Avis concernant une notification relative à un contrôle préalable reçue du délégué à la protection des données de Commission européenne à propos du dossier "Menaces vis-à-vis des intérêts de la Commission dans les domaines contre intelligence, contre terrorisme".

Bruxelles, le 26 janvier 2009 (dossier 2008-440)

1. Procédure

Le 16 juillet 2008, 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 du dossier "Menaces vis-à-vis des intérêts de la Commission dans les domaines contre intelligence, contre terrorisme".

Le 5 septembre 2008, le CEPD a demandé au responsable du traitement des informations complémentaires. Les réponses ont été reçues le 12 septembre 2008. Des questions additionnelles ont été posées le 26 septembre 2008. Des réponses ont été apportées par le responsable du traitement le 14 octobre 2008. Le projet d'avis a été envoyé au responsable du traitement pour commentaires le 6 novembre 2008. A la demande de la Commission une réunion a été organisée le 4 décembre 2008 pour clarifier les faits. Un avis modifié a été envoyé pour commentaires le 19 décembre 2008. Ces derniers ont été reçus le 23 janvier 2009, date à laquelle la suspension du 6 novembre 2008 a été levée.

2. Faits

La ***finalité*** du traitement mis en place par l'unité ADMIN DS 02 est d'assurer la protection du personnel, des bâtiments, des informations et des activités de la Commission européenne ainsi que celle des intérêts des Etats membres en ce qui concerne les menaces relevant des domaines du contre espionnage et du contre terrorisme.

Cette protection comprend notamment (1) la **conduite d'enquêtes de sécurité** et (2) **la réalisation de contrôles de sécurité dits "screening**".

1/ Enquêtes de sécurité

Des enquêtes de sécurité sont menées par les membres de l'unité ADMIN DS 02 à l'aide des informations pertinentes mises à disposition par les Etats membres ou sollicitées auprès d'eux, ainsi que celles collectées au sein de l'institution. La Décision 2001/844/CE met en place un système de sécurité global propre à la Commission dans le cadre duquel il est prévu d'enquêter ou d'ordonner une enquête sur toute fuite concernant les informations classifiées de l'Union européenne qui, d'après les premiers indices, se serait produite à partir de la Commission. De plus, la Charte du Bureau de sécurité du 8 septembre 1994 établit que ce dernier recueille des renseignements permettant d'évaluer les menaces ou risques éventuels

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

pesant sur les services de la Commission et réalise les enquêtes confiées par l'autorité compétente ou déclenchées de sa propre initiative en cas de flagrant délit. Pour ce faire, la décision précise que le bureau a la possibilité d'entendre des membres du personnel ou, en conformité avec les règles applicables en matière de confidentialité, d'avoir accès à tout document interne à la Commission en vue d'obtenir des informations nécessaires à une enquête de sécurité.

a) Les conditions de déclenchement d'une enquête de sécurité

Soit les enquêtes s'effectuent à la Demande du Directeur Général de la DG concernée; celle-ci fait suite à la découverte de faits initiaux donnant à penser qu'une infraction de sécurité a pu être commise. Cette demande est adressée à la DG ADMIN ou au Directeur de la Direction Sécurité. Après approbation du Directeur de la Sécurité, l'unité DS 02 effectue les actes nécessaires de façon à valider les informations reçues, puis à établir les conditions dans lesquelles les faits se sont produits et, s'il y a lieu, à définir les responsabilités des personnels concernés.

Soit lorsque, dans le cadre de l'exercice de leurs compétences, les services de la DS ont à connaître de faits donnant à penser qu'une infraction de sécurité a pu être commise et après avoir validé la valeur des informations reçues, le Directeur de la Sécurité prend l'initiative de demander à la DS 02 l'ouverture d'une enquête destinée à établir les faits et définir les responsabilités éventuellement engagées. Le chef d'unité de la DS 02 est obligatoirement informé de l'ouverture de toute enquête, de ses objectifs et de son contexte. Ces enquêtes font l'objet d'un enregistrement dans la base de données opérationnelle de la DS 02, (n° du cas et nom de dossier ainsi qu'une courte description du cas).

b) Les conditions de mise en œuvre des enquêtes de sécurité

Au sein du secteur Classified Information (CI) de la DS 02, chaque enquête est confiée à un enquêteur en charge. Chaque enquête est strictement soumise à l'obligation du respect de la règle du besoin d'en connaître, à l'intérieur comme à l'extérieur du secteur ainsi qu'à l'extérieur de l'Unité:

- En fonction du degré de confidentialité et du besoin d'en connaître, le Chef d'Unité et le Chef de secteur déterminent les conditions dans lesquelles le dossier doit être traité (information des autres enquêteurs du secteur ou non).

- Tout acte majeur (interview d'un membre du personnel au-delà du niveau de Chef d'Unité ou interview d'un membre du personnel pour lequel une question de responsabilité se pose), donne systématiquement lieu à l'information préalable du Chef d'Unité.

