LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

JOAQUIN BAYO DELGADO
CONTRÔLEUR ADJOINT

M. Philippe RENAUDIERE
Délégué à la protection des données
Commission européenne
BRU-BERL-08/330
B-1049 Bruxelles

Bruxelles, le 31 octobre 2006
JBD/ab D(2006)1155 **C2006-0298**

Objet : "PROCESSUS D'AUDIT INTERNE" à la DG IAS (Commission)

Cher Monsieur,

À la suite de l'examen de la notification transmise en vue d'un contrôle préalable et des informations complémentaires reçues, nous avons conclu que le "processus d'audit interne" à la DG IAS de la Commission européenne (dossier 2006-298) n'est pas soumis au contrôle préalable du contrôleur européen de la protection des données (CEPD).

Le dossier a été soumis en vue d'un contrôle préalable sur la base de l'article 27, paragraphe 2, points b) et a), du règlement.

1) Enregistrement des heures du personnel de l'auditeur interne

Ce traitement a été soumis sur la base de l'article 27, paragraphe 2, point b), du règlement. Les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur compétence, leur rendement ou leur comportement, entrent dans le champ d'application de cet article.

Les informations disponibles nous amènent à conclure que le système d'enregistrement des heures ne vise pas à évaluer des aspects de la personnalité de chacun des membres du personnel, car a) les résultats du relevé des heures ne seront pas pris en compte dans le *processus d'évaluation* du personnel de la Commission; b) les données du système d'enregistrement des heures sont *consolidées* pour comparer le nombre total d'heures indiqué par les membres du personnel avec les heures prévues, ce qui signifie que le format consolidé n'identifie pas chacun des utilisateurs[1]; et c) l'IAS n'utilise pas les données pour déterminer le *nombre d'heures consacrées par chaque membre du personnel* à des activités d'audit ou non ou les heures qu'il a passées dans le cadre d'un audit. Par ailleurs, le formulaire de notification indique en particulier que, pour le moment, les relevés ne servent pas à évaluer chacun des membres du personnel: "*Le personnel a été informé que les données ne seront communiquées sous aucune forme susceptible d'être utilisée à des fins d'évaluation des performances sans l'accord express du CEPD.*".

[1] Note du 25 janvier 2005 sur le "Contrôle du temps consacré aux missions d'audit". IAS/FM D(2004).

Comme il n'est pas prévu d'utiliser les données du système d'enregistrement des heures à des fins d'évaluation, le traitement ne présente aucun risque particulier à cet égard et ne doit pas faire l'objet d'un contrôle préalable du CEPD. Mais si le système d'enregistrement des heures devait servir à évaluer chacun des membres du personnel d'audit, cela entrerait probablement dans le champ d'application de l'article 27, paragraphe 2, point b), du règlement.

2) Fraude avérée ou suspicion de fraude au cours d'un audit

Le processus d'audit interne a été soumis en vertu de l'article 27, paragraphe 2, point a), du règlement. Les traitements de données relatives à des suspicions, infractions, condamnations pénales ou mesures de sûreté sont susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées.

La note du délégué à la protection des données faisant fonction jointe au formulaire de notification d'un contrôle préalable mentionne en particulier que "*si, au cours du processus d'audit, l'IAS dispose d'éléments attestant ou laissant soupçonner une fraude, il fait intervenir l'OLAF ou lui transmet le dossier, car le traitement des fraudes ne le concerne plus*".

Le processus d'audit interne vise principalement à maîtriser les risques relatifs à la qualité des systèmes de gestion et de contrôle et à émettre des recommandations pour améliorer la situation, ainsi qu'à promouvoir la bonne gestion financière. Il est possible que l'audit interne fournisse des éléments attestant ou laissant soupçonner une infraction pénale ou des irrégularités pouvant donner lieu à d'autres procédures, par exemple des enquêtes internes de l'Office européen de lutte antifraude (OLAF). Il s'agit donc de déterminer si un risque particulier se pose. Le processus d'audit interne n'implique pas un tel risque, car les informations relatives à des suspicions d'infractions pénales sont immédiatement transférées à l'OLAF. L'enquête interne effectuée par l'OLAF présente des risques particuliers au regard des droits et libertés des personnes concernées; elle entre donc dans le champ d'application de l'article 27, paragraphe 2, point a), du règlement. Le CEPD a déjà procédé à un contrôle préalable des enquêtes internes de l'OLAF (dossier 2005-418)[2].

