Avis rendu à la suite d'une notification en vue d'un contrôle préalable reçue du délégué à la protection des données de Commission européenne à propos des enquêtes de sécurité au Centre commun de recherche d'Ispra.

Bruxelles, le 31 juillet 2008 (dossier 2007-507)

1. Procédure

Le 3 septembre 2007, le Contrôleur européen de la protection des données (ci-après "le CEPD") a reçu du délégué à la protection des données de la Commission européenne ("DPD)" une notification en vue d'un contrôle préalable concernant les traitements de données effectués dans le cadre de la réalisation d'enquêtes de sécurité à la DG "Centre commun de recherche d'Ispra) (ci-après "CCR d'Ispra").

Le 28 septembre 2007, le CEPD a demandé au CCR d'Ispra des informations complémentaires. Pendant toute la durée de mai et de juin, le CEPD a reçu, dans le cadre d'autres contrôles préalables[1], des réponses à la plupart des questions adressées précédemment au CCR d'Ispra dans sa demande d'informations du 28 septembre 2007, qui lui ont permis de mettre au point un premier projet d'avis. Le 3 Juillet 2008, le CEPD a envoyé le projet d'avis au DPD pour avoir ses observations et pour clarifier certains points de fait en suspens. Une réponse à cet envoi a été reçue par le CEPD le 22 juillet 2008.

2. Examen du dossier

Au sein du CCR d'Ispra, l'unité C 7 est responsable, entre autres, de la sécurité des personnes, des locaux et des informations du CCR d'Ispra. Au sein de cette unité, le service de sécurité (le "SeS") met en oeuvre les politiques et procédures instaurées dans le but d'assurer la sécurité générale du CCR d'Ispra. Le SeS est notamment responsable de la protection des personnes, des locaux et des informations relevant de la Commission et se trouvant au CCR d'Ispra contre les accès non autorisés, les intrusions ou d'autres atteintes. Afin de remplir cette tâche, le SeS effectue des enquêtes portant sur les incidents liés à la sécurité, tels que les accidents de la circulation, les actes de vandalisme, les vols, les accès non autorisés, etc., dans le cadre desquelles des données à caractère personnel font l'objet d'un traitement. Les résultats des enquêtes donnent lieu à un rapport qui décrit les faits survenus. En cas d'atteinte à la sécurité, le SeS limite les dommages, sauvegarde les éléments de preuve et informe al direction de la sécurité, qui décidera comment l'enquête doit être menée.

[1] Notification en vue d'un contrôle préalable reçue du délégué à la protection des données de la Commission européenne concernant la base de données ARDOS (dossier 2007/380) et notification en vue d'un contrôle préalable reçue du délégué à la protection des données de la Commission européenne concernant les enquêtes de sécurité réalisées par la DG ADMIN (dossier 2007-736).

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

Le contrôle préalable qui fait l'objet du présent avis vise à déterminer si le traitement de données effectué par le SeS à l'occasion de la réalisation des enquêtes de sécurité et de l'élaboration des rapports susmentionnés est conforme au règlement (CE) nº 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (ci-après "le règlement (CE) nº 45/2001"). Il ne vise pas à déterminer la conformité, au regard de la protection des données, de procédures pouvant intervenir à la suite de la rédaction du rapport.

2.1 Les faits

La **finalité du traitement** est d'obtenir des informations concernant les incidents tels que les accidents de la circulation, les manquements à la sécurité, les vols, les accès non autorisés, etc., survenus dans les locaux du CCR d'Ispra, l'objectif final étant la rédaction d'un rapport sur les faits survenus. Le rapport vise à identifier les auteurs des actes concernés ainsi qu'à limiter et quantifier les dommages éventuels.

Le directeur du site du CCR d'Ispra ou le directeur général du CCR peuvent décider d'interdire à une personne l'accès d'un site du CCR à la suite de la rédaction d'un rapport attestant qu'un acte répréhensible a été commis. Cette décision est communiquée à la personne concernée et au SeS par lettre signée par l'autorité qui en est à l'origine.

La **responsabilité du traitement des données** incombe au **premier chef** à l'unité C 7 du CCR d'Ispra, qui est responsable, entre autres, des opérations de sécurité du CCR d'Ispra. Plus particulièrement, au sein de ladite unité, le responsable du traitement des données effectué dans le cadre de la réalisation des enquêtes de sécurité est le chef de secteur compétent pour assurer la direction des activités du service de sécurité ("SeS") du CCR d'Ispra. La plupart des traitements de données effectués à l'occasion de la réalisation d'enquêtes de sécurité sont réalisés par le SeS.

Dans le cadre de la réalisation d'enquêtes de sécurité, il y a interconnexion entre les **traitements de données *automatique* et *manuel***. Lorsqu'un incident s'est produit, un dossier papier est élaboré ; il regroupe les plaintes, témoignages, déclarations et les éléments de preuve tels que des photographies. Ce dossier papier est on outre complété par des informations extraites de différentes bases de données telles que SECPAC et ARDOS, des enregistrements de vidéosurveillance et d'autres informations susceptibles d'être utiles. La partie finale du rapport énoncera les principales conclusions de l'enquête. Le rapport sera conservé aussi bien sur support papier que dans la base de données ARDOS[2].

