Avis concernant une notification relative à un contrôle préalable reçue du délégué à la protection des données de la Commission européenne à propos des enquêtes en matière de sécurité.

Bruxelles, le 2 octobre 2008 (Dossier 2007-736)

1. Procédure

Le 17 décembre 2007, le Contrôleur européen de la protection des données (CEPD) a reçu du délégué à la protection des données (DPD) de la Commission européenne une notification relative à un contrôle préalable à propos des enquêtes en matière de sécurité effectuées par le secteur "réquisitions administratives de la Direction générale ADMIN / Sécurité (secteur ADMIN/DS/RA).

Le 1 février 2008, le CEPD a demandé au DPD de la Commission européenne des informations complémentaires. Les réponses ont été reçues le 3 mars 2008. L'avis a été envoyé au DPD pour commentaires le 7 mars 2008. Les commentaires ont été reçus le 10 juillet 2008. La réponse du responsable du traitement a soulevé d'autres questions qui ont été envoyées au DPD de la Commission européenne le 11 juillet 2008 et dont la réponse a été reçue le 15 juillet 2008. Des questions supplémentaires ont été posées au DPD de la Commission européenne le 25 juillet 2008. Les réponses ont été reçues le 1er octobre 2008.

2. Faits

Le secteur ADMIN/DS/RA remplit trois fonctions principales dont les finalités sont les suivantes :

Les mesures contre les faits criminels ou délictueux en ce qui concerne les immeubles occupés par la Commission, les personnes qui y travaillent ou y ont accès à des titres divers, ainsi que les autres actes qui engendrent un préjudice pour l'Institution. Cela inclut la conservation et la préservation d'éléments objectifs de preuves, ainsi que diverses démarches de recherche aux fins de rassembler de tels éléments, d'effectuer des constatations techniques, et de recueillir la déclaration de victimes, de plaignants, de témoins et, le cas échéant, d'auteurs de faits, sans préjudice des dispositions impératives régissant l'action d'Office d'investigation et de discipline (IDOC) et de l'Office européen de lutte antifraude (OLAF).

- l'assistance technique à d'autres services de la Commission qui requièrent la Direction sécurité dans le cadre d'actions ponctuelles relevant de leur compétence. Il s'agit principalement de la Direction ADMIN/IDOC, de l'OLAF, des services social et médical ainsi que de la DG BUDG. Le secteur est aussi chargé, dans le strict respect des procédures internes, de rassembler, conserver et transmettre aux autorités judiciaires divers éléments de preuves et d'information requis par elles.

Adresse postale: rue Wiertz 60 - B-1047 Brussels
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

- L’exercice du devoir de sollicitude de l’Institution envers ses fonctionnaires et autres agents, principalement dans les cas revêtant une certaine urgence.

Ces activités se traduisent par divers actes et, le cas échéant, l’établissement d’un rapport circonstancié des faits, rapport transmis à l’ADMIN/IDOC, à l’OLAF ou éventuellement aux autorités de police ou judiciaires moyennant suivi des procédures internes en la matière.

2.1. Catégories de personnes concernées

Les catégories de personnes concernées par cette activité de traitement sont : tous les fonctionnaires, autres agents et contractuels en activité, anciens fonctionnaires, autres agents et contractuels, les prestataires de services, les contractants, les visiteurs, les personnes externes qui s'adressent spontanément à la Commission et à son personnel, notamment par courrier, courrier électronique, téléphone, télécopie..., ou qui sont victimes, témoins ou auteurs d'une infraction, d'un manquement ou d'un événement préjudiciable à l'Institution ou à son personnel, ou encore tout membre du personnel envers lequel la Commission se doit d'exercer son devoir de sollicitude.

2.2. Catégories de données

Les catégories de données traitées sont : noms, prénoms, éventuellement le lieu et la date de naissance, l'adresse, les coordonnées téléphoniques des personnes concernées, la nature du fait étudié, le lieu et le moment de sa survenance, les éléments probants découverts ainsi que le lien entre ces éléments et les personnes.

Le formulaire de notification, confirmé sur ce point explicitement par le DPD, précise que des catégories particulières de données (visées à l'article 10 paragraphe 1 du règlement) ne sont pas traitées dans le cadre des enquêtes menées par le secteur ADMIN/DS/RA. Toutefois, le traitement de telles données peut, dans des circonstances très exceptionnelles et particulières, avoir lieu en raison de la nature du dossier qui fait l'objet de l'enquête (par exemple, accès aux données relatives à la santé liées à des remboursements effectués par la Caisse maladie et accidents).

En toute état de cause, les données "*relatives aux infractions, aux condamnations pénales ou aux mesures de sureté*" (visées à l'article 10 paragraphe 5 du règlement) sont concernées par le présent traitement.

Le numéro personnel d'un fonctionnaire faisant l'objet d'une enquête figure dans le rapport final, pour que la personne concernée puisse être identifiée avec une absolue certitude et sans ambiguïté.

2.3. Collecte et formes de stockage de données

Chaque fait porté à la connaissance du secteur ADMIN/DS/RA est répertorié dans une **base de données informatique** selon toute une série de critères, tels que le fonctionnaire chargé du dossier, le moment et le lieu des faits, la nature des faits, les coordonnées du service ou de la personne requérante, celles de toutes les autres personnes intervenant, la nature du préjudice encouru et quelques précisions utiles sur le déroulement des événements. Chaque fait reçoit ainsi automatiquement un numéro de dossier.

Ceci a un double but : tout d’abord et vu le grand nombre de dossiers traités, permettre de répondre rapidement et efficacement à toute personne ou à tout service qui ont été en rapport avec le secteur au sujet d’un fait quelconque dans le passé et qui souhaitent apporter des précisions complémentaires, s’enquérir de la suite donnée ou assurer le suivi du dossier à un niveau ultérieur, d’extraire des données comparables (notamment concernant les moments, les lieux et la nature des préjudices) afin de pouvoir identifier le ou les auteurs des faits, de retrouver les objets composant

le préjudice ou d'avoir rapidement accès à des informations utiles permettant d'aider à la résolution rapide d'un cas ultérieur. Les statistiques annuelles sont établies sur la base de ces informations.

Chaque fait répertorié dans la base de données informatique fait l'objet de la constitution d'un **dossier physique** comportant tous documents utiles, tels que la requête initiale, les documents de travail et de procédure, les éléments de preuves, qu'ils soient matériels, photographiques ou documentaires, les comptes-rendus des déclarations recueillies et les rapports établis. Tous ces éléments sont classés sous le numéro de dossier attribué par la base de données informatique.

À la clôture d'une enquête, l'enquêteur chargé du dossier doit préparer un rapport final qui présente les résultats et les conclusions de l'enquête.