En conséquence, le processus d'audit interne même n'est pas soumis à un contrôle préalable en vertu de l'article 27, paragraphe 2, point a).

3) L'audit interne en tant qu'instrument d'évaluation des personnes

Bien que la notification reçue en vue d'un contrôle préalable ne mentionne pas l'article 27, paragraphe 2, point b), comme base pour un contrôle préalable du processus d'audit même, le CEPD a examiné cette possibilité.

L'auditeur interne conseille son institution dans la maîtrise des risques, en formulant des avis indépendants portant sur la qualité des systèmes de gestion et de contrôle et en émettant des recommandations pour améliorer les conditions d'exécution des opérations et promouvoir la bonne gestion financière. Il est chargé notamment a) d'apprécier l'adéquation et l'efficacité des systèmes de gestion internes ainsi que la performance des services dans la réalisation des politiques, des programmes et des actions en relation avec les risques qui y sont associés; et b) d'apprécier l'adéquation et la qualité des systèmes de contrôle et d'audit internes applicables à toute opération d'exécution du budget (article 86, paragraphe 1, du règlement financier[3]).

Comme l'audit interne vise principalement à *évaluer les systèmes de gestion et de contrôle internes et non certaines personnes (ni les responsables ni les membres du personnel)*, le dossier n'entre pas dans le champ d'application de l'article 27, paragraphe 2, point b), du règlement.

---

2 Avis du 23 juin 2006 sur la notification d'un contrôle préalable à propos des enquêtes internes effectuées par l'OLAF (Dossier 2005-418).

3 Règlement (CE, Euratom) n° 1605/2002 du Conseil du 25 juin 2002 portant règlement financier applicable au budget général des Communautés européennes. JO L 248 du 16.9.2002, p. 1-48.

Il convient de noter que les résultats obtenus au cours d'un audit interne ou le résultat définitif d'un audit peuvent avoir d'autres conséquences pour les personnes concernées. Comme il est indiqué plus haut, des enquêtes peuvent être effectuées par la suite, et il se peut également que l'Office d'investigation et de discipline (IDOC) mène une enquête administrative et des procédures disciplinaires internes, qui évaluent clairement le comportement desdites personnes. Un risque particulier se pose sur le plan des procédures d'évaluation de certaines personnes et non au niveau du processus d'audit interne. Les enquêtes administratives et les procédures disciplinaires internes de l'IDOC ont déjà fait l'objet d'un contrôle préalable du CEPD (dossier 2004-187)[4].

Par ailleurs, la section 6 de la notification reçue en vue d'un contrôle préalable mentionne ce qui suit: "*Le cas échéant, des données seront collectées en ce qui concerne les activités externes de la personne concernée si cela a un rapport avec ses activités internes. Dans ce contexte, davantage de données à caractère personnel sur les activités externes de la personne concernée peuvent être collectées.*". Il convient de noter que, si la collecte de données relatives aux activités externes d'une personne concernée comporte un élément d'évaluation du comportement de cette personne, cela ne justifie pas un contrôle préalable, car ce n'est pas la finalité première de l'audit même; il s'agit d'une simple éventualité qui ne se produit pas souvent.

Compte tenu des considérations qui précèdent, nous avons décidé de clore le dossier. Toutefois, si vous estimez qu'il existe d'autres facteurs justifiant un contrôle préalable du processus d'audit interne et du système d'enregistrement des heures, il va de soi que nous sommes prêts à revoir notre position.

Nonobstant ces considérations, fondées sur la notification et les informations reçues en réponse à nos demandes, nous avons examiné certains aspects des opérations de traitement et souhaitons appeler l'attention sur les points ci-après.

