Avis sur une notification en vue d'un contrôle préalable transmise par la déléguée à la protection des données de l'Office européen de lutte antifraude relative au système CBIS de gestion de l'identité et de l'accès

Bruxelles, le 30 juin 2008 (dossier 2008-223)

1. Procédure

Le 11 avril 2008, le Contrôleur européen de la protection des données (ci-après dénommé "le CEPD") a reçu de la déléguée à la protection des données (ci-après dénommé "la DPD") 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 un traitement de données à effectuer dans le cadre du système OLAF de gestion de l'identité et de l'accès fonctionnant avec l'infrastructure "Core Business Information Systems" (ci-après dénommée "CBIS").

Les documents suivants étaient joints à la notification:
- bases pour l'utilisation de la biométrie dans les systèmes de sécurité spécifiques de l'OLAF
- technologie "match-on-card"
- projet de déclaration de confidentialité pour le système OLAF de gestion de l'identité et de l'accès

Le 24 avril, le CEPD a reçu des informations supplémentaire de la DPD relatives à un projet pilote envisagé par l'OLAF dans le cadre du traitement. Il a demandé un nouveau complément d'informations sur ce projet pilote le 30 avril et a suspendu la procédure. Le 5 mai, une réunion s'est tenue entre le personnel du CEPD et l'OLAF pour examiner les questions soulevées. La suspension de la procédure a pris fin le 7 mai, lorsque le CEPD a reçu le complément d'informations sur le projet pilote. Le 4 juin 2008, il a envoyé une lettre contenant une analyse des conditions auxquelles le projet pilote pouvait être accepté. Le 5 juin 2008, l'OLAF a décidé de retirer ledit projet.

Le 13 juin, le CEPD a transmis à la DPD de l'OLAF le projet d'avis pour qu'elle fasse part de ses observations, qu'il a reçues le 23 juin 2008.

2. Examen du dossier

2.1 Les faits

Le champ de la notification

Le système de gestion de l'identité et de l'accès (ci-après dénommé "le SGIA") est un élément de l'infrastructure de sécurité qui protège les systèmes informatiques essentiels de l'OLAF qui, à leur tour, permettent à l'OLAF de mener les enquêtes et toutes les autres activités destinées à protéger

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

les intérêts financiers de l'Union européenne. La notification s'y rapportant doit être rattachée à l'avis rendu par le CEPD à l'issue d'un contrôle préalable du système de contrôle physique d'accès de l'OLAF[1].

Le présent avis porte sur le traitement de données à caractère personnel effectué par l'OLAF, en particulier par sa division "Services informatiques", pour veiller à ce que seules les personnes autorisées aient accès à ses systèmes informatiques essentiels de l'OLAF et pour permettre d'enquêter sur des incidents de sécurité.

Le traitement

Le SGIA de l'OLAF est un service d'annuaire pour les systèmes et applications informatiques fonctionnant dans l'environnement sécurisé de l'OLAF, le CBIS. Il offrira des services d'authentification et de contrôle d'accès dans l'environnement CBIS. Les actes de contrôle d'accès journalisés générés dans l'environnement CBIS sont conservés dans le Security Information and Events Management System (SIEMS).

Il ressort de la notification que l'OLAF estime que la mise en œuvre de ce système est nécessaire pour traiter les informations classifiées.

Selon la politique de l'OLAF en matière de sécurité des informations, élaborée afin de mettre en œuvre ces exigences de sécurité en son sein, le principe du "besoin d'en connaître" doit être strictement appliqué, ce qui implique une identification claire, par exemple une authentification rigoureuse, de tout utilisateur des systèmes de traitement des données opérationnelles de l'OLAF.

L'OLAF a joint à la notification une note intitulée "Bases pour l'utilisation de la biométrie dans les systèmes de sécurité spécifiques de l'OLAF", qui explique pourquoi l'office a adopté la biométrie pour identifier les utilisateurs de ses systèmes de sécurité spécifiques, du point de vue de la protection des données. La politique de la Commission en matière de sécurité des systèmes d'information définit trois facteurs d'authentification: authentification par la connaissance, par la possession et par les caractéristiques personnelles.