Il arrive que certains faits aient pour conséquence que l'accès des immeubles occupés par la Commission doit être interdit à une personne, soit d'urgence, comme par exemple si quelqu'un présente un risque immédiat pour la sécurité des personnes, des biens ou des informations de l'Institution, soit qu'une décision administrative formelle ait été prise en ce sens par l'instance habilitée, soit encore que le lien entre une firme contractuelle et son employé ait été rompu et que ladite personne détienne encore sa carte de service ou d'accès aux immeubles.

Le secteur ADMIN/DS/RA dresse ainsi la **liste des interdictions d'accès aux immeubles occupés par la Commission**. Elle se présente sous forme d'un tableau qui mentionne le nom, le prénom, la date de naissance, le statut, ainsi que le ou les immeubles auxquels l'accès de cette personne est interdit, ainsi que le numéro de dossier correspondant dans les bases de données informatique et physique. Aucun motif de l'application de la mesure n'est mentionné dans ce tableau.

Dans le cadre de ses recherches, le secteur ADMIN/DS/RA a **accès à diverses bases de données**, publiques ou internes à l'Institution où des informations utiles au traitement des dossiers peuvent être recueillies. Sont ainsi consultées les bases de données suivantes :

- Argus

Il s'agit d'une base de données établie et mise à jour par l'unité ADMIN/DS4 dans le cadre de l'établissement des titres et droits d'accès aux immeubles occupés par l'Institution. Cette base de données contient l'identité et la photographie des personnes détentrices d'un droit d'accès, mention de la nature et de la durée de ce droit, mention des caractéristiques de son ou de ses véhicules éventuels, ainsi que du service demandeur du droit.

- Sysper

Il s'agit d'une base de données exploitée par la DG ADMIN et reprenant diverses données relatives au personnel statutaire que la Commission emploie ou a employé.

- Sysper "pensionnés"

Il s'agit d'une base de données exploitée par le PMO et reprenant diverses données relatives au personnel statutaire pensionné.

- Enregistrement d'images vidéo par les caméras de surveillance

Il s'agit d'une série de bases de données exploitées par l'unité ADMIN/DS4 et contenant l'enregistrement récent des images filmées par les diverses caméras de surveillance installées dans et autour de certains immeubles occupés par la Commission[1].

- Congés et absences.

Les recherches effectuées par le Secteur ADMIN/DS/RA dans le cadre de ses compétences propres l'amènent parfois à consulter et/ou à utiliser les données relatives aux demandes de congés ou aux certificats d'incapacité de travail introduits auprès de la DG ADMIN par un membre du personnel, lorsque la disparition inquiétante de cette personne est signalée et qu'une vérification préalable à toute recherche dans l'intérêt de la personne doit être effectuée d'urgence. Ces vérifications portent exclusivement sur l'existence d'un tel document et non sur son contenu.

- Fichiers-tiers.

Une base de données relatives au fichier-tiers exploité par la DG BUDG et reprenant toute entité bénéficiaire de paiements de la part de l'Institution, ainsi que ses coordonnées bancaires. Cette base et utilisée notamment lorsqu'il s'avère nécessaire de communiquer en urgence aux autorités judiciaires les coordonnées bancaires d'une personne dont la disparition inquiétante est signalée.

- Recherches en matière informatique et téléphonique.

L'évolution des technologies est telle que de nombreuses infractions (menaces, tentatives d'escroquerie, diffamations et calomnies, fuites d'informations à caractère sensible…) sont commises, notamment de manière anonyme ou sous de faux noms, par le biais des vecteurs informatique ou téléphonique, ou encore par télécopie. Les recherches effectuées pour tenter de découvrir l'origine de tels faits impute la consultation du trafic téléphonique des lignes exploitées ou payées par l'Institution (exclusivement l'identification des numéros, le moment et la durée des communications, à l'exclusion de leur contenu), du trafic e-mail transitant par le réseau informatique de la Commission, des connexions au réseau internet au départ du réseau interne de la Commission, et de l'utilisation et du contenu des différentes bases de données exploitées au sein de la Commission. Il en est de même lorsqu'ADMIN/DS est sollicitée par les instances habilitées telles que l'ADMIN/IDOC ou l'OLAF, ou encore sur requête formelle des autorités judiciaires, pour effectuer une telle recherche. Une procédure spécifique a été établie dans le cadre particulier de l'autorisation de telles recherches impliquant une requête adressée à la DG DIGIT ou, le cas échéant, à toute autre Direction générale. Une demande écrite est d'abord adressée au DPD de la Commission. Ce dernier a accès aux données motivant ladite demande de recherche. Après autorisation écrite du DPD, la demande motivée est introduite par le Directeur ADMIN/DS auprès du Directeur général ADMIN. Ce n'est qu'avec l'aval écrit de ce dernier que les recherches visées sont entreprises sur base du réquisitoire constatant le suivi de ladite procédure. Ces recherches peuvent amener à une requête adressée à la DG DIGIT et/ou à l'Office "Infrastructures et logistique" - Bruxelles (OIB), ainsi qu'à toute autre DG concernée[2].

Dans ses activités de recherche, le secteur ADMIN/DS/RA est susceptible de faire faire des copies de disques dues aux fins d'analyse des données. La procédure prévue dans l'information administrative 45-2006 du 15/09/2006 est d'application. Un "protocole" spécifique pour régir cette activité n'a pas été mis en place.

[1] Ce traitement de données fait l'objet d'une notification distincte (Dossier EDPS n°2007-271).

[2] En ce qui concerne les recherches effectuées sur de moyens informatiques (utilisations de l'e-mail, d'internet et de matériel informatique) et de communication (téléphone, télécopieur, gsm), les conditions acceptables d'utilisation ainsi que les moyens de contrôle et d'enquête sont décrits dans l'information administrative 45-2006 du 15/09/2006.

- Base de données des accès effectifs aux immeubles et aux zones équipées d'un contrôle d'accès informatisé.

L'accès aux différents immeubles occupés par la Commission est soumis à un contrôle, soit humain (gardiennage), soit électronique. Certains accès soumis au contrôle humain sont consignés dans des registres ad-hoc, complétés par les huissiers ou par les gardes sous la responsabilité de l'unité ADMIN/DS4. Il s'agit notamment en tous temps des accès de visiteurs, de prestataires de services agréés (techniciens, nettoyeurs, gardes…), de corps de métiers autorisés (entreprises diverses). Ce contrôle vise l'accès à l'immeuble lui-même ou à certains de ses locaux verrouillés, par retrait d'une clé contre communication de son identité, mais aussi l'accès aux immeubles par le personnel statutaire en dehors des heures normales de bureau. Certaines zones spécifiques situées au sein même des immeubles occupés par la Commission sont équipées d'un contrôle d'accès informatisé dont la base de données conserve une trace des passages récents enregistrés. Cette base de données est exploitée par l'unité ADMIN/DS4.

- Base de données de la Caisse maladie et accidents.