Le traitement des données porte sur les **catégories** ci-après **de personnes concernées**: *i)* toute personne faisant l'objet d'une enquête et *ii)* les personnes qui coopèrent à l'enquête, par exemple les témoins ou d'autres catégories de collaborateurs.

Ces personnes concernées peuvent être soit des membres du personnel du CCR d'Ispra, soit des tiers. Le personnel du CCR d'Ispra comprend les membres du personnel en activité, tels que les fonctionnaires, les agents temporaires et les agents contractuels ainsi que le personnel extérieur travaillant sous contrat. Il peut également s'agir de fonctionnaires retraités. Les tiers peuvent être des visiteurs ou toute autre personne s'adressant à l'unité C 7 du CCR d'Ispra. Il peut s'agir, entre autres, de personnes qui contactent le SeS par courrier électronique, téléphone, télécopieur, etc., parce qu'elles sont victimes, témoins ou auteurs d'un incident lié à la sécurité.

[2] Une notification en vue d'un contrôle préalable reçue du délégué à la protection des données de la Commission européenne à propos de la base de données ARDOS est actuellement à l'examen du CEPD (dossier 2007/380).

S'agissant des catégories de données à caractère personnel, les données à caractère personnel collectées comprennent, d'une part, les informations relatives à l'incident survenu. Il peut s'agir, selon le cas, d'une description de l'incident, du lieu, de l'heure et de la date, ainsi que des éléments de preuve à l'appui tels que des photographies, des enregistrements de vidéosurveillance, etc. Les informations relatives à la personne à laquelle il est reproché d'avoir provoqué l'incident de sécurité ou qui sont impliquées dans ledit incident sont également collectées. Ces informations peuvent inclure le nom, la date et le lieu de naissance, la nationalité, le sexe, le type de contrat, les détails du contrat de travail, le type d'autorisation d'entrée dans les locaux, y compris les dates de début et de fin de validité, l'adresse privée, le téléphone et l'adresse e-mail.

Les sources d'information sont multiples et comprennent notamment le contenu des différentes bases de données, telles qu'ARDODS et SECPAC . Les informations collectées peuvent aussi émaner des enregistrement de vidéosurveillance, des témoins ou d'autres collaborateurs, ainsi que de la personne soupçonnée.

Les périodes de conservation varient en fonction des résultats de l'enquête. Les informations concernant les cas donnant lieu à l'application de mesures concrètes, telles que l'interdiction d'accès à un site ou à une zone spécifique sont conservées jusqu'à ce que la mesure applicable doive être exécutée. La période maximale de conservation des informations est de cinq ans.

Les rapports concernant les enquêtes de sécurité et les informations connexes donnant lieu à un dossier géré dans le cadre des dispositions de droit pénal sont conservées pendant une durée maximale de dix ans à compter de la date de clôture de l'enquête.

Les rapports aboutissant à la conclusion que l'incident n'était pas un acte illicite ou qu'il n'a pas donné lieu à l'application d'une mesure concrète sont conservés 12 mois après clôture du dossier afin d'évaluer, à très court terme, la réapparition de ce type d'incident ou l'apparition de profils particuliers d'incidents.

Selon la notification, les données peuvent être ***transférées*** aux services concernés sur la base du besoin d'en connaître. Au sein de la Commission, les données peuvent être transférées à la DG ADMIN/Sécurité, à l'OLAF et à l'IDOC. Le rapport et les pièces justificatives peuvent également être transférés aux services répressifs nationaux ou aux autorités judiciaires nationales.

En ce qui concerne le ***droit à l'information***, la notification comporte en annexe une déclaration de confidentialité destinée à fournir des informations aux personnes concernées. La déclaration de confidentialité sera publiée sur le site intranet du CCR d'Ispra. La déclaration de confidentialité n'est pas fournie directement aux personnes concernées, ni aux personnes agissant en tant que témoins ou collaborateurs, pas plus qu'aux personnes accusées d'avoir commis des actes répréhensibles.

La déclaration de confidentialité contient des informations relatives à l'identité du responsable du traitement des données, aux destinataires des données, à l'existence d'un droit d'accès et d'un droit de rectification, y compris le nom de la personne à contacter pour pouvoir exercer ces droits. Elle indique également les délais de conservation des données et rappelle le droit de recourir au Contrôleur européen de la protection des données.

Quant au ***droit d'accès et de rectification***, la déclaration de confidentialité stipule que les personnes concernées disposent de ces droits à l'égard des informations les concernant détenues par le SeS. Elle fournit le nom et l'adresse électronique de la personne à contacter pour exercer ces droits et à laquelle s'adresser pour poser toute question complémentaire concernant le traitement des données à caractère personnel les concernant.

Le CEPD note que le SeS a mis en oeuvre des ***mesures de sécurité***. Les mesures de sécurité utilisées pour conserver le rapport dans la base de données ARDOS font actuellement l'objet d'un examen dans le cadre de l'avis en vue d'un contrôle préalable concernant ARDOS. S'agissant des mesures de sécurité appliquées à la version papier du document, la notification fait référence à des mesures de sécurité exceptionnelles visant à limiter et contrôler l'accès aux secteurs où sont stockés les rapports et les pièces justificatives.

