Avis concernant une notification relative à un contrôle préalable reçue du délégué à la protection des données du Secrétariat Général du Conseil (SGC) à propos de la conduite des enquêtes du Bureau de Sécurité.

Bruxelles, le 12 décembre 2008 (dossier 2008-410)

1. Procédure

Le 2 juillet 2008, le Contrôleur européen de la protection des données (CEPD) a reçu du délégué à la protection des données (DPD) du SGC une notification relative à un contrôle préalable à propos de la conduite des enquêtes du Bureau de Sécurité du SGC.

Le 25 juillet 2008, le CEPD a demandé au responsable du traitement des informations complémentaires. Les réponses ont été reçues le 12 août 2008. Le 17 septembre 2008, une nouvelle liste de questions a été envoyée au responsable du traitement qui y répondra le 15 octobre 2008. Le projet d'avis a été envoyé au DPD pour commentaires le 30 octobre 2008. Ces derniers ont été reçus le 8 décembre 2008.

2. Faits

La ***finalité*** des enquêtes du Bureau de Sécurité du SGC est, en premier lieu, la recherche et la poursuite des infractions pénales ainsi que la recherche et la signalisation du non-respect du règlement de sécurité du Conseil[1] par négligence ou avec l'intention de divulguer et de compromettre les informations classifiées. En second lieu, les enquêtes servent également à prévenir les différentes infractions, négligences, divulgations et compromissions mentionnées ci-dessus. Les enquêtes de contre-renseignement font parties des enquêtes décrites ci-dessus.

La notification porte uniquement sur les enquêtes menées par le Bureau de Sécurité du SGC, les activités connexes du Bureau de Sécurité n'en font pas partie et ne sont donc pas l'objet de l'analyse entreprise ici par le CEPD.

La procédure comprend l'enregistrement de toutes les enquêtes faites par le secteur "Enquêtes et Sécurité des Informations Classifiées UE (ICUE)" du Bureau de Sécurité (BdS). Chaque incident de sécurité, intervention, renseignement, assistance aux autorités belges ou autres est ainsi enregistré. Ces enregistrements permettent d'examiner les incidents à court et à long terme et d'en faire l'analyse en ce qui concerne les menaces et les risques qu'ils posent. Ces enregistrements sont également indispensables pour la délivrance des autorisations (habilitations de sécurité, autorisation d'accès à l'information pour les fonctionnaires) par l'autorité investie du pouvoir de nomination (AIPN), visées au règlement de sécurité du Conseil (2001/264/CE) Partie II, section VI, § 4 et 5. En effet, le § 5 établit que l'autorisation

[1] Décision du Conseil du 19 mars 2001 adoptant le règlement de sécurité du Conseil (2001/264/CE)

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

peut être retirée par l'AIPN lorsqu'elle estime que des motifs le justifient. Toute décision de retrait est notifiée à la personne concernée, qui peut demander à être entendue par l'AIPN, ainsi qu'à l'autorité nationale compétente.

Toute ***personne concernée*** par une enquête menée par le Bureau de Sécurité du SGC est une personne concernée par le traitement. Il est possible de distinguer notamment les catégories de personnes suivantes : les fonctionnaires et autres agents en activité du SGC, les fonctionnaires et agents retraités, les prestataires de services, les experts nationaux détachés, les stagiaires, les délégués des Etats membres, les délégués des Etats tiers, les fonctionnaires d'autres institutions communautaires, les visiteurs, les journalistes, les fonctionnaires des Etats membres, le personnel des firmes externes et les membres de la famille des catégories susmentionnées.

Les données traitées dépendent des faits établis pendant le déroulement des enquêtes. Il peut s'agir de données administratives mais aussi judiciaires.