Le PMO exploite une base de données relative aux interventions de la Caisse Maladie-Accidents au profit du personnel de la Commission. Les recherches effectuées par le Secteur « Réquisitions administratives » dans le cadre de ses compétences propres l'amènent parfois à solliciter la communication d'éléments contenus dans cette base. L'exemple à envisager est celui de l'existence et de l'usage de faux documents introduits par un ayant-droit en vue de bénéficier de remboursements indus. Sauf le cas particulier de requête des autorités judiciaires en vue de l'identification formelle d'une personne amnésique ou décédée, la consultation des bases de données dont question exclut toute donnée médicale.

- Les interventions techniques effectuées dans les bâtiments.

Les Offices des infrastructures logistiques de Bruxelles et de Luxembourg (OIB et OIL) exploitent des bases de données reprenant des informations relatives aux différentes interventions techniques effectuées dans les bâtiments occupés par la Commission.

2.4. Conservation des données

Les données contenues dans la base de données informatique ainsi que dans les dossiers physiques peuvent être conservées par le secteur ADMIN/DS/RA pendant une durée maximale de dix ans prenant cours à la clôture du dossier. Ce délai correspond au délai de prescription généralement admis par la loi dans le cadre de dossiers de type pénal. Les agents traitant les dossiers peuvent en effet être appelés à témoigner devant les instances compétentes.

Les données contenues sur la liste des interdictions d'accès aux immeubles occupés par la Commission sont conservées le temps strictement nécessaire à l'application de la mesure d'interdiction d'accès, et en tous cas pas au-delà de cinq ans après la mise en application de ladite mesure.

Pour permettre la comparaison des précédents et l'élaboration de statistiques, les rapports finals concernant des enquêtes internes peuvent être conservés, une fois rendus anonymes, pendant 50 ans.

2.5. Transferts de données

Le rapport établi ainsi que documents joints au rapport et susceptibles d'étayer les résultats exposés dans le rapport () sont transmis pour suivi à l'instance compétente pour les connaître, à savoir OLAF, IDOC, les autorités judiciaires compétentes des États membres et/ou des Etats tiers

et organisations internationales, ou encore les services médical ou social, l'OIB (secteur « assurances »), ou enfin tout service strictement appelé à entreprendre une action nécessaire suite aux conclusions des recherches. Dans ce dernier cas, une communication partielle du rapport peut être envisagée.

Les données inclus dans le rapport et transmis dépendent du cas traité. Un "rapport type" n'existe pas. D'habitude le rapport contient un résumé des faits et constatations (parfois un dossier photographique de ces dernières), la description des actions entreprises, parfois un évaluation juridique des faits et des recommandations.

2.6. Informations fournies aux personnes concernées

2.6.1. La manière d'informer

- Personne faisant objet d'une enquête

Le secteur ADMIN/DS/RA informe la personne faisant objet d'une enquête lors du recueil de sa déclaration écrite.

En effet, chaque compte-rendu d'une déclaration est précédé d'un texte suivant : "*J'ai pris connaissance du fait que je ne suis nullement obligé de faire la présente déclaration administrative et que, si j'accepte, je peux en demander copie. Vous me signalez que les éléments que je vous communique feront l'objet d'un traitement de données informatisé. Vous me signalez que j'ai ultérieurement l'occasion d'effectuer une déclaration complémentaire si je souhaite modifier ou compléter ces éléments, auxquels je conserve un droit général d'accès.*
Les données personnelles me concernant et qui seraient collectées dans le cadre de la présente affaire sont protégées par les prescrits du Règlement 45/2001, dont je puis avoir connaissance à l'adresse www.cc.cec/security/index_en.html où est également consultable la déclaration de confidentialité relative à la protection des données contenues dans la base à l'usage du secteur "Réquisitions administratives" de la Direction ADMIN/Sécurité.
Les droits d'accès, d'information et de rectification (cfr. art. 13 à 17 et 37 dudit Règlement) sont, en la présente matière, restreints d'une part par les nécessités de prévention, d'enquête, de détection et de poursuite d'infractions, mais aussi par la protection des droits et libertés de chacun (article 20). J'ai connaissance de mon droit de m'adresser au Contrôleur européen de la Protection des données, qui effectuera une vérification dans les cas couverts par l'article 20. Je déclare avoir reçu copie de la déclaration de confidentialité relative à la protection des données contenues dans la base à l'usage du Secteur "Réquisitions administratives" de la Direction ADMIN/Sécurité. Les données personnelles ne peuvent être traitées qu'aux fins pour lesquelles elles ont été transmises."

Dans le cas où les circonstances ne permettent pas d'entrer en contact à un moment ou à un autre du traitement du dossier avec la personne concernée (impossibilité factuelle, comme par exemple en ce qui concerne des personnes disparues ou fugitives), cette opportunité leur sera proposée dès le premier contact ultérieur permettant cette faculté.

Dans l'hypothèse où le service ne procède pas au recueil de la déclaration écrite et n'a aucun contact avec la personne avant de transmettre les données à un autre service (OLAF, IDOC, autorités nationales), la personne concernée n'est pas informée par le secteur ADMIN/DS/RA. La seule information disponible est celle contenue sur le site internet de la Direction Sécurité.

En ce qui concerne les personnes dont l'accès aux immeubles de la Commission est interdit font au préalable l'objet d'une notification de la décision dont question. S'il s'agit de personnel statutaire de la Commission, la DG ADMIN veille à notifier à l'intéressé la décision de l'AIPN compétent et ce n'est qu'après cette notification, sauf impossibilité matérielle (par exemple en ce qui concerne des personnes fugitives et latitentes), que la base de données est complétée. S'il

s'agit de visiteurs, de prestataires de services ou de personnes extérieures (par exemple membres de la famille de personnel statutaire), l'inscription dans la base de données n'intervient que sur dû motif, à condition qu'il y ait danger imminent ou si la personne détient un titre d'accès qu'elle n'a pas restitué ou pas accepté de restituer, et après que la mesure lui ait été signifiée dans la mesure du possible, soit directement par le secteur ADMIN/DS/RA, soit à travers l'employeur s'il s'agit d'un prestataire de services.

- Informateurs, dénonciateurs et témoins

Toute personne qui s'adresse au secteur ADMIN/DS/RA pour signaler un fait ou solliciter une assistance, technique ou personnelle, ou toute personne contactée dans le cadre de recherches est avisée, verbalement ou par écrit selon la nature du contact qu'elle a avec les membres du secteur, du fait que les éléments qu'elle communique seront consignés dans une base de données et qu'elle est loisible, si elle le souhaite, de recontacter son interlocuteur pour compléter ou modifier ultérieurement ces éléments.

En effet, chaque compte-rendu d'une déclaration est précédé d'un texte identique à celui relatif à la "Personne faisant objet d'une enquête" (voir *infra*).