2.2 Aspects juridiques

2.2.1 Contrôle préalable

Le règlement nº 45/2001 CE) relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (ci-après "le règlement (CE) nº 45/2001") s'applique au "*traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier*" et au traitement de données à caractère personnel "*par toutes les institutions et tous les organes communautaires, dans la mesure où ce traitement est mis en oeuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire"*[3].

Pour les raisons exposées ci-après, le CEPD estime que tous les éléments qui déclenchent l'application dudit règlement sont présents dans le traitement des données effectué par le SeS :

En premier lieu, dans le cadre de la réalisation d'enquêtes relatives à différentes sortes d'accidents, des *données à caractère personnel* telles qu'elles sont définies à l'article 2, point a), du règlement (CE) nº 45/2001 font l'objet d'un traitement. En effet, comme l'indique la notification, les données à caractère personnel de personnes intervenant dans l'incident de sécurité (auteurs présumés, témoins, etc.) seront collectées. En deuxième lieu, les données à caractère personnel collectées font l'objet de traitements automatisés ou non automatisés tels que définis à l'article 2, point b), du règlement (CE) nº 45/2001. Par exemple, lorsqu'on établit un rapport sur la base d'informations extraites de bases de données telles que SECPA ou ARDOS, ou d'enregistrements de vidéosurveillance etc., qui sont ultérieurement stockées dans une base de données électronique, des données à caractère personnel font l'objet d'un traitement. Enfin, le CEPD confirme que le traitement est effectué par une institution communautaire, en l'occurrence le Centre commun de recherche d'Ispra, qui fait partie de la Commission européenne et relève du droit communautaire (article 3, paragraphe 1, du règlement (CE) nº 45/2001. Dès lors, il est clair que tous les éléments qui déclenchent l'application dudit règlement sont présents dans les traitements mis en œuvre pour réaliser des enquêtes de sécurité au CCR d'Ispra.

Évaluation visant à établir si les traitements des données relèvent de l'article 27 du règlement.
L'article 27, paragraphe 1, du règlement (CE) nº 45/2001 soumet au contrôle préalable du CEPD "*les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités*". L'article 27, paragraphe 2, comporte une liste des traitements susceptibles de présenter de tels risques. Le CEPD considère que le traitement des données en cause relève du cas prévu à l'article 27, paragraphe 2, du règlement (CE) nº 45/2001.

Tout d'abord, de l'avis du CEPD, ces traitement des données relèvent de l'article 27, paragraphe 2, point a), du règlement (CE) nº 45/2001, lequel prévoit que les traitements de données relatives à "*des suspicions, infractions, condamnations pénales ou mesures de sûreté"* sont soumis au contrôle préalable du CEPD. Dans le présent dossier, en menant des enquêtes sur des incidents tels que des accidents, des manquements à la sécurité, des vols, des accès non autorisés, le SeS traitera des informations susceptibles d'être liés à des présomptions d'infractions ou de délits ou d'autres fautes graves. Cela est confirmé en outre si l'on tient compte du fait que la finalité du traitement est l'élaboration d'un rapport décrivant les faits survenus puis la communication de ce rapport aux autorités répressives et aux autorités judiciaires.

Le CEPD estime en outre que la notification relève également de l'article 27, paragraphe 2, point b), du règlement (CE) nº 45/2001, qui prévoit que les traitements destinés à "*évaluer des aspects de la*

[3] Extrait de l'article 3, paragraphe 2, du règlement (CE) nº 45/2001.

personnalité des personnes concernées, tels que leur (…) comportement" sont soumis au contrôle préalable du CEPD. Dans le présent dossier, il est certain que le comportement des personnes sera évalué afin d'établir leur participation à certains faits, déclenchant ainsi l'application de l'article 27, paragraphe 2, point b).

Contrôle préalable effectué a posteriori. 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.

Notification et date prévue pour l'avis du CEPD. La notification du DPD a été reçue le 3 septembre 2007. Le délai de deux mois au cours desquels le CEPD est tenu de rendre un avis a été suspendu pendant 299 jours pour obtenir des informations supplémentaires et permettre au DPD et au responsable du traitement de présenter des observations sur le projet d'avis du CEPD. L'avis sera donc adopté au plus tard le 29 septembre 2008 (compte tenu du fait que le mois d'août ne compte pas).

2.2.2 Licéité du traitement

Les données à caractère personnel ne peuvent faire l'objet d'un traitement que sur la base des fondements juridiques visés à l'article 5 du règlement (CE) n 45/2001.

Comme l'indique la notification, parmi les différents motifs énumérés dans ledit article, les traitements notifiés en vue d'un contrôle préalable relèvent de l'article 5, point a), selon lequel les données ne peuvent être traitées 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*".

Afin de déterminer si les traitements sont conformes à l'article 5, point a), du règlement (CE) nº 45/2001, trois éléments sont à prendre en considération : il convient de se demander, premièrement, si le traité ou d'autres actes législatifs prévoient les traitements effectués par l'unité C 7 du CCR d'Ispra, et notamment par le SeS ; deuxièmement, si les traitements sont effectués dans l'intérêt public; et troisièmement, si les traitements sont nécessaires. Evidemment, les trois questions sont étroitement liées.

Fondements juridiques pertinents figurant dans le traité ou dans d'autres actes législatifs. Le CEPD prend note de l'éventail d'instruments juridiques exposés ci-après qui, tant d'un point de vue général que d'un point de vue plus spécifique, fournissent les fondements juridiques qui confèrent un caractère légitime aux traitements réalisés dans le cadre d'enquêtes.