Chaque enquête est particulière et nécessite des catégories de données spécifiques comme par exemple : les enregistrements par les lecteurs de badge, l'utilisation des cartes TESA/KABA, l'analyse du modus operandi (la façon récurrente d'opérer un acte malveillant), des photos, des renseignements portant sur des véhicules suspects, des enregistrements de vidéosurveillance et des données de trafic des communications téléphoniques et des communications électroniques.

Certaines bases de données sont reliées automatiquement à la base de données "Conduite des enquêtes". C'est le cas de la base de données des accréditations des journalistes[2], de la base de données des habilitations de sécurité et du logbook électronique du Centre de Sécurité (7 jours sur 7 et 24 heures sur 24). Les données traitées proviennent donc également de ces bases de données.

En principe, le traitement est ***automatisé***. Cependant, les dossiers classifiés (au sens de la décision 2001/264/CE) ou sensibles sont traités et conservés sur support papier (***procédure manuelle***) ou sur ordinateur autonome (dit "stand alone").

Le Bureau de Sécurité gère toutes les enquêtes prévues par la Décision 198/03 du Secrétaire Général du Conseil/Haut Représentant concernant les tâches du Bureau de Sécurité. Une enquête regroupe l'ensemble des informations collectées et des actions entreprises pour résoudre les problèmes liés à un ou plusieurs incidents de sécurité. Ces informations et actions sont conservées sous forme de documents automatisés. Ils sont le résultat de l'importation de données depuis différentes bases de données et de la saisie d'autres informations. Une enquête se déroule selon les étapes suivantes : le lancement, la première intervention, l'enquête ultérieure, le rapport et finalement l'analyse.

a) Les conditions de lancement d'une enquête peuvent être multiples : les rapports d'incidents sont les événements le plus souvent pris en compte. Il s'agit d'un formulaire électronique qui est disponible sur le site web du Bureau de Sécurité. Il est accessible à toute personne ayant accès à l'intranet du SGC. Les autres événements déclencheurs sont les suivants : le flagrant délit (l'enquête est alors lancée à l'initiative de l'enquêteur), le "logbook" (journal électronique) du Centre de Sécurité qui enregistre chaque incident de sécurité 24 heures sur 24 et 7 jours sur 7, les rapports rédigés par le service de gardiennage du SGC, une demande

[2] Le traitement de données "accréditation des journalistes", 2004-259 a déjà été analysé par le CEPD, son avis a été publié le 16 septembre 2008.

officielle des autorités belges ou d'un autre Etat membre, une demande officielle des services d'enquêtes d'autres institutions et ou finalement, une demande de l'AIPN.

b) La première intervention vise à collecter toutes les informations sur place : les témoignages, l'identification de toutes les personnes présentes sur les lieux, la conservation des traces, les interrogatoires des victimes/auteurs et les photographies pertinentes. La première intervention inclut également la coordination avec les autres services concernés.

c) Pendant l'enquête ultérieure le Bureau va collecter les informations pertinentes, interroger les témoins et les suspects (cela dans le cadre stricte de l'article 6 de la Décision 198/03), informer et assister, en cas de nécessité, les services de police belge ou autre, faire appel, pour assistance à la DGA/5 (Systèmes d'information et de communication), faire des recherches et vérifications à l'aide de la base de données du Bureau de Sécurité. Tous les moyens pour collecter l'information sont exploités : enregistrements de vidéosurveillance, enregistrements par badge d'accès, le trafic des communications par téléphone de service et le trafic des communications électroniques. Le Bureau va également exploiter tous les contacts externes et internes pertinents dans la conduite d'une enquête.

d) La dernière étape est l'analyse des faits : La "Conduite des enquêtes" est une application spécifique qui permet tant la consultation que la mise à jour des données récoltées. Le fait que les informations soient stockées dans une base de données dédiée, augmente l'efficacité des analyses sur le long terme. L'enregistrement des étapes fait l'objet d'un "log in" dans la base de données. La base de données peut créer un rapport en format WORD.