- Toute demande d'accès au dossier personnel ou tout autre acte tombant sous l'application des exceptions et limitations prévues à l'article 20 du règlement 45/2001, sont soumis à l'approbation et à la signature du Chef d'Unité et/ou du Directeur de la Sécurité.

Le Chef de secteur est systématiquement tenu informé par les enquêteurs du secteur de l'ordre du jour des réunions et interviews ainsi que de tous les actes d'enquêtes prévus. Il informe le Chef d'Unité, pour validation, de l'ordre du jour des initiatives à venir et de l'orientation des enquêtes.

Le Directeur est tenu informé au cas par cas en fonction des enjeux propres à chaque dossier soit en temps réel quand jugé nécessaire par le Chef d'Unité DS 02, soit au moins une fois par mois lors de réunions bilatérales "monthly working plan".

Depuis avril 2008, une réunion mensuelle au Cabinet du Commissaire en charge des aspects "sécurité" au cours de laquelle la DS est représentée par le Directeur de la Sécurité et le Chef de l'Unité DS 02, donne lieu à l'exposé des cas et enquêtes en cours.

c) Le traitement et les destinataires du rapport final

Le rapport final d'enquête établi par les enquêteurs est systématiquement soumis à l'approbation du Chef d'Unité et du Directeur de la DS. Dans les cas où l'enquête a été initiée suite à la demande d'un Directeur Général de la Commission, ce rapport final est transmis à la signature du Directeur Général ADMIN, via le Directeur de la DS et le Chef d'Unité DS 02.
Dans le cas où l'enquête a été mise en œuvre à l'initiative du Directeur de la DS, le rapport final est transmis par le Directeur Général ADMIN au Directeur Général dont la DG est concernée par l'enquête.

Indépendamment de ces transmissions, au cas où une responsabilité *pourrait concerner* un enjeu soit disciplinaire soit contraires aux intérêts financiers de l'institution l'IDOC et/ou l'OLAF sont informés et les éléments significatifs du dossier leur sont transmis. Cette transmission s'effectue toujours par la chaîne hiérarchique Chef d'Unité/Directeur de la Sécurité/Directeur Général ADMIN. Pour le cas où d'autres interlocuteurs des Etats membres devraient être informés soit de l'enquête en cours, soit de ses résultats, le Chef de l'Unité DS 02 prend la décision en accord avec le Directeur de la DS, de transmettre les informations jugées nécessaires.

2/ Contrôles de sécurité dits "screening"

La gestion des menaces inclut des contrôles de sécurité dits "screening" de toute personne d'un pays tiers susceptible d'être recrutée ou d'obtenir un contrat à la Commission. À la demande des Directions Générales concernées (les DGs ont reçu pour instruction de l'ADMIN DS 02 d'aviser la DS avant le recrutement ou l'arrivée de ressortissant de pays-tiers pouvant constituer une menace en vue d'un contrôle de sécurité de la personne), l'ADMIN DS 02 contacte ses correspondants (autorités nationales de sécurité) au sein des Etats membres pour savoir s'il existe des éléments défavorables à la venue de cette personne au sein de l'institution. En effectuant sa demande, la DS 02 précisera le contexte générale du dossier (le future poste, ses caractéristiques générales, etc). Pour cette procédure, la DS 02 travaille avec des informations de toute nature par opposition au "oui/non" reçu d'une autorité nationale de sécurité dans le cadre d'une procédure d'habilitation de sécurité. Tout screening est fondé sur une évaluation préalable des risques encourus pour l'institution. Cette évaluation est elle-même fonction du ou des pays-tiers possiblement concernés, de la conjoncture particulière liée, ainsi que des informations dont dispose la DS provenant des services partenaires des Etats Membres ou des autres Institutions. Il existe des critères d'évaluation qui sont classifiés (ils peuvent être par exemple liés à la situation politique particulière, à un conflit, ou des enjeux liés aux domaines de compétence concernés). C'est en fonction du risque que telle personne peut représenter pour l'Institution (aussi bien dans le domaine de la protection de l'information, du terrorisme ou du droit commun) que la décision est prise.

Il est également possible qu'une DG formule une demande de contrôle de sécurité pour le ressortissant d'un Etat membre. Cette demande se fait alors à l'initiative de la DG. L'ADMIN DS 02 décide ou non de lancer la procédure de screening en fonction des critères classifiés et de l'évaluation préalable, expliqués précédemment.

La procédure de screening découle du point 4.4 alinéa b de la partie I de la décision 2001/844/CE qui précise : "les mesures de sécurité doivent (...) être conçues de façon à permettre de repérer les personnes dont l'emploi pourrait nuire à la sécurité des informations classifiées et des installations importantes contenant de telles informations, et de les exclure ou de les changer de poste".