L'OLAF a décidé de mettre en œuvre un système combinant deux facteurs d'authentification, à savoir la possession et les caractéristiques personnelles pour ses deux systèmes de contrôle d'accès (physique et informatique). Selon le document fourni au CEPD, l'OLAF a adopté les empreintes digitales comme facteur d'authentification par les caractéristiques personnelles parce qu'il estime 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 ou plus onéreux. En ce qui concerne l'authentification par la possession, l'OLAF a recours à une carte à puce. Les données biométriques des utilisateurs sont stockées uniquement sur cette carte à puce et ne peuvent être utilisées à d'autres fins.

L'authentification dans le CBIS repose sur des certificats et des empreintes digitales numériques. Les certificats sont stockés sur les badges OLAF personnels (cartes à puces) des utilisateurs et protégés par un programme d'authentification biométrique "match-on-card" (concordance entre les empreintes de l'utilisateur et les données contenues dans la carte). Chaque utilisateur aura trois modèles d'empreintes digitales stockés sur son badge OLAF, qui est une interface de contact utilisée par le système d'authentification informatique CBIS.

Enregistrement

L'enregistrement d'un utilisateur comporte deux procédures indépendantes:

a) le certificat numérique de la carte est enregistré dans le système de contrôle d'accès et est associé à une personne dans la base de données;

[1] Avis rendu le 7 avril 2008 à la suite d'une notification en vue d'un contrôle préalable concernant un système de contrôle d'accès et d'identité (dossier 2007-635), disponible sur le site web du CEPD.

b) les empreintes de trois doigts de la personne concernée sont numérisées par le système, qui en calcule un modèle numérique, 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.

C'est pourquoi les mêmes procédures d'enregistrement sont utilisées pour recueillir les empreintes digitales utilisées pour les contrôles d'accès physiques et informatiques. Toutefois, les modèles sont stockés dans deux puces différentes.

Spécificités techniques

La technologie utilisée repose sur Precise 250 MC, dont l'OLAF a précisé les spécificités au CEPD. Il s'agit d'un système combinant un lecteur d'empreintes digitales et un lecteur de carte à puce, qui stocke et fait correspondre l'information "empreinte digitale" dans l'environnement sécurisé de la carte même, ce qui élimine la nécessité de traiter des informations sensibles dans des ordinateurs personnels et des bases de données (système "match-on-card").

Les cartes contiennent un certificat numérique et trois modèles d'empreintes digitales permettant une authentification biométrique par "match-on-card". S'il y a trois modèles d'empreintes digitales, c'est pour réduire le risque de rejet.

Par modèle biométrique, on entend les données qui représentent l'empreinte enregistrée. Il comprend 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'enregistrement 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.

Le lecteur biométrique numérise l'empreinte digitale d'une personne et l'envoie à la puce à contact, qui vérifie sa concordance avec une des empreintes stockées. Si le résultat est positif, la puce à contact transmet le certificat numérique correspondant 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.

Sur la base des informations qu'il a reçues, le CEPD constate que le taux de faux rejets utilisé dans toutes les puces à contact n'est pas fixé de manière précise, mais est "*estimé à 1 %*".

En outre, il est possible de faire dix essais par doigt enregistré avant que le système ne bloque la carte.

Le serveur de la base de données centrale est l'interface administrative avec le système. Il conserve les informations sur les utilisateurs et leurs droits d'accès. Il garde aussi la trace de toutes les tentatives d'accès, que celui-ci soit accordé ou refusé.

Base juridique
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; article 8, article 11, paragraphe 1, et article 12, paragraphe 3;
- la décision 1999/352/CE de la Commission: considérants 4 et 5; 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; et
- la politique de la Commission en matière de sécurité des systèmes d'information.