Les dossiers d'enquête, tant les dossiers sur papier que les fichiers électroniques sont conservés au secteur "Enquêtes et Sécurité des ICUE" et cela pour une période de trente ans. Cette ***durée de conservation*** se justifie d'après le SGC pour les raisons suivantes : (i) le délai de prescription pour les crimes graves en Belgique s'élève à vingt ans et la section Enquêtes doit pouvoir répondre aux questions venants des autorités belges ou autres, concernant certains faits commis plusieurs années auparavant. (ii) Certains dossiers de renseignement, en matière d'espionnage ou de terrorisme peuvent s'étaler sur de très longues périodes (parfois plusieurs dizaines d'années). (iii) La carrière moyenne d'un fonctionnaire s'étale sur plus au moins trente ans et les différentes étapes de cette carrière ainsi que les incidents survenus pendant celle-ci sont des éléments indispensables pour ébaucher le profil d'une personne impliquée dans des enquêtes compliquées.

Les ***destinataires*** des données proviennent soit de l'intérieur du SGC, c'est le cas de l'AIPN, du conseil de discipline lorsqu'une enquête administrative est envisagée ou en cours et de la DGA 1 dans les cas d'intervention de l'assurance du SGC (par exemple la transmission du nom du témoin d'un accident), soit à d'autres institutions communautaires comme l'OLAF soit enfin à l'extérieur des institutions communautaires lorsque les données sont communiquées aux autorités judiciaires des Etats membres. Les données sont transmises sous forme de rapport Word. Les données brutes qui ont menées au rapport restent au Bureau de Sécurité.

En ce qui concerne les ***droits des personnes concernées***, le Conseil a adopté la décision du 13 septembre 2004 portant adoption de dispositions d'application en ce qui concerne le règlement (CE) no 45/2001 du Parlement européen et du Conseil 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, dont la Section 5 décrit la procédure permettant au personnes concernées d'exercer leur droit.

L'information à fournir à la personne concernée se fait via la Décision n°198/03 du Conseil portant sur les tâches du Bureau de Sécurité qui est portée à la connaissance de tout le personnel. Plus spécifiquement, son article 6.3 précise : "lorsqu'on constate qu'un fonctionnaire ou agent du Secrétariat général a pu être personnellement impliqué dans une affaire, l'intéressé en est rapidement informé par le Bureau de Sécurité. La communication de cette information peut être différée avec l'accord du Secrétaire général adjoint si elle risque de compromettre l'enquête ou dans les cas où le secret absolu est de rigueur aux fins de l'enquête et où il faut recourir à des procédures d'enquête relevant de la compétence d'une autorité judiciaire nationale. En tout état de cause, une fois l'enquête terminée, des conclusions faisant nommément référence à la personne concernée ne peuvent être tirées sans que l'intéressé n'ait eu la possibilité d'exprimer son point de vue sur tous les faits qui le concernent."

Le ***verrouillage*** et ***l'effacement*** des différentes catégories de données est possible, endéans les deux jours ouvrables, après la requête légitime de la personne concernée.

[...]

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 effectuées par le Bureau de Sécurité du SGC. Le traitement comprend des opérations de collecte, de consultation, de conservation d'effacement, etc. de données. Il est réalisé par une institution européenne et est mis en œuvre pour l'exercice d'activités relevant en partie du champ d'application du droit communautaire. Le traitement de données à caractère personnel est en grande partie automatisé. Le règlement est donc applicable.

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

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

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 porte également 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 problèmes sérieux dans la mesure où les recommandations du CEPD peuvent encore être adoptées si nécessaire.

La notification du DPD a été reçue le 2 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 102 jours (71 jours de suspension + le mois d'août). L'avis sera dès lors rendu le 15 décembre 2008 au plus tard.