En fonction des éléments de réponses reçus, l'ADMIN DS 02 adresse les recommandations correspondantes aux Directions Générales l'ayant sollicitée. Ces recommandations peuvent être écrites ou orales ou concerner des conseils pratiques sur les mesures de sécurité supplémentaires à mettre en place. Cela peut aller jusqu'à la recommandation de ne pas recruter la personne. Ces recommandations sont destinées à être communiquées au Local Security Officer (LSO) ou bien à la personne responsable du recrutement.

L'analyse des informations résultant des enquêtes de sécurité et des contrôles de sécurité ("screening") permet également à l'unité ADMIN DS 02, de **produire des évaluations des menaces** pesant sur l'institution ainsi que des analyses de situations spécifiques.

3/ Autres informations concernant les enquêtes et contrôles de sécurité

Les procédures de traitement sont ***manuelles*** ou ***automatisées***. Les mécanismes de liaison avec les services de sécurité des Etats membres par exemple et les données qui en découlent sont automatisés mais une version papier des informations échangées peut aussi être éditée et archivée après circulation parmi les personnes habilitées.

Les ***personnes concernées*** par le traitement sont distinctes selon les deux procédures. En ce qui concerne les enquêtes de sécurité, il s'agit du personnel de la Commission et de toute personne qui pourrait constituer un risque pour la sécurité des personnels, des informations ou des biens de l'Institution, ceci incluant les visiteurs et les journalistes voire les parents d'un membre du personnel mais à l'exclusion des personnels des autres institutions européennes. En ce qui concerne la procédure de screening, il s'agit des personnes susceptibles d'être recrutées ou d'obtenir un contrat à la Commission, notamment des pays tiers, et représentant une menace pour l'institution.

Toute information pertinente relative à la menace considérée, notamment les ***données*** fournies par le Etats membres sont traitées. Ces informations peuvent inclure des données relevant de l'article 10 du règlement (CE) 45/2001 ("règlement"). La DS 02 peut demander l'accès aux bases de données de la Commission. Dans ce cas les données sont celles que gèrent les services de la Commission. L'Unité dispose également d'informations provenant des services de renseignement et de sécurité des Etats membres et dans ce cas les données transmises sont classifiées. Les aspects liés aux croyances religieuses, politiques, aux condamnations ou suspicions peuvent être concernés pour autant qu'ils participent au risque à évaluer ou aux besoins de l'enquête. S'agissant de l'accès aux données de contenu des communications électroniques, la DS 02 peut demander l'accès au contenu des échanges d'e-mails lorsqu'une enquête de sécurité est ouverte et avec l'autorisation du Directeur Général ADMIN et sous accord préalable du Délégué à la protection des données.

Les données sont ***conservées*** aussi longtemps que la menace est constituée pour l'institution et aussi longtemps que les demandes exprimées par les Etats membres peuvent concerner ces données. S'agissant des informations classifiées, il faut rappeler que leur traitement s'effectue en fonction d'une part des spécifications prévue par la Décision 844/2001 sachant que, d'autre part, toute décision affectant ces documents ne peut être prise sans l'accord du service d'origine du document. En ce qui concerne les screenings, le responsable du traitement précise

que ce traitement a été mis en place récemment et qu'ainsi aucune durée de conservation n'a encore été fixée. Le responsable projette d'établir une durée de conservation de 10 années. Si nécessaire, ***l'effacement*** et le ***verrouillage*** peuvent être réalisés dans un délai de 30 jours suivant une demande justifiée.

Les ***destinataires*** du traitement varient en fonction des catégories de données. Ainsi en matière d'enquête de sécurité les rapports d'enquête sont-ils adressés aux services concernés selon des résultats de l'enquête (IDOC, OLAF, AIPN concernée). Pour les demandes de "screening" les DGs à l'origine de la demande ne reçoivent que les recommandations appropriées au cas. D'autres interlocuteurs des Etas membres peuvent également être destinataires des données. Il s'agit des autorités judiciaires et des services de sécurité et de renseignement des Etats membres. Dans le cas de transfert aux autorités judiciaires (ce cas ne s'est à ce jour pas encore produit) l'ADMIN DS 02 envisage d'établir une décision motivée prouvant la nécessité du transfert.

Dans le cas des enquêtes de sécurité, les personnes concernées peuvent exercer leurs ***droits*** en s'adressant au responsable du traitement. Si une ou plusieurs des exceptions prévues à l'article 20 limitent l'application des articles 13 et 14, les personnes concernées peuvent demander la vérification du traitement par le CEPD comme prévu à l'article 20.4. du règlement.