Responsable du traitement
Le traitement des données relève essentiellement de la responsabilité de l'OLAF, en particulier de celle des Services informatiques, qui s'occupent de l'ensemble des systèmes informatiques.

Personnes concernées
Selon la notification, les personnes concernées sont les membres du personnel travaillant dans les locaux de l'OLAF et ayant besoin d'accéder à l'environnement informatique sécurisé CBIS.

Catégories de données concernées
Les catégories de données concernées sont les suivantes:

- données personnelles d'identification: nom,
- données organisationnelles d'identification: numéro personnel, direction, unité, division;
- numéro de la carte;
- informations relatives à la procédure d'habilitation;
- modèles d'empreintes digitales;
- droits d'accès à l'application: CBIS;
- profil d'accès physique (famille);
- certificat numérique.

Plus précisément, les données ci-après sont journalisées par le système de contrôle d'accès chaque fois qu'un badge est présenté à un lecteur de carte: date, heure, nom, autorisation ou refus de l'accès, nom du groupe d'accès, et numéro et description du lecteur de cartes.

Destinataires des données
Selon la notification, les destinataires CBIS sont les membres du personnel de l'OLAF responsables du contrôle d'accès CBIS. Plus précisément, la déclaration de confidentialité transmise au CEPD indique que: "*le personnel des ressources humaines et de la sécurité de l'OLAF a accès aux informations se trouvant dans le SGIA. Le personnel des services informatiques et de soutien des applications de l'OLAF a accès aux parties des informations dont il a besoin pour pouvoir prester les services qu'ils vous fournissent*". Il n'y a pas de destinataires en dehors de l'OLAF.

Traitement automatisé/manuel
Automatisé: l'identité des utilisateurs et les informations utiles pour le contrôle d'accès sont transmises au SGIA à partir de la base de données du système de gestion des ressources humaines de la Commission (COMREF). Les données nécessaires sont automatiquement exportées chaque nuit du COMREF vers le SGIA du CBIS.

Le SGIA contrôle l'accès aux applications du CBIS. Les actes de sécurité générés par les systèmes du CBIS sont transmis au SGIA, qui numérise ces informations de manière à en permettre le contrôle.

Manuel: le Service des ressources humaines de l'OLAF peut lancer un workflow qui modifie les droits d'accès dans l'environnement CBIS. Les services de l'OLAF participant à la gestion des systèmes et applications CBIS doivent approuver ou refuser un changement avant sa mise en œuvre.

Information des personnes concernées
Selon la notification, une déclaration de confidentialité sera disponible sur l'Intranet de l'OLAF.

La déclaration générale de confidentialité comprend les éléments suivants: une explication du système de contrôle d'accès de l'OLAF, la liste des informations à caractère personnel collectées, ainsi que la finalité pour 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) nº45/2001, 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 à caractère personnel seront effacées du SGIA au moment où une personne quitte l'OLAF, sauf s'il s'agit d'un utilisateur du système de gestion des dossiers, auquel cas la période de conservation sera de 20 ans. Les personnes qui ont eu accès au système de gestion des dossiers perdront leur accès au SGIA et toutes leurs informations personnelles (sauf le nom et le service de l'utilisateur) seront effacées. Quant à la carte, sa puce sera effacée, et elle sera réutilisée par un autre utilisateur ou détruite.

Les actes de contrôle d'accès journalisé générés dans l'environnement CBIS sont conservés pendant un an dans le système de gestion des données et actes de sécurité du CBIS, qui fait partie de l'infrastructure du SGIA.

Comme pour le système de contrôle d'accès électronique, la période de conservation pour le contrôle d'accès journalisé 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.

Stockage
Les données sont enregistrées dans une base de données sur un disque dur avec back-up. Le stockage des modèles d'empreintes digitales se fait uniquement dans les badges d'identification personnels de l'OLAF.