Dans le cas où les circonstances ne permettent pas d'entrer en contact à un moment ou à un autre du traitement du dossier avec la personne concernée, cette opportunité leur sera proposée dès le premier contact ultérieur éventuel permettant cette faculté.

2.6.2. Le contenu de l'information

Si l'information est envoyée par email une réponse automatique suivante (en français et en anglais) est automatiquement générée : "*Votre message a bien été enregistré et sera traité dans les meilleurs délais. Il est porté à votre connaissance que les données que vous avez communiquées feront l'objet d'un traitement informatisé. Il vous est possible de faire modifier ou compléter ces données par même voie. Les données personnelles sont protégées par les prescrits du Règlement 45/2001, repris à l'adresse "www.cc.cec/security/index_en.html". Le droit d'en connaître peut être, en la présente matière, restreint d'une part par les nécessités de prévention, d'enquête, de détection et de poursuite relatives à des infractions, mais aussi par la nécessaire protection des droits et libertés de chacun (article 20 dudit Règlement)". Dominique Baudoux, Raf Philips, Direction ADMIN/Sécurité – Secteur Réquisitions administratives*"

Selon l'information fournie par le responsable du traitement, sous peu, la réponse automatique sera la suivante :
"*Votre message a bien été enregistré et sera traité dans les meilleurs délais. Il est porté à votre connaissance que les données que vous avez communiquées feront l'objet d'un traitement informatisé. Il vous est possible de faire modifier ou compléter par même voie ces données auxquelles vous conservez un droit général d'accès. Les données personnelles sont protégées par les prescrits du Règlement 45/2001, repris à l'adresse www.cc.cec/security/index_en.html où est également consultable la déclaration de confidentialité relative à la protection des données contenues dans la base à l'usage du secteur "Réquisitions administratives" de la Direction ADMIN/Sécurité.*
Les droits d'accès, d'information et de rectification (cfr. art. 13 à 17 et 37 dudit Règlement) sont, en la présente matière, restreints d'une part par les nécessités de prévention, d'enquête, de détection et de poursuite d'infractions, mais aussi par la protection des droits et libertés de chacun (article 20). J'ai connaissance de mon droit de m'adresser au Contrôleur européen de la Protection des données, qui effectuera une vérification dans les cas couverts par l'article 20. Je déclare avoir reçu copie de la déclaration de confidentialité relative à la protection des données contenues dans la base à l'usage du Secteur "Réquisitions administratives" de la Direction ADMIN/Sécurité. Les données personnelles ne peuvent être traitées qu'aux fins pour lesquelles elles ont été transmises."

Si l'information est fournie lors de la déposition de la déclaration écrite, la personne concernée reçoit la "Déclaration de confidentialité - Protection des données - Bases de données à l'usage du Secteur « Réquisitions administratives » de la Direction ADMIN/Sécurité". Ce document contient l'information sur l'identité du responsable du traitement, les finalités du traitement, les destinataires des données, l'existence d'un droit d'accès et de rectification des données, les délais de conservation et les mesures de sécurité et le droit de saisir le CEPD dans le contexte de demande d'accès aux données.

2.7. Droit d'accès et de rectification

En principe, le secteur ADMIN/DS/RA ne communique pas, ni aux personnes faisant objet d'une enquête, ni aux informateurs et témoins, des rapports et autres documents liés à l'enquête. Cela dans le but de ne commettre aucun impair pouvant mettre à mal les procédures entamées par les instances compétentes (IDOC/OLAF/autorités judiciaires nationales). Selon la notification, la communication du contenu de rapports dressés par le secteur ADMIN/DS/RA incombe à ces dernières, dans le cadre des procédures qui régissent leur action propre.

Les personnes concernées ont toutefois la possibilité de corriger les informations qu'elles ont communiquées ou qui leurs sont communiquées, que ce soit immédiatement ou ultérieurement, par d'une déclaration complémentaire qu'elles peuvent faire parvenir et qui fera partie intégrante du dossier. Cette faculté est systématiquement communiquée lors de contacts avec les personnes concernées, et également exposée sur le site de la Direction ADMIN/Sécurité. Selon le contrôleur cette procédure garantit la rectification et la mise à jour des données en fonction des développements ultérieurs.

Selon le responsable du traitement, en ce qui concerne les données qui ne sont pas communiquées directement par la personne concernée, elles entrent dans le cadre des exceptions mentionnées à l'article 20 du Règlement 45/2001. Toute personne peut dès lors saisir le Contrôleur européen de la protection des données afin que celui-ci contrôle l'aspect licite du traitement. Il est toujours loisible à une personne concernée de faire appel au Délégué à la protection des données de la Commission, qui peut vérifier les données la concernant et, le cas échéant, les faire modifier ou les faire supprimer pour un motif légitime évoqué.

2.8. Sécurité

Des mesures de sécurité ont été adoptées pour protéger les documents électroniques et sur papier.

[...]

3. Aspects juridiques

3.1. Contrôle préalable

Le contrôle préalable porte sur le traitement de données à caractère personnel dans le contexte des enquêtes de sécurité internes effectuées par le secteur ADMIN/DS/RA. Le traitement est réalisé par une institution européenne, dans le cadre du droit communautaire. Le traitement de données à caractère personnel est en partie automatisé et le traitement manuel concerne des données contenues ou appelées à figurer dans un fichier. Le règlement est donc applicable.

L'article 27, paragraphe 1, du règlement soumet au contrôle préalable du CEPD tous "*les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités*". L'article 27, paragraphe 2, comporte une liste des traitements susceptibles de présenter de tels risques.

Selon l'article 27, paragraphe 2, point b), du règlement, les opérations destinées à "*évaluer des aspects de la personnalité des personnes concernées, tels que leur (…) comportement*" sont soumises au contrôle préalable du CEPD. Dans le cas présent, le comportement des personnes est analysé par le secteur ADMIN/DS/RA.

En outre, 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 également soumis au contrôle préalable du CEPD. Dans le cas d'espèce, le traitement pourrait porter sur ce type de données.

Etant donné que le responsable de traitement établit une liste des interdictions d'accès aux immeubles occupés par la Commission, l'article 27, paragraphe 2, point d) relatif aux *traitements visant à exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat*, est également applicable.

Dans la mesure où le responsable du traitement peut effectuer des analyses des disques durs des ordinateurs contenant des données privées, le CEPD, conforment à l'interprétation constante du règlement, considère que l'article 27, paragraphe 1 du règlement est applicable.

Étant donné que le contrôle préalable vise à faire face à des situations susceptibles de présenter certains risques, l'avis du CEPD devrait être rendu avant le début du traitement concerné. Or, en l'espèce, le traitement a déjà commencé. Cela ne devrait cependant pas poser de problème sérieux dans la mesure où d'éventuelles recommandations du CEPD peuvent encore être adoptées si nécessaire.