Les personnes concernées sont ***informées*** de manière générale via la déclaration de confidentialité publiée sur le site de la Direction de la Sécurité ainsi que sur le portail Europa. Dans le cadre d'une enquête administrative de sécurité, tout personnel sollicité pour effectuer une déclaration reçoit systématiquement le texte de la déclaration de confidentialité spécifique au traitement. La déclaration de confidentialité expose le champ de compétence de l'unité ADMIN DS 02 (les finalités du traitement), cite le responsable du traitement et la base légale, mentionne les destinataires, le caractère obligatoire ou facultatif de la réponse aux questions, le délai de conservation des données, l'origine des données et les droits d'accès et de rectification de la personne concernée. Les personnes faisant l'objet d'un screening ne seront normalement pas informées, à moins qu'elles ne fassent par exemple un recours suite à un refus de recrutement auquel cas la DG justifierait son refus en évoquant les recommandations de la DS. La DS quant à elle utiliserait les exceptions prévues à l'article 20 du règlement si les menaces pesant sur l'institution sont toujours d'actualité.

Des ***mesures de sécurité*** ont été adoptées (...).

3. Aspects juridiques

3.1. Contrôle préalable

Le contrôle préalable porte sur le traitement de données à caractère personnel ("toute information concernant une personne identifié ou identifiable", article 2.a du règlement) dans le contexte des enquêtes de sécurité et "screening" effectués par l'unité ADMIN DS 02 de la Commission. Le traitement comprend des opérations de collecte, de consultation, de conservation, d'effacement, etc. de données à caractère personnel.

Le traitement est réalisé par une institution européenne et est mis en œuvre pour l'exercice d'activités relevant du champ d'application du droit communautaire. En effet, les activités misent en place par l'unité ADMIN DS 02 visent bien la gestion des menaces vis-à-vis des intérêts de la Commission dans les domaines de contre intelligence et contre terrorisme. La base juridique, analysée au point suivant, est pour une part la décision de la Commission du 29 novembre 2001 (2001/844/CE, CECA, Euratom). La Décision de la Commission du 31

janvier 2006 modifiant la décision 2001/844/CE, ajoute d'ailleurs un nouveau considérant après le considérant 7 de l'annexe. Il est libellé comme suit: "les présentes dispositions sont sans préjudice de l'article 286 du traité, ni du 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 des données".

Enfin, le traitement de données à caractère personnel est en grande partie automatisé (article 3.2 du règlement). Le règlement est donc applicable en l'espèce.

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 l'unité ADMIN DS 02.

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.

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 16 juillet 2008. 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 103 jours + le mois d'août. L'avis sera dès lors rendu le 28 janvier 2009 au plus tard.

3.2. Base juridique et licéité du traitement

Selon l'article 5, point a), du règlement, 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".* Les enquêtes et contrôles de sécurité menés par l'unité ADMIN DS 02 sont des missions d'intérêt public (lutte contre les menaces vis-à-vis des intérêts de la Commission dans les domaines de contre intelligence, contre terrorisme, protection des informations classifiées UE, etc.). En outre, l'unité ADMIN DS 02 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 traitement de données dans le cadre d'enquêtes de sécurité et de screening est fondé sur différents instruments législatifs allant du plus général au plus particulier.

Il s'agit tout d'abord de la Décision de la Commission n°844/2001 du 29 novembre 2001 relative aux dispositions de la Commission en matière de sécurité. L'article 5.2. précise l'organisation de la sécurité au sein de la Commission. En ce qui concerne les enquêtes de sécurité, l'article 24.2 portant sur la gestion des infractions à la sécurité et la compromission des informations classifiées de l'UE précise le rôle du responsable de la sécurité et de l'autorité de sécurité en de tels cas. En ce qui concerne la procédure de screening, l'article 4.4 portant sur les objectifs des mesures de sécurité stipule en son paragraphe b) :

Les mesures de sécurité doivent:

b) être conçues de façon à permettre de repérer les personnes dont l'emploi pourrait nuire à la sécurité des informations classifiées et des installations importantes contenant de telles informations, et de les exclure ou de les changer de poste;

La Décision de la Commission du 19 septembre 1994 relative aux missions du Bureau de sécurité ((Décision C(94) 2129) décrit de manière plus détaillée les tâches du bureau de sécurité, entre autres :

en son article 3 :

Ordinary tasks

The Security Office shall be responsible for the protection of persons, property and activities at the Commission.

Accordingly, its tasks shall include:
(a) gathering information to assess potential threats or risks to Commission departments;
(b) studying proposals and implementing security measures intended to combat such threats or risks;
(c) informing Commission staff of obligations with respect to security;
(d) monitoring compliance with current security rules by Commission departments;
(e) maintaining order in Commission buildings within the framework of the applicable laws;
(f) conducting investigations entrusted to it by the competent authority, or initiated on its own initative when offenders are caught in flagrante delicto, aimed at ensuring secure operating conditions in the Commission or at obtaining information relating to any illegal acts occurring in its departments for the purposes of a judicial inquiry or disciplinary action.

en son article 4 :