En premier lieu, le règlement nº 3 du Conseil de la Communauté Européenne de l'Énergie Atomique, du 31 juillet 1958 détermine, entre autres, les mesures de sûreté à appliquer aux informations traitées par la Communauté. Il prévoit également la création d'un bureau de sécurité et d'agents de sécurité. En deuxième lieu, la décision de la Commission du 29 novembre 2001 prévoit également une structure similaire comprenant un bureau de sécurité de la Commission et, au niveau des services de la Commission, des responsables locaux de sécurité. La décision comporte en outre les dispositions de la Commission en matière de sécurité. Ces dispositions énoncent, entre autres, les principes de base et les normes de sécurité. En troisième lieu, la décision de la Commission C(94) 2129 du 8 septembre 1994 énonce les tâches du bureau de sécurité. Parmi les tâches ordinaires à accomplir par le bureau de sécurité, la décision mentionne le maintien de l'ordre dans les bâtiments de la Commission (article 3, point a), ainsi que les enquêtes qui lui sont confiées par l'autorité compétente ou ouvertes de sa propre initiative lorsque les auteurs d'infractions sont surpris en flagrant délit (article 3, point f). Ces enquêtes ont pour but d'assurer des conditions de sécurité

dans le fonctionnement des services au sein de la Commission ou d'obtenir des informations relatives à tout acte illicite survenant dans ses services, aux fins d'enquête judiciaire ou d'action disciplinaire. Enfin, l'énoncé de mission ("mission statement") du Service de sécurité du CCR d'Ispra énonce les tâches du Service de sécurité du CCR d'Ispra. Entre autres tâches qui y sont énumérées, il est prévu que le Service de sécurité mènera des investigations et des enquêtes concernant les questions liées à la sécurité, telles que des incidents, des vols, des actes de vandalisme, des accidents de la route, une utilisation abusive des TIC[4], etc.

Le CEPD considère que, tant d'un point de vue général que d'un point de vue plus spécifique, les fondements juridiques énoncés plus haut prévoient l'existence d'un Service de sécurité de la Commission, doté d'un bureau central et de bureaux locaux tels que celui du CCR d'Ispra. Lesdits fondements juridiques prévoient également le type de traitements décrits dans la notification. En effet, les actes juridiques susmentionnés permettent au Service de sécurité de la Commission d'effectuer des traitements visant à obtenir des informations dans le but d'assurer des conditions de sécurité dans le fonctionnement des services de la Commission et d'obtenir des informations relatives à tout acte illicite survenant dans ses services, aux fins d'enquête judiciaire ou d'action disciplinaire. Dans cette optique, le CEPD estime que lesdits actes juridiques constituent des fondements juridiques valables conférant un caractère légitime aux traitements de données effectués dans le but de découvrir des informations relatives à des incidents survenus dans les locaux du CCR d'Ispra.

Le CEPD constate toutefois que le cadre juridique exposé plus haut ne donne pas une image parfaitement claire des tâches concrètes et des compétences propres au bureau de sécurité de la Commission (DG ADMIN, direction de la sécurité) et de celles qui sont dévolues aux bureaux de sécurité existant au niveau des institutions, des services et des département, tels que le bureau de sécurité du CCR d'Ispra. À cet égard, la question se pose de savoir si le Service de sécurité du CCR d'Ispra est habilité à effectuer les traitements de données visant à obtenir les informations ou si cette tâche relève seulement de la compétence du bureau de sécurité de la Commission (DG ADMIN).

Compte tenu du caractère sensible des informations collectées, il apparaît nécessaire d'avoir une certitude absolue quant à l'institution ou à l'organe habilité à exercer les activités en question. Le CEPD appelle donc le CCR d'Ispra, en liaison avec la DG ADMIN, à clarifier ce point. Si le SeS du CCR d'Ispra est effectivement compétent pour mener des enquêtes de sécurité, le CEPD demande au CCR d'Ispra et à la DG ADMIN d'envisager l'éventualité d'adopter des fondements juridiques supplémentaires établissant clairement les compétences du Service juridique du CCR d'Ispra et confirmant sa compétence, conjointement avec la DG ADMIN, pour mener des enquêtes relatives aux incidents et élaborer des rapports sur leur survenance.

Les traitements sont effectués dans l'intérêt du public. Le CEPD note que le CCR d'Ispra, et notamment le SeS, effectue les traitements dans l'exercice légitime de l'autorité publique dont il est investi. Comme l'indique l'énoncé de mission du SeS, ce service est habilité à mener des enquêtes et est tenu de le faire avec l'objectif général de protéger les personnes, les biens et les activités relevant du CCR d'Ispra. Compte tenu de la nature de ces activités, il est clair que qu'elles sont exercées dans l'intérêt public pour autant qu'il soit dans l'intérêt public d'enquêter sur l'identité de l'auteur des incidents et d'empêcher à l'avenir la répétition des mêmes faits..