La notification du DPD a été reçue le 17 décembre 2007. Conformément à l'article 27, paragraphe 4, le présent avis doit être rendu dans les deux mois qui suivent la réception de la notification. La procédure a été suspendue pendant 197 jours et pendant le mois d'août 2008. L'avis sera dès lors rendu le 3 octobre 2008 au plus tard.

3.2. Licéité du traitement

La licéité du traitement doit être examiné à la lumière de l'article 5, point a), du règlement, qui prévoit que le traitement de données à caractère personnel ne peut être effectué que si: "*le traitement 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".*

Le traitement de données dans le cadre d'enquêtes administratives internes est basé sur la Décision de la Commission du 19 septembre 1994 relative aux missions du Bureau de sécurité ainsi que sur la Décision de la Commission n°844/2001 du 29 novembre 2001 relative aux mesures de sécurité.

Les instruments précités indiquent que les enquêtes administratives menées par le secteur ADMIN/DS/RA sont des missions d'intérêt public (lutte contre la criminalité, protection des personnes et des biens, etc.). En outre, le secteur ADMIN/DS/RA effectue ces activités dans l'exercice légitime d'une autorité publique et respecte donc l'obligation juridique qui lui est faite d'examiner les questions relevant de sa compétence.

Le CEPD attire attention sur le fait que la formulation "*lutte contre la criminalité*", qui implique l'usage de la répression par l'Etat, n'est pas la plus adaptée à la lumière de la base juridique du traitement. Le responsable de traitement a informé le CEPD que cette formulation sera remplacée, dans les textes où elle figure, par la phrase suivante : "*recherches relatives à toute infraction pénale et/ou administrative, qu'elle soit survenue dans les locaux occupés par la Commission, que*

certains membres de son personnel en soient préjudiciés ou y soient impliqués, ou encore que la Commission elle-même y soit impliquée ou soit préjudiciée".

La "nécessité" du traitement doit être analysée en termes concrets. Dans cette perspective, il convient de ne pas perdre de vue que le traitement de données à caractère personnel effectué dans le cadre des enquêtes doit être proportionné à l'objectif général du traitement (enquêter sur les faits délictueux ou criminels, protéger des personnes et des biens, etc.), ainsi qu'à l'objectif particulier du traitement dans le contexte de l'affaire en cause (il convient d'examiner, par exemple, la gravité du fait qui fait l'objet de l'enquête, le type de données requis pour éclaircir les faits, etc.). Il convient dès lors d'évaluer le caractère proportionné du traitement au cas par cas.

3.3. Traitement portant sur des catégories particulières de données

L'article 10, paragraphe 5, dispose que: *"[l]e traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que s'il est autorisé par les traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités ou, si cela s'avère nécessaire, par le contrôleur européen de la protection des données".* En l'espèce, le traitement des données visées est autorisé par les actes législatifs mentionnés au point 3.2 ci-dessus.

Au delà de cette hypothèse, selon l'article 10, paragraphe 1, du règlement, le traitement de catégories particulières de données (c'est-à-dire les "*données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé ou à la vie sexuelle*") est interdit. Le règlement prévoit certaines exceptions à l'article 10, paragraphe 2. Il semble toutefois très probable que, si une exception devait s'appliquer, seuls les points b) et d) seraient éventuellement concernés.

En effet, le type de données décrites à l'article 10, paragraphe 1, ne fera l'objet d'un traitement qu'à titre exceptionnel. Cependant, il peut arriver, par exemple, que les consultations des fichiers de régime d'assurance maladie de l'UE révèlent des données relatives à la santé. Dans ce cas, il convient de respecter l'interdiction générale établie à l'article 10, paragraphe 1, ou d'examiner de façon restrictive s'il est nécessaire d'appliquer une exception. Quoi qu'il en soit, le personnel du secteur ADMIN/DS/RA chargé des dossiers ne doit pas perdre de vue la règle que les exceptions doivent rester exceptionnelles et doit éviter d'inclure des catégories particulières de données, à moins que l'une des circonstances prévues à l'article 10, paragraphe 2 ne soit présente dans l'affaire en cause ou qu'il ne soit nécessaire d'appliquer l'article 10, paragraphe 4.

3.4. Qualité des données

Aux termes de l'article 4, paragraphe 1, point c), les données à caractère personnel doivent être "*adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement*".

Si certaines données types, telles que le nom et la date de naissance, figureront de manière systématique dans les dossiers d'enquêtes, le contenu exact de ces dossiers diffèrera naturellement selon les cas. Il y a toutefois lieu de prévoir des garanties pour veiller au respect du principe de la qualité des données. Ces garanties pourraient prendre la forme d'une recommandation générale adressée aux personnes qui gèrent ces dossiers, en vue de leur rappeler ce principe et de les inviter à veiller au respect de celui-ci.

Le responsable du traitement a adressé une instruction écrite, contre signature, au personnel du secteur "Réquisitions administratives", rappelant le principe de la qualité des données à respecter avec attention.

Le CEPD recommande aussi que lorsque l'accès à des données personnelles apparaît nécessaire aux fins de l'enquête, cet accès soit effectué en respectant des garanties appropriées et en tenant compte de tout risque potentiel d'irrecevabilité des preuves, au cours d'une procédure pénale ultérieure, que pourrait entraîner le non-respect des droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel lors de la collecte de preuves. Une attention particulière au respect de ces principes doit être portée lorsque l'accès à des dossiers qui sont manifestement de nature privée apparaît nécessaire aux fins de l'enquête.

Ces principes s'appliquent également aux traitements requérant des analyses criminalistiques d'ordinateurs. Il y a lieu de prendre les précautions spécifiques concernant l'accès au contenu d'un ordinateur appartenant à une institution communautaire, car il peut également comporter des fichiers utilisés par la personne concernée à des fins privées (par exemple, dans le dossier "My documents", ou les messages électroniques marqués comme étant "privés") ou des fichiers qui ne sont pas pertinents ou qui sont excessifs au regard des fins de l'enquête. La réalisation de telles analyses criminalistiques d'ordinateurs doit être soumise à des mécanismes d'autorisation particuliers. À cet égard, le CEPD recommande l'adoption d'un protocole officiel de "procédures opératoires normalisées" pour la réalisation d'analyses criminalistiques d'ordinateurs, qui contribuera également à garantir le respect du principe de la qualité des données[3].

Aux termes de 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*". La procédure mise en place doit permettre raisonnablement de penser que les données sont exactes et mises à jour. Ce principe est étroitement lié à l'exercice du droit d'accès, de rectification, de verrouillage et d'effacement (voir le point 3.8 ci-dessous).

Les données doivent également être "*traitées loyalement et licitement*" (article 4, paragraphe 1, point a), du règlement). La question de la licéité a déjà été examinée. Quant à la loyauté, il convient de lui accorder une grande attention dans le cadre d'un sujet aussi sensible. Elle concerne les informations fournies au fonctionnaire visé par une enquête (ainsi qu'aux autres personnes concernées) et la rapidité avec laquelle ces informations lui sont transmises, afin que le droit de défense puisse être respecté.