Special powers

1. In order to protect the security of Commission departments, the President may, if the circumstances so dictate, require the Security Office to perform the following tasks, while ensuring the due respect for human rights and fundamental freedoms that is incumbent on the European Communities :
(a) check the identity of persons entering a Commission building, and if appropriate refuse them access;
(b) check the identity of persons within Commission buildings;
(c) inspect items carried by persons entering or leaving Commission buildings;
(d) confiscate as a precautionary measure any documents or objects relevant to an administrative investigation;
(e) hear staff members, or, in conformity with the rules on confidentiality, inspect any internal

Commission documents in order to obtain information required for an administrative investigation.
2. Officials of the Security Office shall be authorized to carry a sidearm in accordance with the conditions laid down by the national laws in force, and in Commission buildings in accordance with the conditions laid down by the officers' superiors.
3. The Security Office may turn to a security firm to carry out, under the direction and the supervision of the Security Office, tasks relating to entry control.

Enfin en son article 6, la Décision prévoit :

The Security Office shall handle relations with :
(a) national security and intelligence services with a view to collecting the information required to assess potential threats and risks to the Commission;
(b) national authorities with respect to questions concerning the protection of Commission buildings, application of criminal laws and the immunity of officials from legal proceedings where matters of security are involved;
(c) the security services of other Community institutions with a view to developing a coordinated or common security policy.

Le traitement mis en place par l'unité ADMIN DS 02 de la Commission répond à des besoins de sécurité clairement énoncés dans les instruments juridiques précités, et repose donc sur une base légale conforme. Ceci vient à l'appui de la licéité du traitement.

Le CEPD souhaite cependant préciser que la base juridique de la procédure de screening est peu explicite et de nature assez générale. Sans remettre en cause la nécessité d'une telle procédure, le CEPD souhaiterait voir cette base juridique plus détaillée et couvrant un champ d'application plus large afin de couvrir toutes les possibilités de lancements d'une procédure de screening. En effet, la base juridique actuelle limite la procédure à "*la sécurité des informations classifiées et des installations importantes contenant de telles informations*". Or, la menace qui pèse sur l'institution et sur les Etats membres peut être de toute nature et pourrait concerner des informations/domaines non classifiés. Cette dimension devra être prise en compte dans l'élaboration de la nouvelle base juridique.

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 et des contrôles de sécurité doit être proportionné à l'objectif général du traitement (protéger les intérêts de l'institution et des Etats membres), 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 faisant 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. Sous réserve de cette analyse au cas par cas, la licéité du traitement proposé est respecté.

3.3. Traitement portant sur des catégories particulières de données

L'article 10, paragraphe 5, du règlement 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 probable que, si une exception devait s'appliquer, seul le point d. (*le traitement porte sur des données manifestement rendues publiques par la personne concernée ou est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice* (...)) serait éventuellement concerné.

Le type de données décrites à l'article 10, paragraphe 1, ne fera pas l'objet d'un traitement systématique mais va certainement apparaître dans le cadre des enquêtes et des procédures de screening. 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 de l'unité DS 02 chargée des dossiers ne doit pas perdre de vue qu'il s'agit là d'exceptions et qu'il s'agit d'éviter d'inclure des catégories particulières de données, à moins que la circonstance prévue à l'article 10, paragraphe 2, point d. ne soit présente dans l'affaire en cause ou qu'il ne soit nécessaire d'appliquer l'article 10, paragraphe 4 du règlement ("*Sous réserve de garanties appropriées, et pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphes 2 peuvent être prévues 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, sur décision du contrôleur européen de la protection des données*").

3.4. Qualité des données

Aux termes de l'article 4, paragraphe 1, point c) du règlement, 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 (nom, catégorie de personne, etc.) figureront de manière régulière dans la procédure de screening, le contenu exact des dossiers lui diffèrera naturellement selon les cas. Il en ira de même pour les dossiers d'enquêtes de sécurité. Il y a donc 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.

En ce qui concerne la procédure de screening, le CEPD se réjouit du fait que la DS 02 évalue préalablement à son lancement la demande de screening effectuée par une DG au moyen des critères classifiés dont elle dispose et évite ainsi la collecte de données excessives en entamant une procédure de screening non fondée. Le CEPD souhaiterait qu'il soit précisé dans la notice d'information que le déclenchement de la procédure de screening ne se fait qu'après l'évaluation (selon des critères spécifiques) de la demande de screening par la DS 02, afin de lever toute ambiguïté quant à l'apparent arbitraire du lancement d'une telle procédure (voir point 3.9).

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 à la personne visée 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 (voir le point 3.9 ci-dessous).

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 concernant les enquêtes de sécurité sont conservées aussi longtemps que la menace pèse sur l'institution et aussi longtemps que les demandes exprimées par les Etats membres peuvent concerner ces données. La DS.2 n'a donc pas établi de durée de rétention "limite" des données. Le CEPD comprend que cette analyse, dans le cas de dossiers par essence toujours particuliers, se fasse au cas par cas. Cependant, afin de s'assurer de la destruction effective des données lorsque la réalisation des finalités pour lesquelles elles ont été collectées est atteinte, le CEPD recommande de mettre en place une procédure permettant d'éviter que les données ne soient conservées plus longtemps que nécessaire.