Mesures de sécurité
La notification comporte une section relative aux mesures de sécurité. Toutefois, les informations données ne portent pas spécifiquement sur le SGIA; en réalité, le SGIA est protégé par les mêmes normes de sécurité que celles appliquées au CBIS de l'OLAF, qui ont fait l'objet d'une analyse horizontale de la part du CEPD.

En ce qui concerne les aspects touchant à la sécurité, la politique et les procédures de la Commission en matière de sécurité s'appliquent à l'infrastructure informatique de l'OLAF. La décision nº 3602 de la Commission du 17 août 2006 définit les mesures de sécurité en vigueur. Son annexe I énonce les exigences en matière de sécurité pour les systèmes informatiques de la CE, son annexe II décrit les responsabilités des divers acteurs, et son annexe III recense les règles applicables aux utilisateurs.

Pour le fonctionnement des autres systèmes informatiques sous sa responsabilité, l'OLAF utilise actuellement les réseaux TI centraux de la CE (Centre Telecom + SNET) et les services de sécurité EC corporate Users provisioning/authentication (par exemple, NET1 MS Active Directory, LDAP et ECAS) proposés au niveau central par la division DIGIT pour toutes les DG et services de la Commission.

Par ailleurs, la déclaration de confidentialité comprend un chapitre consacré à la sécurité, où l'on peut lire ceci: "*Afin de protéger vos données à caractère personnel, un certain nombre de mesures techniques et organisationnelles ont été mises en place* (…)".

(…)

2.2 Aspects juridiques

2.2.1 Contrôle préalable

Le présent avis relatif à un contrôle préalable porte sur le traitement d'informations à caractère personnel auquel procède l'OLAF, en particulier l'Unité des Services informatiques, pour assurer que seules les personnes autorisées aient accès aux systèmes informatiques essentiels de l'OLAF et permettre d'enquêter sur les incidents de sécurité. Comme cela a déjà été expliqué ci-dessus, la notification du contrôle d'accès au CBIS de l'OLAF doit être rattachée à l'avis relatif à un contrôle préalable antérieur que le CEPD a adopté à propos du système de contrôle d'accès physique de l'OLAF[2].

Le règlement (CE) n°45/2001[3] 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*". Pour les raisons exposées ci-dessous, tous les éléments justifiant l'application du règlement sont réunis en l'espèce.

Premièrement, des *données à caractère personnel* telles que définies à l'article 2, point a), du règlement 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, ainsi que de traitements manuels. En fait, 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 des Services informatiques établit les modèles d'empreintes. Par ailleurs, l'Unité des Ressources humaines ou l'Unité des Services informatiques de l'OLAF peuvent effectuer un traitement manuel dans le cadre de la gestion du CBIS. Enfin, le traitement est effectué par un *organe communautaire*, à savoir l'Office européen de lutte antifraude, dans le cadre du droit communautaire (article 3, paragraphe 1, du règlement). Par conséquent, tous les éléments justifiant l'application du règlement sont réunis en l'espèce.

L'article27, paragraphe1, du règlement soumet au contrôle préalable du CEPD "*les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées 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. Cette opinion 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 relève également les possibilités d'interconnexions et l'état actuel des outils technologiques, qui peuvent avoir des conséquences inattendues 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.

---

2 Voir la note 2.

3 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 (ci-après dénommé "le règlement").

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 jusqu'à ce que les recommandations accompagnant l'avis aient été prises en compte et que le CEPD ait été averti de leur mise en œuvre (article 27, paragraphe 4, troisième alinéa), sauf si un calendrier est prévu (voir la conclusion).

La notification a été reçue le 11 avril 2008. Conformément à l'article 27, paragraphe 4, du règlement, le délai de deux mois dans lequel le CEPD doit rendre son avis a été suspendu pendant 8 jours au total afin d'obtenir des informations complémentaires, plus 10 jours pour permettre la présentation d'observations sur le projet d'avis. Le présent avis doit donc être adopté au plus tard le 30 juin 2008.