Critère de la nécessité. pour mener des enquêtes visant à trouver des informations sur des incidents liés survenus dans les locaux du CCR d'Ispra, il apparaît nécessaire de traiter des données à caractère personnel. Si l'on ne procède pas au traitement de ces données, le CCR ne sera pas en mesure de s'acquitter de ses tâches. Ainsi, dans une perspective générale, le traitement apparaît nécessaire aux fins de la réalisation des enquêtes. Cela dit, il convient de tenir compte du fait que la "nécessité" du traitement des données doit être également être analysée i*n concreto* pour chaque cas particulier et, en l'espèce, pour chaque enquête spécifique. Dans cette optique, il ne faut pas oublier que le traitement de données à caractère personnel à effectuer dans le cadre du traitement

[4] Communication au personnel nº 45/2006, du 15 septembre 2006, régissant l'utilisation acceptable des services TIC de la Commission (équipement informatique, courrier électronique et système d'accès internet, téléphone, téléfax et gsm) http://intracomm.cec.eu-admin.net/guides/publications/infoadm/2006/ia06045_fr.html

d'informations relatives à des incidents déterminés doit être doit être proportionné à l'objectif général du traitement (qui est d'assurer la sécurité des personnes et des bâtiments) ainsi qu'à l'objectif particulier du traitement dans le contexte du dossier en cause. La proportionnalité doit dès lors être évaluée au cas par cas.

2.2.3. Traitement portant sur des catégories particulières de données catégories

La finalité du traitement étant de faciliter la collecte d'informations sur les incidents donnant lieu à des présomptions d'actes répréhensibles, ces informations devraient se rapporter dans un certain nombre de cas à des infractions, des condamnations pénales ou des mesures de sûreté. À cet égard, le CEPD rappelle l'article 10, paragraphe 5, du règlement, qui stipule que *"le 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"*. Dans le présent dossier, le traitement des données mentionnées est autorisé par les actes législatifs visés au point 2.2.2 ci-dessus.

En ce qui concerne les catégories particulières de données, l'article 10, paragraphe 1, du règlement stipule que "*le traitement des données à caractère personnel révélant 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 sont interdits*".

Il ne ressort pas de la notification aux fins de contrôle préalable que les données relevant des catégories visées à l'article 10, paragraphe 1, du règlement (CE) nº 45/2001 soient traitées dans le cadre des enquêtes. Compte tenu de l'objectif général poursuivi par l'unité C 7 du CCR d'Ispra lorsqu'elle effectue des traitements de données, le CEPD croit comprendre que la collecte de catégories particulières de données n'est pas l'objectif principal de l'unité C 7 du CCR d'Ispra.

Le CEPD estime toutefois que, dans le cadre des enquêtes, l'unité C 7 du CCR d'Ispra peut entrer en possession, peut-être involontairement, de catégories particulières de données, qui ne seront souvent d'aucun intérêt/importance pour l'enquête. À cet égard, le CEPD rappelle le principe de la qualité des données, selon lequel les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et/ou pour lesquelles elles sont traitées ultérieurement (article 4, paragraphe 1, point c)). Conformément à ce principe, si des catégories particulières de données qui ne sont à l'évidence pas pertinentes pour les finalités d'une enquête sur un incident sont collectées, celles-ci ne devraient pas être mentionnées dans le rapport écrit. Il convient de veiller à ce que les responsables de la sécurité soient informés de cette règle.

2.2.4 Qualité des données

Conformément à l'article 4, paragraphe 1, point c) du règlement (CE) nº 45/2001, les données à caractère personnel doivent être *"adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et/ou traitées ultérieurement"*. C'est ce que l'on appelle le principe de la qualité des données.

Si certaines données types, telles que le nom, la date de naissance etc. figurent de manière systématique dans les enquêtes relatives à des incidents, le contenu exact d'un dossier différera naturellement selon les cas. Il y a toutefois lieu de prévoir des garanties pour veiller au respect du principe de la qualité des données. Par exemple, la décision d'ouvrir une enquête à la suite d'une demande de renseignements devrait définir l'objet et l'étendue de l'enquête. Cela contribuerait à limiter les informations collectées à celles qui relèvent de l'enquête. Le CEPD considère qu'il convient de donner aux enquêteurs, avant le début de l'enquête, des instructions citant l'article 4, paragraphe 1, point c), du règlement (CE) n° 45/2001 afin de les encourager à faire preuve d'une plus grande prudence à l'égard de la collecte de preuves ou de données dans un dossier d'enquête. Le personnel appelé à mener les enquêtes administratives et à établir les rapports doit être informé de ces instructions et s'y conformer.

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"*.

Ce principe est étroitement lié à l'exercice du droit d'accès, de rectification, de verrouillage et d'effacement (voir le point 2.2.7 ci-après). En outre, un système d'enquête garantissant la prise en compte des éléments de preuve à charge et à décharge présente un intérêt pour l'exactitude et l'exhaustivité des données traitées. En conséquence, et compte tenu de son importance du point de vue de la qualité des données, le CEPD recommande d'informer de ce principe les responsables de la sécurité.

2.2.5. Conservation des données

Conformément à l'article 4, paragraphe 1, point e), du règlement (CE) n° 45/2001, les données à caractère personnel peuvent être conservées sous une forme permettant l'identification des personnes concernées "*pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont collectées et/ou pour lesquelles elles sont traitées ultérieurement*."