En ce qui concerne les données relatives à la procédure de screening, le CEPD estime que la proposition faite par l'Unité ADMIN.DS 02 de conserver les données pour une durée de 10 ans est en conformité avec l'article 4 paragraphe 1, point e).

Par ailleurs, en vertu de l'article 37 §1, les données de trafic, à savoir les données qui sont nécessaires afin d'établir les communications, doivent être effacées ou rendues anonymes à la fin de la communication. Des exceptions à ce principe sont prévues par l'article 20 notamment lorsque cette exemption est nécessaire pour "garantir la protection de la personne concernée" ou "assurer la sécurité nationale, la sécurité publique et la défense des Etats membres".

Les données de trafic récoltées dans une enquête sont conservées comme les autres données aussi longtemps que la menace pèse sur l'institution en ce qui concerne les enquêtes et pour dix années en ce qui concerne les screenings. Cette conservation des données peut se fonder sur les exceptions prévues par l'article 20, le cas échéant.

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.

Si des données sont transférées à la suite d'une demande du destinataire, tant la DS 02 que le destinataire assument la responsabilité de la légitimité du transfert, conformément à l'article 7 paragraphe 2. La DS 02 est tenu de vérifier la compétence du destinataire et d'évaluer à titre provisoire la nécessité du transfert de ces données. Si des doutes se font jour quant à la nécessité de ce transfert, la DS 02 demande au destinataire un complément d'information.

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.

En outre, la DS 02 doit inclure dans le dossier une note faisant état du transfert des données.

Dans le cas sous analyse, les transferts sont de nature différente en fonction de la procédure envisagée. Les transferts dans le cadre des enquêtes de sécurité peuvent se faire vers l'IDOC, l'OLAF, l'AIPN concernée, alors que les transferts concernant la procédure de screening (sous forme de recommandations appropriées) se font au LSO ou au responsable recrutement du service concerné.

Dans le cas du screening, la DS 02 évalue en amont la nécessité de la demande de screening faite par la DG et limite les informations transmises à ce qui est strictement nécessaires (recommandations). Elle respecte ainsi les obligations prévues aux articles 7.1 et 7.2.

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 le secteur judiciaire et les autorités nationales de sécurité;

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 le secteur judiciaire et les autorités nationales de sécurité;

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 et de sécurité 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.

Bien qu'il appartienne au destinataire de démontrer l'intérêt et la nécessité de la réception des informations selon l'article 8, point a), le CEPD estime, compte tenu des activités propres de la DS 02, que cette disposition signifie que, si l'envoi des informations n'a pas lieu à la demande du destinataire, c'est à l'expéditeur qu'il appartient de vérifier cette nécessité. Par conséquent, si la DS 02 envoie, de sa propre initiative, des données à caractère personnel à des autorités nationales compétentes, il doit démontrer que les données sont nécessaires à l'exécution d'une mission effectuée dans l'intérêt public. La DS 02 doit procéder à cette évaluation chaque fois qu'il transfère des données à caractère personnel et établir une décision motivée exposant la nécessité du transfert. Le CEPD se réjouit du fait que la DS 02 envisage la rédaction d'une telle décision en cas d'un tel transfert aux autorités judiciaires dans le cadre des enquêtes de sécurité. Pour rappel, un tel transfert n'a pas encore eu lieu. Dans le cadre de la procédure de screening, la DS 02 respecte cette obligation car elle évalue en amont la nécessité de faire une demande aux autorités nationales de sécurité. Il est à noter que dans cette procédure, la demande d'information à l'autorité nationale de sécurité (accompagnée du nom de la personne, poste à pourvoir, ...) est le seul transfert qui ait lieu.

Pour les Etats membres qui n'ont pas étendu l'application de la directive 95/49/CE aux autorités judiciaires, de sécurité ou à d'autres autorités concernées par le traitement, 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

Dans l'hypothèse où des données personnelles seraient transférées aux autorités de pays tiers et/ou à des organisations internationales, l'article 9 du règlement 45/2001 s'applique. Le CEPD tient à souligner que ces transferts sont de nature exceptionnelle et que ce point est ajouté à l'analyse uniquement afin de couvrir toutes les éventualités du traitement. A ce jour, la DS 02 n'a pas d'exemple de tels transferts.

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 possibilité pour la DS.2 est de demander l'autorisation de transfert au CEPD, tel que prévu 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*".