3.5. Conservation des données

Les données à caractère personnel doivent être "*conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. L'institution ou l'organe communautaire prévoit, pour les données à caractère personnel qui doivent être conservées au-delà de la période précitée à des fins historiques, statistiques ou scientifiques, soit qu'elles ne seront conservées que sous une forme qui les rend anonymes, soit, si cela est impossible, qu'elles ne seront stockées qu'à condition que l'identité de la personne concernée soit cryptée. Les données ne doivent en tout cas pas être utilisées à des fins autres qu'historiques, statistiques ou scientifiques*" (article 4, paragraphe 1, point e), du règlement).

Les données contenues dans la base de données informatique ainsi que dans les dossiers physiques sont conservées pendant une durée de dix ans prenant cours à la clôture du dossier. Ce délai correspond au délai de prescription généralement admis par la loi dans le cadre de dossiers

[3] Voir sur ce point l'avis du CEPD du 23 juin 2006 (dossier 2005-418) concernant une notification relative à un contrôle préalable reçue du délégué à la protection des données de l'Office européen de lutte antifraude (OLAF) à propos des enquêtes internes effectuées par l'OLAF.

de type pénal. Les agents traitant les dossiers peuvent en effet être appelés à témoigner devant les instances compétentes.

En ce qui concerne les données contenues sur la liste des interdictions d'accès aux immeubles occupés par la Commission, elles sont conservées pendant cinq ans après la mise en application de l'interdiction.

Pour permettre la comparaison des précédents et l'élaboration de statistiques, les rapports finals concernant des enquêtes internes peuvent être conservés, une fois rendus anonymes, pendant 50 ans.

Le CEPD estime que cette politique de conservation de données est conforme aux dispositions du règlement.

3.6. Transfert de données

3.6.1. Transferts de données à caractère personnel entre institutions ou organes communautaires ou en leur sein

Selon l'article 7, paragraphe 1, du règlement : "*Les données à caractère personnel ne peuvent faire l'objet de transferts entre institutions ou organes communautaires ou en leur sein que si elles sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire*".

Cela signifie que, les rapports et/ou les documents connexes (données à caractère personnel) sont transférés uniquement si cela est "nécessaire" à l'exécution légitime de missions relevant de la compétence du destinataire. Il convient, à cet égard, de prendre en considération le critère de proportionnalité, compte tenu, par exemple, de la nature des données recueillies et traitées ultérieurement, ainsi que de la compétence du destinataire.

En tout état de cause, conformément à l'article 7, paragraphe 3, du règlement, il convient d'informer le destinataire que les données à caractère personnel ne peuvent être traitées qu'aux fins pour lesquelles elles ont été transmises. A la suite de cette recommandation, le responsable du traitement a décidé d'ajouter en note en bas de première page de tout rapport transmis la phrase : "*les données à caractère personnel ne peuvent être traitées qu'aux fins pour lesquelles elles ont été transmises*"

3.6.2. Transfert de données à caractère personnel aux États membres

Deux scénarios peuvent être observés dans les États membres :

a) les États membres dans lesquels la législation relative à la protection des données adoptée en application de la directive 95/46/CE couvre tous les secteurs du système juridique national, y compris le secteur judiciaire ;

b) les États membres dans lesquels la législation relative à la protection des données adoptée en application de la directive 95/46/CE ne couvre pas tous les secteurs et, en particulier, pas le secteur judiciaire.

En ce qui concerne le premier scénario, l'article 8 du règlement prévoit ce qui suit : *"Sans préjudice des articles 4, 5, 6 et 10, les données à caractère personnel ne sont transférées à des destinataires relevant de la législation nationale adoptée en application de la directive 95/46/CE que si : a) le destinataire démontre que les données sont nécessaires à l'exécution d'une mission effectuée dans l'intérêt public ou relevant de l'exercice de l'autorité publique, (...)"*.

Dès lors, même si les autorités judiciaires n'entrent pas dans le champ d'application de la directive 95/46/CE, l'article 8 du règlement doit être pris en considération si l'État membre, lors de la transposition de ladite directive, a étendu son application à ces autorités publiques.

Pour les pays qui n'ont pas étendu l'application de la directive 95/49/CE aux autorités judiciaires, il convient de prendre en considération l'article 9 du règlement. Dans le cas de ces pays, la Convention 108 du Conseil de l'Europe, qui, pour ce qui concerne la question étudiée, peut être considérée comme fournissant un niveau de protection adéquat, est en tout état de cause applicable aux autorités judiciaires.

3.6.3. Transfert aux autorités de pays tiers et/ou à des organisations internationales

En vertu de l'article 9.1 du règlement "*le transfert de données à caractère personnel à des destinataires autres que les institutions communautaires, et qui ne sont pas soumis à la législation nationale adoptée en application de la directive 95/46/CE, ne peut avoir lieu que pour autant qu'un niveau de protection adéquat soit assuré dans le pays du destinataire ou au sein de l'organisation internationale destinataire, et que ce transfert vise exclusivement à permettre l'exécution des missions qui relèvent de la compétence du responsable du traitement*". Ainsi, les transferts vers les Etats qui n'offrent pas de niveau de protection adéquat ne sont, en principe, pas possibles.

Toutefois, l'article 9.6 stipule que des dérogations sont possibles, notamment dans le cas où "*le transfert est nécessaire ou rendu juridiquement obligatoire pour des motifs d'intérêt public importants ou pour la constatation, l'exercice ou la défense d'un droit en justice*" (article 9.6.d). Etant donné que cette disposition est une exception, son interprétation doit être stricte. Une utilisation systématique de cette dérogation ne peut donc pas avoir lieu. Seule peut être acceptée une utilisation occasionnelle dans des cas où le transfert est particulièrement nécessaire par rapport à la finalité du traitement. En tout état de cause, l'utilisation de l'article 9.6 ne peut créer une situation où les droits fondamentaux de la personne concernée soient violés.

Une autre forme de dérogation est prévue à l'article 9.7 qui stipule que le transfert peut être autorisé par le CEPD "*lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants; ces garanties peuvent notamment résulter de clauses contractuelles appropriées*". Lors de transfert des données, le responsable de traitement doit fournir au destinataire une information sur les principes de la protection des données et s'assurer que la vie privée et les droits et libertés fondamentaux de la personne concernée sont garantis par le destinataire.

En vertu de l'article 9.8, le secteur ADMIN/DS/RA doit informer le CEPD des catégories de cas dans lesquels il a appliqué l'article 9.6 et 9.7. A ce fin le CEPD recommande de mettre en place un registre des transferts occasionnels effectués en vertu de la dérogation de l'article 9.6 et 9.7. Ce registre pourrait contenir les informations suivantes : finalités du transfert, personnes concernées, catégories de données, information des personnes concernées (si applicable), droits d'accès (direct ou indirect), base juridique et légalité de transfert, destinataires de données, indication de temps de conservation des données par le destinataire, etc. Ce registre devrait être toujours tenu à disposition du CEPD.