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.

Parmi les différents motifs énumérés audit article 5, le traitement notifié en vue d'un contrôle préalable relève du 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, il convient de répondre aux trois questions qui suivent. 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; article 8, article 11, paragraphe 1, et article 12, paragraphe 3;
- la décision 1999/352/CE de la Commission: considérants 4 et 5; 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.

* Le traitement est effectué **dans l'exercice légitime de l'autorité publique**. Le CEPD constate que la Commission met le traitement en œuvre 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, 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 des Communautés[4].

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 estimer nécessaire d'adopter des mesures de sécurité spécifiques, y compris en mettant en place des systèmes de contrôle d'accès stricts à ses systèmes informatiques, et de permettre des enquêtes sur des incidents de sécurité à 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 Traitement 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.

2.2.4 Qualité des données

Adéquation, pertinence et proportionnalité. Selon l'article 4, paragraphe 1, point c), du règlement, les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement. Ce principe est appelé "principe de la qualité des données". En vérifiant si le traitement dont il est question ici, à savoir essentiellement le traitement de données biométriques, respecte ce principe, le CEPD a fait les constatations qui suivent.

Ainsi qu'il est indiqué dans la notification, chaque membre du personnel de l'OLAF ayant besoin d'accéder à l'environnement sécurisé du CBIS est considéré comme une personne concernée.

En outre, la notification précise que le système en question est un service d'annuaire pour les systèmes et applications informatiques relatifs à l'environnement TI sécurisé de l'OLAF. Les actes de contrôle d'accès journalisés générés dans l'environnement du CBIS sont conservés dans le système de gestion des données et actes de sécurité du CBIS, qui fait partie de l'infrastructure du SGIA.

L'authentification dans le CBIS repose sur des certificats et des empreintes digitales numériques. Les certificats sont stockés sur les badges personnels OLAF des utilisateurs (cartes à puces) et protégés par un système de "match-on-card" biométrique. Pour chaque utilisateur, trois modèles d'empreintes digitales devront être stockés sur son badge OLAF.

En conséquence, chaque membre du personnel de l'OLAF ayant besoin d'accéder à l'environnement TI sécurisé du CBIS doit porter un badge OLAF afin d'être autorisé à accéder audit environnement. Pour le CEPD, il est entendu que seules les personnes qui ont besoin de cet accès doivent enregistrer leurs empreintes digitales dans la puce à contact.

Par ailleurs, l'OLAF a joint à la notification des documents étayant les raisons pour lesquelles des éléments biométriques sont utilisés dans ses systèmes de sécurité spécifiques. Selon la politique de l'OLAF en matière de sécurité des informations, élaborée afin de mettre en œuvre les exigences de sécurité applicables au sein de l'OLAF, le principe du besoin d'en connaître doit être strictement appliqué, ce qui implique une identification claire, par exemple une authentification rigoureuse, 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 ce principe du besoin d'en connaître comme

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

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.

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.

Loyauté et licéité. L'article 4, paragraphe 1, point a), du règlement exige que les données soient traitées loyalement et licitement. La question de la licéité a été analysée ci-dessus (point 2.2.2). Celle de la loyauté est étroitement liée à l'objet du point 2.2.9, à savoir les informations fournies aux personnes concernées.

Exactitude. Selon l'article 4, paragraphe 1, point d), du règlement, 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 d'enregistrement ou 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. Le CEPD a analysé, dans son avis relatif au contrôle d'accès physique de l'OLAF, les règles à suivre lors de la mise en œuvre d'un système biométrique. Nous décrivons ci-après ces caractéristiques essentielles et analysons la mesure dans laquelle elles ont été prises en compte dans le système TI biométrique de contrôle d'accès examiné.

- Premièrement, toute phase d'enregistrement 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 et l'analyse du système de contrôle d'accès physique, l'OLAF n'a pas prévu de taux d'enregistrements impossibles, puisqu'il part du principe que l'ensemble du personnel pourra être enregistré.