En vertu de l'article 9.8, la DS.2 doit informer le CEPD des catégories de cas dans lesquels il a appliqué l'article 9.6 et 9.7. A cette 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 de l'autorisation accordée en vertu de l'article 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 CEPD est conscient du fait que la décision 2001/844/CE a prévu au point 26 de sa partie II les principes régissant la communication d'informations classifiées de l'UE à des Etats tiers ou à des organisations internationales. Le point 26.1.1. stipule entre autres "*l'acceptation par des Etats tiers ou des organisations internationales d'informations classifiées UE implique l'assurance que ces informations ne seront pas utilisées à d'autres fins que celles qui ont motivé leur communication ou les échanges d'informations, et qu'ils leur assureront la protection requise par le Commission*". Le CEPD relève ce point car il se réjouit que de tels transferts soient soumis aux conditions strictes de sécurité établies par la décision 2001/844/CE. Il précise cependant que ces transferts doivent aussi, comme expliqué ci-dessus, répondre aux conditions de protection des données prévues par le règlement 45/2001.

3.7. Confidentialité des communications

Conformément à l'article 36 du règlement (CE) n° 45/2001, "les institutions et organes communautaires garantissent la confidentialité des communications réalisées au moyen de réseaux de télécommunications et des équipements de terminaux dans le respect des principes généraux du droit communautaire".

Les communications électroniques (interceptées) dans le cadre d'enquêtes de sécurité relèvent de l'article 36 du règlement 45/2001 et toute limitation du principe de confidentialité doit se faire "dans le respect des principes généraux du droit communautaire". Le concept de "principes généraux du droit communautaire" fait référence aux droits de l'homme fondamentaux consacrés notamment par la Convention européenne des droits de l'homme.

Dans la pratique, cela signifie que toute limitation du principe de confidentialité des communications doit se faire dans le respect des droits de l'homme fondamentaux consacrés par la Convention européenne des droits de l'homme. Elle ne peut exister que si elle "est prévue par la loi" et "constitue une mesure qui, dans une société démocratique, est nécessaire" à la sécurité nationale, à la sûreté publique, à la défense de l'ordre et à la prévention des

infractions pénales, à la protection de la morale ou à la protection des droits et des libertés d'autrui.

Le fait que l'accord du délégué à la protection des données de la Commission soit requis lorsque les services compétents accèdent à des données de contenu sur le ou les postes de travail de la personne concernée constitue une garantie supplémentaire du respect de l'article 36 du règlement.

Le CEPD estime que l'obligation du respect de la confidentialité des communications ne peut être levée que dans des circonstances exceptionnelles, lors d'une investigation liée à une enquête de sécurité où aucun autre moyen moins invasif n'a pu être utilisé. En tout état de cause la levée du respect de la confidentialité des communications ne peut pas être une procédure ordinaire et elle doit toujours être limitée aux données strictement nécessaires.

3.8. Droit d'accès et de rectification

a) Enquêtes de sécurité

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[1]. 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 la 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 de cet avis, la personne concernée peut s'adresser au responsable du traitement pour exercer ses droits. Le CEPD comprend que ces deux droits peuvent être limités conformément à l'article 20 du règlement en certaines occasions (voir ci-dessous). Ces limitations doivent être "nécessaires" et en aucun cas devenir une règle générale. 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).

[1] 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).

L'article 20 du règlement prévoit donc certaines limitations, 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 "pré disciplinaire" ou "pré pénale". L'intérêt de l'autorité qui est censée suivre l'enquête (IDOC, OLAF, 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 la DS 02 : *"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 la DS 02 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[2].

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 de sécurité menées par la DS 02, ce droit revêt une importance cruciale pour garantir la qualité des données utilisées, laquelle est, en l'espèce, liée au droit de défense. Le droit de

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

rectification implique aussi que la rectification faite des données inexactes ou incomplètes soit communiquée aux tiers destinataires des données, conformément à l'article 17. 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.

b) Procédure de screening

Les articles 13 et 14 du règlement 45/2001 s'appliquent également à la procédure de screening. Vu la sensibilité des données traitées dans ce cadre, il est probable que les exceptions prévues à l'article 20 soient applicables. Le droit d'accès est cependant un principe fondamental qui doit être assuré à la personne concernée. Dès lors chaque demande d'accès doit être analysée au cas par cas et ne pas être refusée de manière systématique. Il ne peut être exclu en effet que la menace supposée se révèle infondée et que le droit d'accès direct puisse dès lors être accordé. Ce principe fondamental doit être exprimé dans l'information générale fournie aux personnes concernées même si la pratique verra les exceptions prévues à l'article 20 s'appliquer (voir le point 3.9).

3.9. Information de la personne concernée

a) Enquêtes de sécurité

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 ce qui concerne les enquêtes. 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 donné aux personnes concernées est décrit de manière détaillée au point 2.6. Il s'agit d'un document intitulé : déclaration de confidentialité - protection des données publié sur l'intranet de la Commission et sur le portail externe, Europa. Cette déclaration est également donnée à toute personne sollicitée pour effectuer une déclaration dans le cadre d'une enquête de sécurité. L'information se passe donc à deux niveaux en ce qui concerne les enquêtes de sécurité : général pour toute personne potentiellement concernée par le traitement et particulier lorsqu'une personne est directement impliquée dans une enquête de sécurité, le CEPD s'en réjouit.