Le responsable du traitement a informé le CEPD lors de la rédaction de l'avis qu'une information sera ajoutée en note en bas de première page de tout document transmis : "*les données à caractère personnel ne peuvent être traitées qu'aux fins pour lesquelles elles ont été transmises*". Cette information sera complétée par une mention des principes de la protection des données et du nécessaire respect de la vie privée et des droits et libertés fondamentaux des personnes concernées, principe que doit respecter le destinataire du rapport.

Par ailleurs, le responsable du traitement s'est engagé à tenir un registre informatique de ces transferts reprenant le numéro du dossier, la date de transmission, le destinataire, la finalité du transfert, les personnes concernées, les catégories des données, l'éventuelle information des personnes concernées, les droits d'accès (direct ou indirect), la base juridique et la légalité du transfert, et l'indication du temps de conservation des données par le destinataire.

3.7. Traitement incluant le numéro personnel ou un autre numéro identifiant de portée générale

Le secteur ADMIN/DS/RA utilise le numéro personnel d'un fonctionnaire visé par une enquête, ce numéro figurant dans le rapport final. Dans le cas présent, l'utilisation du numéro personnel est raisonnable, puisqu'elle a pour seul but d'identifier la personne concernée par le dossier. Le CEPD considère que ce numéro peut faire l'objet d'un traitement dans le scénario mentionné.

3.8. Droit d'accès et de rectification

Selon l'article 13 du règlement, la personne concernée a le droit d'obtenir, sans contrainte, 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.

Le droit d'accès est le droit de la personne concernée d'être informée de tout renseignement la concernant traité par le responsable du traitement. Par principe, ce droit doit être interprété en liaison avec la notion de données à caractère personnel. En effet, une vision large des données à caractère personnel a été adoptée dans le règlement, et le Groupe de l'article 29 a également donné une large interprétation à ce concept[4]. Le respect du droit d'accès et de rectification est directement lié au principe de la qualité des données et, dans le cadre des enquêtes, il se superpose en grande partie au droit de défense.

En outre, le droit d'accès est également applicable lorsqu'une personne concernée demande l'accès aux dossiers d'autres personnes, si ceux-ci contiennent des informations la concernant. Tel est le cas lorsque des informateurs ou des témoins demandent l'accès à des données les concernant dans le cadre d'une enquête menée à l'égard d'une autre personne.

Les informations peuvent être obtenues 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).

Comme indiqué au point 2.6, la règle générale appliquée par le secteur ADMIN/DS/RA est le refus de l'accès aux données à caractère personnel relatives à la personne concernée contenues dans le dossier d'enquête. Selon le responsable du traitement, un tel droit d'accès serait nuisible à l'enquête devant les instances compétentes (IDOC/OLAF/autorités nationales, etc.).

Le CEPD estime que le principe de refus d'accès aux données est manifestement contraire à l'article 13 du règlement. Le responsable de traitement ne peut pas appliquer l'exception comme une règle générale. Il convient de ne pas perdre de vue que les limitations d'un droit fondamental ne peuvent être appliquées de manière systématique. Ces limitations doivent être "nécessaires". Le "critère de nécessité" doit être apprécié au cas par cas et, tout comme le droit d'information, les droits d'accès et de rectification devront être garantis "*lorsque cela ne risque pas de nuire à l'enquête"* (voir le point 3.9 ci-dessous). C'est ainsi, par exemple, que la nature de certaines affaires ne justifiera pas toujours le refus d'accès et de rectification au cours d'une enquête interne

[4] Cf. Avis 4/2007 du 20 juin 2007 sur le concept de données à caractère personnel adopté par le Groupe de travail "Article 29" sur la protection des données (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_fr.pdf).

du secteur ADMIN/DS/RA. C'est pourquoi le CEPD recommande d'inclure une règle générale d'accès aux données, compte tenu de son importance aux fins de la protection des données.

Toutefois, l'article 20 du règlement prévoit certaines limitations de ce droit, notamment lorsqu'une telle limitation constitue une mesure nécessaire pour "*a) assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales; b) sauvegarder un intérêt économique ou financier important d'un État membre ou des Communautés européennes, y compris dans les domaines monétaire, budgétaire et fiscal; c) garantir la protection de la personne concernée ou des droits et libertés d'autrui"*. En outre, il peut être nécessaire dans certains cas de ne pas accorder à la personne concernée un accès direct afin de ne pas nuire au bon déroulement de l'enquête, même s'il n'y a pas d'enquête pénale au sens de l'article 20 du règlement (CE) n° 45/2001 mais une enquête "prédisciplinaire" ou "prépénale". L'intérêt de l'autorité qui est censée suivre l'enquête (OLAF, IDOC, autorités nationales) peut également être pris en compte à cet égard.

En tout état de cause, le paragraphe 3 de l'article 20 doit être pris en compte et respecté par le secteur ADMIN/DS/RA : *"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"*. En ce qui concerne le droit d'information, cette disposition doit être lue en combinaison avec les articles 11, 12 et 20 du règlement (voir le point 3.9 ci-dessous).

En outre, il y a lieu de tenir compte également du paragraphe 4 de l'article 20 : *"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"*. Le droit d'accès indirect devra alors être garanti. En effet, 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.

L'article 20, paragraphe 5, dispose que *"L'information visée aux paragraphes 3 et 4 peut être reportée aussi longtemps qu'elle prive d'effet la limitation imposée sur la base du paragraphe 1"*. Il peut se révéler nécessaire pour le secteur ADMIN/DS/RA de différer cette information conformément à cette disposition, afin de protéger l'enquête. La nécessité d'un tel report doit être appréciée au cas par cas.

Comme indiqué précédemment, le droit d'accès implique le droit de la personne concernée à être informée des données la concernant. Cependant, comme on l'a déjà noté, ce droit peut être limité pour garantir "*la protection (…) des droits et libertés d'autrui"*. Il y a lieu d'en tenir compte dans le cadre de la présente analyse pour ce qui concerne l'accès de la personne concernée à l'identité des dénonciateurs. Le Groupe de l'article 29 a fait la déclaration suivante: "*La personne accusée dans le rapport d'un dénonciateur ne peut en aucune circonstance obtenir des informations concernant l'identité du dénonciateur sur la base du droit d'accès de la personne accusée, sauf lorsque le dénonciateur fait une fausse déclaration par malveillance. Dans les autres cas, la confidentialité de l'identité du dénonciateur doit toujours être garantie*". Il convient d'appliquer la même approche pour ce qui concerne les informateurs[5].