A) L'audit interne est une procédure générale et non une mission d'enquête particulière

Le contrôleur a joint au formulaire de notification un projet de note d'information sur le "Traitement des données à caractère personnel au cours des audits de l'IAS". Ce projet de note vise à fournir à l'audité (Directeur général) des informations sur la protection des données dans le cadre d'un audit, qui peuvent donc être communiquées à l'ensemble de son personnel au début d'un audit. Ce projet de note mentionne en particulier ce qui suit:

> "*L'article 86 du règlement financier charge l'auditeur interne de formuler des avis sur la mise en œuvre des systèmes de gestion et de contrôle au sein des institutions. Son paragraphe 2 prévoit que l'auditeur interne dispose d'un accès complet et illimité à toute information requise pour l'exercice de ses tâches.*
>
> *Dans le cadre de l'audit mené, l'auditeur peut collecter des données à caractère personnel au sujet du personnel de l'audité ou des sous-traitants avec lesquels l'audité est en relation. Il s'agirait principalement de comptes rendus de réunions, d'opérations figurant dans les systèmes informatiques et d'instructions opérationnelles données par l'audité ou au nom de celui-ci. Ces informations sont couvertes par le règlement (CE) n° 45/2001 du Conseil. L'exception spécifiée à l'article 2, point g), de ce règlement confirme l'accès complet et illimité visé au paragraphe précédent.".*

L'article 2, point g), du règlement stipule que "les autorités qui sont susceptibles de recevoir communication de données dans le cadre d'une mission d'enquête particulière ne sont pas considérées comme des destinataires".

Comme il est indiqué plus haut, le processus d'audit interne revêt un caractère général. Il ne peut être considéré comme une mission d'enquête particulière, car il ne vise pas à enquêter sur certaines personnes ou sur certains comportements; il a plutôt pour objet d'examiner des systèmes et les risques qui peuvent y être associés à un niveau plus général. Dès lors, comme l'article 2, point g),

[4] Avis du 20 avril 2005 sur la notification d'un contrôle préalable reçu à propos du dossier "Enquêtes administratives et procédures disciplinaires internes de la Commission européenne" (Dossier 2004-187).

n'est pas applicable aux activités d'audit proprement dites, l'article 7 (transferts de données) ainsi que les articles 11 et 12 (droit d'information) s'appliquent dans ce cas; il s'agit des seules dispositions concernées par l'exception visée à l'article 2, point g).

Néanmoins, en ce qui concerne l'article 7, le CEPD estime que, compte tenu de la nature des compétences confiées aux institutions et organes de contrôle, il convient d'interpréter le deuxième paragraphe de cet article dans ce contexte et que c'est à l'autorité de contrôle requérante qu'il appartient d'évaluer la nécessité de recevoir les données demandées.

B) Application des limitations visées à l'article 20 du règlement

Le même projet de note mentionne ce qui suit:

> *"Pour que le processus d'audit puisse se dérouler correctement, cet accès illimité aux données bénéficie de l'exception visée à l'article 20, paragraphe 1, point e), du règlement (CE) n° 45/2001, qui limite l'application de l'article 4, paragraphe 1, sur la qualité des données, de l'article 11 et de l'article 12, paragraphe 1, sur les informations à fournir à la personne concernée et des articles 13 à 17 sur les droits de la personne concernée, tout en exigeant de l'auditeur interne qu'il informe la personne concernée en vertu de l'article 20, paragraphe 3, du règlement."*. La section 8 de la notification reçue en vue d'un contrôle préalable mentionne en particulier ce qui suit: "*Le processus d'audit interne est couvert par l'article 20, paragraphe 1, point e), qui limite les droits de la personne concernée d'obtenir, de vérifier et de rectifier les données à caractère personnel détenues par l'auditeur interne. Dans les cas sensibles, il ne serait pas dans l'intérêt de l'institution d'informer la personne concernée spontanément, ou sur demande, de la nature exacte de toute donnée à caractère personnel collectée au cours d'un audit.*".

