossier 2007-501).

9 Le CEPD a fait la même remarque s'agissant du Flexitime spécifique à la DG INFSO dans le dossier 2007-0218.

10 Le CEPD a mis en avant cette notion des meilleures techniques disponibles dans son rapport annuel 2006. Par ailleurs, le CEPD se tient à disposition pour fournir des orientations concernant d'éventuels autres choix technologiques à l'avenir.

Conclusion:

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

- réexaminer la question et envisager la possibilité de limiter la liste des personnes dont les empreintes devront être enregistrées sur les cartes;
- tenir compte, outre des aspects de sécurité, de considérations liées à la protection de la vie privée/des données lorsqu'il procèdera à des analyses d'impact à l'avenir;
- mettre au point des procédures de secours tenant compte de l'impossibilité temporaire pour des membres du personnel de faire l'objet d'un relevé d'empreintes lors de la phase d'enrôlement et concevoir des mesures de remplacement pour résoudre le problème des faux rejets;
- mettre en place une procédure prévoyant que les membres du personnel de l'OLAF devront renouveler leur enregistrement à intervalles réguliers;
- réexaminer la période de conservation des données un an après le début de l'exploitation du nouveau système;
- s'agissant des futurs transferts de données, veiller à informer les institutions communautaires recevant des données traitées dans le cadre du système de reconnaissance des empreintes digitales que les données à caractère personnel peuvent uniquement être traitées aux fins qui ont motivé leur transmission;
- modifier la déclaration de confidentialité conformément aux recommandations du présent avis et s'assurer qu'une copie de cette déclaration est remise aux personnes concernées ou qu'elle est mise à leur disposition afin qu'elles puissent la consulter.
- revenir sur sa décision relative au choix technologique qu'il a opéré en procédant à une nouvelle évaluation compte tenu du choix des meilleures techniques disponibles et des discussions sur les futurs systèmes de sécurité.

Fait à Bruxelles, le 4 avril 2008

(Signé)

Joaquín BAYO DELGADO
Contrôleur européen adjoint de la protection des données