  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 place une procédure de secours en ce sens que trois modèles d'empreintes digitales, et non un seul, sont relevés durant la phase d'enregistrement. Au cours du processus d'authentification biométrique, l'utilisateur placera l'un des trois doigts qu'il a choisis au moment de l'enregistrement.

  Même si cette solution diminue le risque d'enregistrements impossibles, il reste possible que certaines personnes ne puissent être enregistrées dans le système de reconnaissance des empreintes digitales. Dans un tel cas, la personne concernée serait victime d'une discrimination, sans parler de la possibilité qu'elle soit empêchée de remplir ses obligations contractuelles. C'est pourquoi le CEPD suggère que l'OLAF mette en œuvre une solution de remplacement réaliste pour les cas d'enregistrements impossibles permanents, qui devra tenir compte du niveau de risque de sécurité du CBIS et protéger les droits des personnes concernées.

- Deuxièmement, des mesures semblables doivent être prévues pour les personnes qui ont été dûment enregistrées, mais qui ne peuvent pas être identifiées (ce que l'on appelle

[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 (CE) du Conseil 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).

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 un environnement TI sécurisé, 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 l'environnement TI sécurisé du CBIS de l'OLAF).

En ce qui concerne le système de contrôle d'accès de l'OLAF, le taux de faux rejets pour l'ensemble du bâtiment est, selon les informations transmises au CEPD, "*estimé à 1%*", ce qui correspond au niveau de sécurité auquel devrait satisfaire le SGIA de l'OLAF. Le CEPD a quelques observations à formuler à cet égard:

1. Le CEPD s'étonne de constater que le taux de faux rejets ne soit pas défini de manière précise mais "estimé". Ce taux se fonde généralement sur la politique en matière de sécurité de l'opérateur, qui déterminera un seuil en dessous duquel une empreinte digitale sera toujours rejetée afin d'atténuer le risque qu'un imposteur ait accès aux données.

2 Le CEPD s'étonne aussi de voir que l'OLAF a décidé de mettre en œuvre un taux de faux rejets qui est le même que celui utilisé pour le contrôle d'accès physique à ses bâtiments. En fait, dans le cas du CBIS, l'accès est directement accordé aux données stockées dans des systèmes informatiques, et l'on pourrait s'attendre à ce que le niveau de sécurité soit plus élevé. C'est pourquoi le CEPD suggère que l'OLAF fixe pour le CBIS un taux de faux rejets précis, qui reflètera la politique qu'il a adoptée en matière de sécurité.

3. De plus, le CEPD suggère que, en cas de faux rejet, l'OLAF mette au point une procédure qui permettrait de traiter le problème d'une manière qui ne soit pas trop contraignante pour les personnes concernées. En d'autres termes, la procédure de remplacement devrait fournir des solutions suffisamment simples au problème de non identification et de rejet. Le CEPD souhaite à cet égard que l'OLAF renouvelle à intervalles réguliers le processus d'enregistrement de manière à maintenir une qualité élevée des données. Ce renouvellement est justifié, notamment, par le fait que les éléments biométriques, en particulier les empreintes digitales, peuvent évoluer au cours de la vie d'une personne concernée et que l'état de la peau du doigt concerné peut se modifier avec le temps, ainsi que par la qualité du modèle d'empreinte digitale enregistré. La périodicité du renouvellement pourrait être déterminée et mise en œuvre après une année d'exploitation du nouveau système, sur la base de l'expérience ainsi acquise par l'OLAF. Ce point souligne aussi combien il importe que l'OLAF fixe un taux de faux rejets précis.

- Enfin, le système de contrôle d'accès informatique de l'OLAF repose sur des modèles d'empreintes digitales stockés dans des cartes, associés à l'utilisation de lecteurs. Contrairement au contrôle d'accès physique, il utilise un dispositif d'authentification fondé sur une concordance (match-on-card) à 100 %. 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 bases de données donne souvent lieu[6].