En ce qui concerne le moment où ces informations doivent être fournies, lorsque les activités de renseignement sont menées dans le cadre d'une enquête, les informations doivent être données en temps opportun et donc à un moment où cela ne nuira pas à l'enquête. En effet, le moment où l'information est fournie peut être différent de celui du premier enregistrement ou de la première communication des données, compte tenu de l'article 20 du règlement (voir ci-après).

En ce qui concerne l'hypothèse où la DS 02 ne procède pas au recueil de la déclaration écrite et n'a aucun contact avec la personne avant de transmettre les données à un tiers (OLAF, IDOC, autorités nationales), la DS 02 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. 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 dans le respect des recommandations formulées par le CEPD dans son 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).

Comme précisé pour les droits d'accès et de rectification, le CEPD comprend que l'information de la personne concernée peut être limitée conformément à l'article 20 du règlement en certaines occasions (voir ci-dessus). Mais ces limitations doivent être "nécessaires". Le "critère de nécessité" doit être apprécié au cas par cas tout comme c'est le cas pour les droits d'accès et de rectification. L'information de la personne concernée devra être garantie lorsqu'elle ne risque pas de compromettre l'enquête. Les limitations au droit de l'information de la personne concernée ne doivent en aucun cas devenir une règle générale.

b) Procédure de screening

En ce qui concerne la procédure de screening, seul l'article 12 s'applique. En effet, les données ne sont jamais collectées auprès de la personne concernée.

Bien que la teneur des informations fournies dans la déclaration de confidentialité corresponde aux informations qui doivent être communiquées en vertu des articles 11 et 12, il ressort de l'analyse faite par le CEPD que l'information concernant la procédure de screening est trop vague pour assurer aux personnes concernées un traitement loyal (les personnes concernées par exemple ne sont pas uniquement des personnels contractuels). Les personnes concernées devraient recevoir de manière individuelle la déclaration de confidentialité ou à tout le moins un lien vers cette dernière (un lien vers la déclaration de confidentialité dans l'avis de recrutement pourrait par exemple être un moyen d'information général mais direct). En effet, la procédure étant a priori tout à fait inconnue des personnes concernées (il ne s'agit pas d'une procédure classique concernant le recrutement) pour laquelle ces dernières ne vont pas se renseigner "naturellement", il convient de leur fournir cette information de manière proactive. Cette information générale est d'autant plus importante qu'il n'est prévu aucune procédure d'information particulière pour la procédure de screening.

Le CEPD souhaite rappeler que les limitations prévues à l'article 20 ne peuvent être appliquées de manière systématique mais bien être traitées au cas par cas. La dernière phrase du point 1.2 de la déclaration devra être amendée en conséquence.

La partie consacrée au délai de conservation des données devra être amendée pour la procédure de screening en fonction de la durée adoptée par la DS 02. La partie consacrée à la base légale devra être adaptée en fonction des nouveaux textes adoptés.

3.10. Mesures de sécurité

Des mesures de sécurité ont été adoptées. Les conditions de protection des données et d'accès physiques sont celles requises par la Décision du Conseil du 29 novembre 2001 adoptant le règlement de sécurité du Conseil (2001/844/CE). De manière générale, les accès physiques et informatiques sont limités aux personnels disposant du besoin d'en connaître et des habilitations de sécurité correspondantes.

Au regard de l'ensemble des mesures de sécurité prises, le CEPD estime que celles-ci semblent adéquates au sens 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, la DG ADMIN DS doit:

- évaluer la proportionnalité des activités de traitement au cas par cas ;
- mettre en place une base juridique plus détaillée et couvrant un champ d'application plus large afin de couvrir toutes les possibilités de lancements d'une procédure de screening.
- mettre en place une procédure permettant d'éviter que les données ne soient conservées plus longtemps que nécessaire conformément à l'article 4.1.e ;
- 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 ;
- vérifier dans le cadre des enquêtes, la compétence du destinataire et d'évaluer à titre provisoire la nécessité du transfert de ces données lorsque le destinataire fait une demande de transfert, conformément à l'article 7.2 ;
- 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 ;
- inclure dans le dossier d'enquête une note faisant état du transfert des données ;
- 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 si de tels transferts devaient avoir lieu ;
- réviser la déclaration de confidentialité pour la partie screening,
- fournir aux personnes concernées par le screening la déclaration de confidentialité de manière proactive, conformément à l'article 12 ;
- ajouter la durée de conservation des données prévue pour la procédure de screening dans la déclaration de confidentialité ;
- dans le cadre des enquêtes, 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, le cas échéant.

Fait à Bruxelles, le 26 janvier 2009.

(signé)

Peter HUSTINX
Contrôleur européen de la protection des données