La durée de conservation varie selon les catégories de données. Le CEPD considère que la période de conservation de cinq ans pour les données relatives aux cas ayant donné lieu à l'application de mesures concrètes (comme l'interdiction d'accès à un site ou à un secteur particulier) est satisfaisante. Le CEPD juge également satisfaisante la durée de 10 ans applicable aux informations relatives à des cas ayant donné lieu à un dossier à gérer dans le cadre du droit pénal. Ce délai tient compte de la période nécessaire au titre de la législation nationale pour que les infractions soient effacées des fichiers.

Les rapports permettant de conclure que les faits survenus ne constituaient pas des actes répréhensives ou qu'ils n'ont pas donné lieu à l'application de mesures concrètes sont conservés douze mois après qu'ils ont été clôturés afin d'évaluer, à très court terme, la réapparition de ce type d'incidents ou l'apparition de profils particuliers d'incidents. Le CEPD estime que cette durée de conservation est elle aussi satisfaisante.

2.2.6 Transfert de données

Les articles 7, 8 et 9 du règlement (CE) n° 45/2001 prévoient certaines obligations, qui s'appliquent lorsque les responsables du traitement communiquent des données à caractère personnel à des tiers. Les règles diffèrent selon qu'il s'agit d'un transfert, au titre de l'article 7 du règlement, vers des institutions ou organes communautaires, au titre de l'article 8, vers des destinataires relevant de la directive 96/46/CE ou, au titre de l'article 9, vers d'autres types de destinataires.

Transferts de données à caractère personnel entre institutions ou organes communautaires ou en leur sein. Les faits décrits dans les notifications effectuées en vue d'un contrôle préalable révèlent que les données sont communiquées à des institutions ou organes communautaires tels que l'OLAF, l'IDOC ou la direction"sécurité" de la DG ADMIN.

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."*

Selon la notification, les rapports et les documents connexes (données à caractère personnel) ne sont communiqués aux institutions ou organes communautaires susmentionnés que si nécessaire et sur la base du besoin d'en connaître. Compte tenu des compétences des organes destinataires, il apparaît

que les transferts sont nécessaires à l'exécution légitime de missions relevant de la compétence des destinataires. Il convient, à cet égard, de prendre en considération le critère de proportionnalité, compte tenu, par exemple, de la nature des données collectées et traitées ultérieurement, ainsi que de la compétence du destinataire.

En tout état de cause, il y a lieu d'informer le destinataire que les données à caractère personnel ne peuvent être traitées qu'aux fins pour lesquelles elles ont été transmises.

Transfert de données à caractère personnel aux États membres. Selon la notification, les données peuvent être transférées aux services répressifs et judiciaires des 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 dans son droit national, 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.

Étant donné que, en l'espèce, les données ne sont pas demandées par le destinataire, mais que le transfert est décidé unilatéralement par l'unité 7 du CCR d'Ispra, cette dernière doit établir la "nécessité" du transfert dans une décision motivée. Aux fins de la mise en œuvre de cette règle, et comme il a été suggéré plus haut pour ce qui concerne les transferts de données aux institutions et organes communautaires, le CEPD recommande que les enquêteurs de l'unité 7 du CCR d'Ispra suivent la même approche que dans le cadre de l'article 7 du règlement (CE) n° 45/2001 et que, dans un avis motivé, ils dressent la liste de tous les transferts de données qui seront effectués ou qui l'ont été dans le contexte d'un cas précis, et qu'ils en décrivent la nécessité. Ces procédures devraient être communiquées aux enquêteurs.

2.2.7 Droit d'accès et de rectification

Le droit d'accès est le droit de la personne concernée d'être informée de toute donnée la concernant qui est traitée par le responsable du traitement. Conformément à l'article 13 du règlement (CE) n° 45/2001, 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. Ces informations peuvent donc être obtenues directement par la personne concernée (ce qu'on appelle "l'accès direct") ou, dans certaines circonstances, par une autorité publique (ce qu'on appelle "l'accès indirect", qui est généralement exercé par une autorité chargée de la protection des données, soit le CEPD dans le cas présent).

La déclaration de confidentialité stipule que les particuliers disposent de ces droits à l'égard des informations les concernant détenues par l'unité C 7du CCR d'Ispra. Elle donne une adresse fonctionnelle de courrier électronique qui est celle de la personne à contacter pour demander à exercer ces droits. La pratique telle que décrite dans la déclaration de confidentialité est conforme à l'article 13 du règlement (CE) nº 45/20001.

Cette déclaration ne prévoit pas la possibilité, dans certains cas, de reporter l'obligation de prévoir un accès ou une rectification afin de préserver l'enquête. Toutefois, dans certains cas, l'unité C 7 du CCR d'Ispra peut se prévaloir de certaines des exceptions prévues à l'article 20, paragraphe 1, du règlement (CE) n° 45/2001 pour reporter ce droit. Cela peut notamment être licite lorsqu'une telle

limitation "*constitue une mesure nécessaire pour sauvegarder* (…) *a) la prévention, la recherche, la détection et la poursuite d'infractions pénales* ; l'unité C 7 du CCR d'Ispra peut également se prévaloir de l'article 20, paragraphe 1, point c), pour retarder l'octroi de l'accès si elle estime nécessaire de reporter la fourniture des informations afin de garantir "*la protection de la personne concernée ou des droits et libertés d'autrui*", par exemple si elle considère que la divulgation d'informations peut révéler l'identité du dénonciateur ou de l'informateur, ce qui peut être le cas dans un certain nombre de dossiers. Pour déterminer si elle doit se prévaloir d'une exception, l'unité C 7 du CCR d'Ispra doit réaliser une évaluation au cas par cas des circonstances qui entourent le traitement des données en jeu.