2.2.5 Conservation des données

L'article 4, paragraphe 1, point e), du règlement pose le principe selon lequel les données à caractère personnel doivent être "*conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des*

[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), disponible sur le site web du CEPD.

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 […], 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."

Selon la notification, les données à caractère personnel seront effacées du SGIA au moment où une personne quitte l'OLAF, sauf s'il s'agit d'un utilisateur du système de gestion des dossiers, auquel cas la période de conservation sera de 20 ans. Les personnes qui ont eu accès au système de gestion des dossiers perdront leur accès au SGIA et toutes leurs informations personnelles (sauf le nom et le service de l'utilisateur) seront effacées. Quant à la carte, sa puce sera effacée, et elle sera réutilisée par un autre utilisateur ou détruite.

Par ailleurs, les informations journalisées relatives au contrôle d'accès seront conservées pendant 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 dans son cas, compte tenu du caractère sensible de ses activités opérationnelles.

Le CEPD estime que la rapidité est un élément essentiel pour la détection des incidents de sécurité: 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 actes posés pendant les incidents de sécurité et que, dans le cas de l'OLAF, une période très courte pourrait créer des difficultés pratiques. Il part du principe que l'OLAF a mis en place une procédure d'identification des incidents et de réaction à ceux-ci afin qu'ils soient détectés et signalés dès que possible (et si ce n'est pas le cas, qu'il devrait la mettre au point). On peut supposer que l'OLAF s'efforce de détecter les incidents immédiatement après qu'ils ont eu lieu et, en tout état de cause, au plus tard quelques mois après. Compte tenu de ce qui précède, le CEPD est d'avis qu'une période de conservation d'un an est trop longue et il invite l'OLAF à réexaminer la période qu'il a fixée en réévaluant la nécessité de la raccourcir sur la base des 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. Il est dès lors 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.

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. Il tient néanmoins à souligner que, en cas d'utilisation de ces données au-delà de la période de conservation, il est nécessaire de les rendre anonymes (article 4, paragraphe 1, point e), du règlement).

2.2.6 Transfert des données

D'après la notification et la déclaration de confidentialité, le personnel du service des ressources humaines et du service de sécurité de l'OLAF ont accès aux informations figurant dans le SGIA.

Le CEPD rappelle que l'article 7 du règlement 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, i) que le destinataire a les compétences requises et ii) que le transfert est nécessaire. Le CEPD estime que tel est le cas pour signaler des incidents de sécurité. Toutefois, il conviendra d'apprécier au cas par cas si un transfert donné satisfait à ces exigences. Outre ce qui précède, et conformément à l'article 7 du règlement, il convient d'informer le destinataire que les données à caractère personnel ne peuvent être traitées que pour les finalités pour lesquelles elles ont été transmises.

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

L'article 10, paragraphe 6, du règlement 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 relatif à un contrôle préalable[7], comment on peut qualifier le numéro d'une puce RFID intégrée dans une carte: le numéro d'identification associé à la puce RFID est une donnée à caractère personnel rentrant dans le champ d'application du règlement. 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, et il y a dès lors lieu de respecter les principes applicables en matière de protection des données. Le recours au numéro personnel est nécessaire parce que le numéro d'identification de la carte est communiqué au système de contrôle d'accès. 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 étant donné que ce numéro est utilisé pour identifier la personne dans le système et qu'il contribue dès lors à garantir l'exactitude des données.

2.2.8 Droit d'accès et de rectification

Selon l'article 13 du règlement, la personne concernée a le droit d'obtenir du responsable du traitement, sans contrainte, à tout moment dans un délai de trois mois à partir de la réception de la demande d'information et gratuitement, 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 confère à la personne concernée le droit de rectifier les données inexactes ou incomplètes.