L'article 14 du règlement accorde à la personne concernée le droit à la rectification des données inexactes ou incomplètes. Compte tenu de la sensibilité de la plupart des enquêtes menées par le secteur ADMIN/DS/RA, ce droit revêt une importance cruciale pour garantir la qualité des données utilisées, laquelle est, en l'espèce, liée au droit de défense. Toute limitation au titre de l'article 20 du règlement doit être appliquée à la lumière de ce qui a été dit aux paragraphes précédents concernant le droit d'accès.

[5] Il n'est pas nécessaire, en revanche, de garantir la confidentialité de l'identité des témoins.

Enfin, il y a lieu d'établir des règles afin que, dès qu'une enquête est close, le fonctionnaire visé par l'enquête puisse rectifier toute donnée le concernant en demandant l'inclusion dans le dossier d'enquête des documents relatifs à toute évolution ultérieure au cours de la phase de suivi (décision de la Cour statuant en sens contraire, par exemple).

3.9. Information de la personne concernée

Le règlement prévoit que la personne concernée doit être informée lorsque des données à caractère personnel la concernant sont recueillies et énumère une série de mentions obligatoires dans cette information, afin de garantir le traitement loyal de ces données. En l'espèce, les données pourraient être recueillies soit directement auprès de la personne concernée, soit indirectement, par le biais d'informateurs, par exemple.

L'article 11 du règlement (*Informations à fournir lorsque les données sont collectées auprès de la personne concernée*) et l'article 12 (*Informations à fournir lorsque les données n'ont pas été collectées auprès de la personne concernée*) sont donc tous les deux applicables en l'espèce. Cela signifie que les informations pertinentes doivent être fournies soit au moment de la collecte (article 11), soit lorsque les données sont enregistrées ou communiquées à un tiers pour la première fois (article 12), sauf si la personne concernée est déjà informée.

Le type d'informations données aux personnes concernées est décrit de manière détaillée au point 2.6. Cependant, bien que la teneur des informations fournies puisse parfois correspondre partiellement aux informations qui doivent être communiquées en vertu des articles 11 et 12, on constate que les informations visées dans ces dispositions ne sont pas toutes effectivement données. Il convient de tenir compte du fait que toutes les exigences prévues au paragraphe 1 des articles 11 et 12 doivent être respectées, y compris celles mentionnées au point f), puisque, compte tenu de la sensibilité des affaires, les personnes concernées doivent avoir connaissance de toutes les garanties auxquelles elles ont droit. Ainsi, en ce qui concerne le contenu de la déclaration de confidentialité spécifique, le CEPD recommande d'ajouter l'information sur la base juridique du traitement ainsi que l'information sur le droit de saisir le CEPD à tout moment de la procédure et non seulement dans le contexte de l'accès aux données. Le responsable du traitement a informé le CEPD lors de la procédure que la déclaration de confidentialité sera complétée.

En ce qui concerne le moment où ces informations doivent être fournies, il a déjà été indiqué au point 2.6.1 du présent avis que le secteur ADMIN/DS/RA informe les personnes concernées dès la première prise de contact avec elles. En ce qui concerne l'hypothèse où le service ne procède pas au recueil de la déclaration écrite et n'a aucun contact avec la personne avant de transmettre les données à un autre service (OLAF, IDOC, autorités nationales), le secteur ADMIN/DS/RA doit, en vertu de l'article 12 du règlement, informer la personne concernée dès l'enregistrement des données la concernant ou au plus tard lors de la première communication des données à des tiers. Une simple information par le site internet de la DG ADMIN n'est pas suffisante à cet égard. On ne peut pas raisonnablement attendre que les personnes concernées consultent ce site spontanément. Cette recommandation ne concerne pas, évidemment, des situations où le contact avec la personne concernée est impossible pour des raisons factuelles (personne disparue, fugitive,...)

L'article 20 du règlement cité précédemment prévoit certaines limitations du droit d'information (voir le point 3.8 ci-dessus).

En outre, le paragraphe 5 de l'article 20 du règlement devra être appliqué dans des circonstances spécifiques : *"L'information visée aux paragraphes 3 et 4 peut être reportée aussi longtemps qu'elle prive d'effet la limitation imposée sur la base du paragraphe 1"*. (Le paragraphe 3 prévoit que la personne concernée a le droit d'être informée des raisons qui motivent cette limitation et de

son droit de saisir le CEPD ; le paragraphe 4 prévoit un droit d'accès indirect par l'intermédiaire du CEPD et la communication du résultat de cet accès à la personne concernée).

3.10. Mesures de sécurité

Après l'examen minutieux des mesures de sécurité décrites au point 2.8, le CEPD estime que ces mesures sont appropriées au regard de l'article 22 du règlement.

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. En particulier, le responsable du traitement doit:

- évaluer la proportionnalité des activités de traitement au cas par cas ;
- faire en sorte que, lorsque l'accès à des dossiers qui sont manifestement de nature privée apparaît nécessaire aux fins de l'enquête, cet accès soit effectué dans le respect de garanties adéquates ;
- adopter un protocole officiel de "procédures opératoires normalisées" pour la réalisation d'analyses criminalistiques d'ordinateurs, qui contribuera également à garantir le respect du principe de la qualité des données ;
- introduire, conformément à l'article 7, paragraphe 1, du règlement, un avis au destinataire visant à l'informer que les données à caractère personnel ne peuvent être traitées qu'aux fins pour lesquelles elles ont été transmises ;
- transmettre les rapports et/ou les documents connexes (données à caractère personnel) uniquement s'ils sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire. Il y a lieu à cet égard de tenir compte du critère de proportionnalité ;
- établir la nécessité d'un transfert aux autorités judiciaires dans une décision motivée, à la lumière de l'article 8 du règlement ;
- mettre en place un registre des transferts occasionnels effectués en vertu de la dérogation de l'article 9.6 et 9.7 et en informer le CEPD ;
- inclure la règle générale concernant l'exercice du droit d'accès par la personne concernée, sur la base de l'article 13 du règlement, cet accès pouvant être limité s'il est susceptible de nuire à l'enquête, ce qui doit être décidé au cas par cas ;
- établir des règles afin que, dès que l'enquête est terminée et en tenant compte de l'article 20, la personne concernée puisse rectifier les données à caractère personnel la concernant, en vue de leur mise à jour à la lumière des faits ultérieurs ;
- informer la personne concernée dès l'enregistrement des données la concernant ou au plus tard lors de la première communication des données à des tiers ;
- lorsqu'une limitation est appliquée au titre de l'article 20, le mentionner dans le dossier ;
- informer la personne concernée, conformément à l'article 20, paragraphes 3 et 4, du règlement ;
- respecter le contenu des informations qui doivent être fournies à la personne concernée, conformément au paragraphe 1 des articles 11 et 12 du règlement (y compris le point f);

Fait à Bruxelles, le 2 octobre 2008.

(signed)

Joaquín BAYO DELGADO
Contrôleur européen adjoint de la protection des données