Si l'unité C 7 du CCR d'Ispra se prévaut d'une exception pour reporter la fourniture d'informations, elle ne devrait pas perdre de vue que les limitations d'un droit fondamental ne peuvent être appliquées de manière systématique. L'unité C 7 du CCR d'Ispra doit évaluer dans chaque cas si les conditions sont réunies pour appliquer une des exceptions prévues, par exemple, à l'article 20, paragraphe 1, point a) ou c). Par ailleurs, comme l'indique l'article 20, la mesure doit être "nécessaire". Pour ce faire, il faut que le "test de nécessité" soit réalisé au cas par cas. Si l'unité C 7 du CCR fait valoir une exception, elle doit le faire dans le respect de l'article 20, paragraphe 3, aux termes duquel *"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*". Toutefois, l'unité C 7 du CCR peut reporter la fourniture de ces informations en se prévalant de l'article 20, paragraphe 5, aux termes duquel *"la fourniture des informations visées aux paragraphes 3 et 4 peut être reportée aussi longtemps qu'elle prive d'effet la limitation imposée sur la base du paragraphe 1"*.

Par ailleurs, il convient de tenir dûment compte du fait que le traitement loyal de données à caractère personnel dans le cadre d'une enquête ou d'une procédure judiciaire ultérieure implique l'exercice des droits de la défense. Pour exercer ces droits, la personne concernée doit normalement être en mesure de savoir qu'une procédure a été ouverte à son encontre. Toute exception doit donc être strictement limitée et adoptée au cas par cas.

2.2.8 Information de la personne concernée

Conformément aux articles 11 et 12 du règlement (CE) n° 45/2001, les responsables qui collectent des données à caractère personnel sont tenus d'informer les personnes concernées du fait que leurs données sont collectées et traitées. Les personnes concernées ont en outre le droit d'être informées, entre autres, des finalités du traitement, des destinataires des données et des droits particuliers auxquels elles peuvent prétendre en tant que personnes concernées.

Pour évaluer si le responsable du traitement des données fournit bien en l'espèce les informations en question à la personne concernée, il faut examiner deux questions : tout d'abord dans quelle la mesure les informations ont été effectivement fournies d'une manière qui permette à la personne concernée de lire et de stocker les informations pour les relire ultérieurement et, deuxièmement, dans quelle mesure les informations fournies et leur contenu sont conformes au règlement (CE) nº 45/2001.

Le canal de communication : Selon la notification, le canal de communication par lequel les personnes sont informées est le site intranet du Service de sécurité d'Ispra. En outre, toujours selon la notification, les personnes concernées, y compris les auteurs des incidents et les témoins, en cas de déclarations écrites ou orales, sont "*informées que des données sont collectées et fournies*". Tel ne sera pas le cas, en revanche, lorsque ces personnes ne sont pas interrogées ou ne fournissent pas de déclarations écrites.

Le CEPD estime que la pratique de la publication d'informations sur le site intranet du Service de sécurité du site d'Ispra est positive au regard de l'information des personnes concernées. Il reconnaît par ailleurs que, en formulant des déclarations écrites ou orales, les personnes concernées sont implicitement informées du type de données collectées à leur sujet. Toutefois, de l'avis du CEPD, la combinaison de ces deux mécanismes ne permet pas de fournir aux personnes concernées des

informations appropriées de telle manière qu'elles puissent les lire et les stocker pour s'y référer ultérieurement. Le CEPD est notamment préoccupé de ce que, dans certains cas, les personnes concernées, par exemple les témoins, puissent contacter le Service de sécurité sans visiter le site web dudit Service, contournant ainsi la déclaration de confidentialité Cela est d'autant plus probable pour les auteurs du comportement illicite. Ce problème est encore plus marquant si l'on prend en compte le fait que certaines des personnes concernées peuvent ne pas avoir accès au site intranet du Service de sécurité du site d'Ispra, ce qui sera le cas des personnes extérieures au site. Il serait facile d'éviter d'en arriver là si l'on fournissait directement aux personnes en question la déclaration de confidentialité. Le CEPD demande donc à l'unité C 7 du CCR d'Ispra de définir une procédure permettant de fournir la déclaration de confidentialité aux personnes au sujet desquelles des données à caractère personnel sont collectées. Pour ce qui est des témoins, la fourniture d'informations pourrait s'effectuer au moment où les déclarations orales ou écrites sont acceptées. Pour toute autre personne, cela pourrait se faire dans le cadre de la procédure de déclaration écrite/orale impliquant la signature de la déclaration de la part de son auteur.