La notification 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 et à la déclaration de confidentialité complémentaire fournie 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'exercice 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 l'environnement TI sécurisé du CBIS.

Le CEPD note que, selon la notification, l'article 20 du règlement 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 sont remplies.

---

[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" (dossier2007-218).

2.2.9 Information de la personne concernée

Les articles 11 et 12 du règlement énumèrent les informations à fournir à la personne concernée: ils 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. En l'espèce, une partie des données est collectée directement auprès de la personne concernée et une autre partie auprès de tiers.

Les personnes concernées sont informées au moyen d'une "*déclaration de confidentialité concernant le système de gestion de l'identité et de l'accès de l'OLAF*". Un projet de cette déclaration de confidentialité a été communiqué au CEPD pour montrer que ces articles sont respectés.

Le CEPD a également examiné le contenu des informations contenues dans la déclaration de confidentialité pour vérifier s'il satisfait aux exigences énoncées aux articles 11 et 12 du règlement. Ces informations ont trait aux finalités du traitement et à la manière dont le traitement est effectué, aux conditions d'exercice du droit d'accès et de rectification, aux délais de conservation des données et à la possibilité de saisir le CEPD. Le CEPD estime que la déclaration de confidentialité contient la plupart des informations requises en vertu des articles 11 et12 du règlement. Néanmoins, il est d'avis que quelques modifications permettraient de garantir le plein respect de ces articles, en particulier:

- mentionner le caractère obligatoire ou facultatif des réponses aux questions ainsi que les conséquences éventuelles d'un défaut de réponse (par exemple, les 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;
- mentionner que, si nécessaire, les informations peuvent être transmises aux fins d'une enquête administrative.

En outre, la déclaration de confidentialité est en principe fournie aux personnes qui sont soumises à une procédure d'enregistrement afin de pouvoir accéder au système informatique CBIS. Dans un autre avis relatif à 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*"). Il 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

Selon l'article 22 du règlement, le responsable du traitement doit 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.

Le CEPD fait observer que l'infrastructure TI spécifique de l'OLAF a fait l'objet d'un examen horizontal de sa part dans le cadre d'une autre procédure. Il n'y a pas lieu de refaire cet examen dans le cadre du présent avis.

(…)

[8] Voir l'avis sur le contrôle d'accès à la Banque centrale européenne (dossier2007-501).

3. Conclusion

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

A) *avant* de mettre en œuvre le traitement envisagé:

- veiller à ce que seules les personnes qui ont besoin d'accéder à l'environnement TI sécurisé du CBIS doivent enregistrer leurs empreintes digitales dans la puce à contact;
- définir un taux de faux rejets précis correspondant au niveau de sécurité spécifique du CBIS;
- modifier la déclaration de confidentialité en suivant la recommandation figurant dans le présent avis et veiller à ce qu'une copie en soit remise aux personnes ou soit mise à leur disposition d'une manière qui leur permette de la consulter;

B) *après* le démarrage du traitement:

- mettre au point, pour les cas d'impossibilité permanente d'enregistrement, une solution de remplacement réaliste qui tienne compte de l'impossibilité de relever les empreintes digitales d'un membre du personnel lors de la phase d'enregistrement;
- après une année d'exploitation du système, envisager un renouvellement à intervalles réguliers de l'enregistrement des membres du personnel de l'OLAF ou mettre au point des mesures de remplacement permettant de faire face aux faux rejets;
- réexaminer la durée de la période de conservation des données à l'issue de la première année d'exploitation du nouveau système;
- veiller à ce que, si des transferts de données ont lieu à l'avenir, des avis soient envoyés aux institutions communautaires qui reçoivent des données traitées dans le contexte du système de contrôle d'accès, pour les informer que les données à caractère personnel ne peuvent être traitées que pour les finalités pour lesquelles elles ont été transmises.

Fait à Bruxelles, le 30 juin 2008.

(Signé)

Joaquín BAYO DELGADO
Contrôleur adjoint de la protection des données