L'article 20, paragraphe 1, point e), permet de limiter ces droits "pour autant qu'une telle limitation constitue une mesure nécessaire pour… e) assurer une mission de contrôle… ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés aux points a) et b)". Ces deux derniers points autorisent une telle limitation pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales (point a)); ou pour sauvegarder un intérêt économique ou financier important… des Communautés européennes, y compris dans les domaines monétaire, budgétaire et fiscal (point b)).

L'article 20, paragraphe 3, dispose ce qui suit: *"Si une limitation prévue au paragraphe 1 est imposée, la personne concernée est informée conformément au droit communautaire des principales raisons qui motivent cette limitation et de son droit de saisir le contrôleur européen de la protection des données."*.

Les informations figurant dans la notification de contrôle préalable et dans le projet de note susmentionné semblent contradictoires en ce qui concerne la question de savoir si les limitations sont appliquées par le contrôleur d'une manière générale ou seulement dans les "cas sensibles". Il convient de souligner que la limitation visée à l'article 20, paragraphe 1, point e), s'applique uniquement dans les cas où elle constitue une "mesure nécessaire" pour sauvegarder un des intérêts énumérés dans cet article. Le "critère de nécessité" exige que les limitations soient appliquées au cas par cas et qu'elles soient justifiées. Cela signifie qu'une limitation ne peut être appliquée à chaque cas et à chaque situation prévue à l'article 20, paragraphe 1, du règlement, mais bien que la nécessité d'une limitation devrait être démontrée dans chaque cas et pour chaque article spécifique (article 4, paragraphe 1, article 11, article 12, paragraphe 1, articles 13 à 17 et article 37, paragraphe 1) du règlement dont il est prévu de limiter l'application.

Par ailleurs, comme le droit d'accès peut être exercé directement par la personne concernée ("accès direct") ou, dans certaines circonstances, par une autorité publique ("accès indirect", normalement exercé par une autorité chargée de la protection des données, le CEPD en l'occurrence), il convient de tenir compte de l'article 20, paragraphe 4, du règlement, qui prévoit ce qui suit: *"Si une limitation prévue au paragraphe 1 est invoquée pour refuser l'accès à la personne concernée, le contrôleur européen de la protection des données lui fait uniquement savoir, lorsqu'il examine la réclamation, si les données ont été traitées correctement et, dans la négative, si toutes les corrections nécessaires ont été apportées."*. L'accès indirect devra alors être garanti. Cette disposition jouera un rôle, par

exemple, dans les cas où la personne concernée a été informée de l'existence du traitement, ou en a connaissance, mais où son droit d'accès reste limité eu égard à l'article 20.[5]

C) Au cas où des données relatives au trafic seraient mises en mémoire aux fins d'audit, le traitement devrait se dérouler conformément aux lignes directrices figurant dans le document du CEPD sur le contrôle des communications électroniques (à diffuser sous peu).

D) Au cas où la section "Absence" du système d'enregistrement des heures traiterait certaines données relatives à la santé portant sur la maternité ou l'absence pour cause de maladie, le CEPD jugerait cela excessif pour les besoins du système en vertu de l'exigence de qualité des données visée à l'article 4, paragraphe 1, point c), du règlement. Une indication selon laquelle la personne était en "congé" (le fait que cela soit pour une raison de santé n'est pas pertinent) devrait suffire pour atteindre l'objectif visant à déterminer le temps consacré à des activités d'audit ou non.

Je vous saurais gré de bien vouloir transmettre ces considérations au contrôleur et nous tenir informés de la nécessaire mise en œuvre.

Nous vous remercions de votre coopération,

Cordialement,

Joaquín BAYO DELGADO
Contrôleur européen adjoint de la protection des données

[5] Pour la notion d'accès indirect, voir également le point 2.2.8 "Droit d'accès et de rectification" de l'avis du 23 juin 2006 sur la notification d'un contrôle préalable à propos des enquêtes internes effectuées par l'OLAF (Dossier 2005-418).