Dans le cas présent, l'application de l'article 20 du règlement (CE) nº 45/2001 permet à l'unité C 7 du CCR d'Ispra de *reporter* l'information pour sauvegarder les intérêts visés au paragraphe 1, point a), dudit article, à savoir assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales. L'unité C 7 du CCR d'Ispra peut aussi se prévaloir du point c) dudit paragraphe s'il estime qu'il est nécessaire de reporter l'information pour garantir "*la protection de la personne concernée ou des droits et libertés d'autrui*", par exemple si elle considère que la divulgation d'informations peut révéler l'identité du dénonciateur ou de l'informateur, ce qui peut être le cas dans un certain nombre de dossiers. Pour déterminer si elle est tenue de fournir des informations ou si une exception s'applique, l'unité C 7 du CCR d'Ispra doit réaliser une évaluation au cas par cas des circonstances qui entourent le traitement des données en jeu.

Si l'unité C 7 du CCR d'Ispra se prévaut d'une exception pour reporter l'information, elle ne devrait pas perdre de vue que les limitations d'un droit fondamental ne peuvent être appliquées de manière systématique. Elle doit évaluer dans chaque cas si les conditions sont réunies pour appliquer une des exceptions prévues, par exemple, à l'article 20, paragraphe 1, point a) ou c). Par ailleurs, comme l'indique l'article 20, la mesure doit être "nécessaire". Pour ce faire, il faut que le "test de nécessité" soit réalisé au cas par cas. Enfin, si l'unité C 7 du CCR fait valoir une exception, elle doit le faire dans le respect de l'article 20, paragraphe 3, aux termes duquel *"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*". Toutefois, l'unité C 7 du CCR peut reporter l'information en se prévalant de l'article 20, paragraphe 5, aux termes duquel *"la fourniture des informations visées 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 contenu de la déclaration de confidentialité. Le CEPD a par ailleurs vérifié le contenu des informations fournies dans la déclaration de confidentialité et estime que, le plus souvent, ladite déclaration contient les informations requises au titre des articles 11 et 12 du règlement (CE) nº 45/2001. En effet, elle contient les informations relatives à l'identité du responsable du traitement, aux destinataires des données, à l'existence d'un droit d'accès et du droit de rectification, y compris le nom de la personne à contacter pour faire valoir ces droits. Elle mentionne également le droit de recourir au Contrôleur européen de la protection des données. Le CEPD estime que les informations énoncées ci-après font défaut et demande à l'unité C 7 du CCR de les indiquer:

Tout d'abord, le CEPD considère que la déclaration de confidentialité devrait mentionner la base juridique habilitant l'unité C 7 du CCR à effectuer le traitement des données. Cela est particulièrement important si l'on tient compte du caractère plutôt sensible du type de données en question, qui peut avoir pour effet que des personnes se voient traduire devant la justice pénale. En deuxième lieu, le CEPD considère que la description des finalités du traitement n'est pas complète car elle ne décrit pas quelle est l'utilisation finale recherchée du rapport réalisé par l'unité C 7 du

CCR. Enfin, le CEPD estime que la description des délais prévus pour le stockage des données devrait être complétée par l'indication des délais applicables aux rapports qui ne donnent lieu ni à l'application d'une mesure concrète ni à une transmission aux autorités répressives nationales.

2.2.9 Mesures de sécurité

Selon les articles 22 et 23 du règlement (CE) n° 45/2001, le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à caractère personnel à protéger. Ces mesures de sécurité doivent notamment empêcher toute communication ou tout accès non autorisés, toute destruction accidentelle ou illicite, toute perte accidentelle ou toute modification, ainsi que toute autre forme de traitement illicite. Le CCR confirme qu'il a adopté les mesures de sécurité requises en vertu de l'article 22 du règlement. Le CEPD n'a aucune raison de croire que le CCR n'a pas mis en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à caractère personnel à protéger.

3. Conclusion

Rien ne porte à croire à une violation des dispositions du règlement 45/2001, à condition que les considérations énoncées dans le présent avis soient pleinement prises en compte. L'OLAF doit en particulier garder à l'esprit les points suivants:

* il est nécessaire que le CCR d'Ispra, conjointement avec la DG ADMIN, précise les compétences du Service de sécurité du CCR d'Ispra, notamment pour confirmer qu'il est compétent, conjointement avec la DG ADMIN, pour effectuer des enquêtes relatives à des incidents et élaborer des rapports décrivant les faits survenus.
* il convient de veiller à ce que seules les données qui sont pertinentes aux fins de l'enquête soient collectées et consignées dans le rapport écrit. Il convient d'accorder une attention particulière à des catégories particulières de données. Il conviendrait de veiller à ce que les agents de sécurité chargés d'effectuer les enquêtes et d'élaborer les rapports soient informés de ces règles.
* Lorsque des données sont transférées au sein des institutions et des organes de l'UE ainsi qu'à des autorités nationales (de police et judiciaires), il conviendrait d'adresser aux destinataires de ces données un avis les informant que les données en question ne peuvent être traitées qu'aux fins pour lesquelles elles ont été transmises.
* Lorsque des données sont transférées, il convient de veiller à ce que cette transmission ne s'effectue que si le transfert est nécessaire. Cette nécessité devrait être confirmée dans un avis motivé.
* Lorsque c'est possible, la déclaration de confidentialité devrait être fournie directement aux personnes concernées. Il y a lieu d'établir une procédure à cet effet.
* Il convient de modifier la déclaration de confidentialité de la manière suggérée par le présent avis.

Fait à Bruxelles le 31 juillet 2008

(Signé)

Joaquín BAYO DELGADO
Contrôleur adjoint de la protection des données