3.2. Base juridique et licéité du traitement

Le traitement de données dans le cadre d'enquêtes de sécurité est fondé sur différents instruments législatifs allant du plus général au plus particulier. Le règlement intérieur du Conseil (Décision 2006/683/CE) précise que : *Le Conseil décide de l'organisation du secrétariat général. Sous son autorité, le Secrétaire général et secrétaire général adjoint prennent toutes les mesures nécessaires pour assurer le bon fonctionnement du secrétariat général* (article 23).

Le règlement de sécurité du Conseil adopté par la Décision 2001/264/CE entérine la mise en place d'un système de sécurité global du Conseil, du Secrétariat Général et des Etats Membres au regard des activités dans des domaines qui requièrent un certain degré de confidentialité. La section I de la partie II du règlement stipule que le Secrétaire Général/Haut représentant a la responsabilité d'enquêter ou de faire enquêter sur toute fuite concernant les informations classifiées de l'UE si, à première vue, les indices montrent qu'une telle fuite s'est produite au SGC ou dans l'un ou l'autre des organismes décentralisés de l'UE. La section I décide de la mise en place du bureau de sécurité qui doit coordonner, superviser et exécuter les mesures de sécurité. La section X est consacrée à la définition et à la gestion des infractions à la sécurité et compromissions d'informations classifiées de l'UE. La section définit également plus précisément le rôle de l'autorité chargée de la sécurité en cas d'infraction à la sécurité et compromissions d'informations classifiées de l'UE.

Enfin, plus spécifiquement encore, la Décision 198/3 du SGC décrit les tâches du Bureau de Sécurité et plus particulièrement ce qui concerne ses enquêtes.

L'article 2 prévoit : *le Bureau de sécurité, en conformité avec le règlement de sécurité (...) : enquête sur toute fuite, divulgation non autorisée ou compromission d'informations classifiées de l'UE, si, à première vue, les indices montrent qu'une telle fuite s'est produite au Secrétariat Général ou dans l'un ou l'autre des organismes décentralisés de l'UE*;

L'article 5 stipule : *Si une personne est surprise alors qu'elle est en train de commettre un acte ou une omission contraire au droit pénal de l'État d'accueil, le Bureau de sécurité effectue immédiatement une enquête et peut, conformément à la législation de l'État d'accueil, retenir la personne concernée jusqu'à ce que les autorités nationales compétentes aient été contactées et soient en mesure de l'interroger.*

L'article 6 mentionne : *Sans préjudice de l'obligation qu'a le Bureau de sécurité de prêter assistance à l'Office européen de lutte antifraude dans l'exécution concrète des enquêtes menées par celui-ci, lorsque le Bureau de sécurité soupçonne qu'une infraction a été commise, est en train d'être commise ou sera probablement commise dans un bâtiment du Conseil ou dans un lieu où se déroulent ses travaux, ou lorsqu'il détient des informations en ce sens, il en informe immédiatement le Secrétaire général/Haut représentant ou le Secrétaire général adjoint et procède à une enquête. Lors d'une telle enquête, le Bureau de sécurité peut, avec l'autorisation du Secrétaire général/Haut représentant ou du Secrétaire général adjoint et en cas d'extrême urgence:*

- *interroger toute personne se trouvant dans un bâtiment du Conseil ou dans un lieu où se déroulent ses travaux;*

- *avoir accès à tout local dans les bâtiments du Conseil ou les lieux où se déroulent ses travaux;*
- *avoir accès à tous les documents et informations nécessaires dans le cadre de l'enquête.*

2. Les informations transmises ou obtenues au cours d'enquêtes internes, quelle qu'en soit la forme, sont soumises au secret professionnel et sont protégées au titre du règlement (CE) nº 45/2001 et/ou des autres dispositions applicables au Conseil.
L'article 11 précise : *Les enquêtes sur des questions liées à la sécurité relèvent de la responsabilité du Bureau de sécurité sous la direction du Secrétaire général/Haut représentant ou du Secrétaire général adjoint. Aucun membre du personnel du Secrétariat général ni aucun tiers ayant un contrat avec ce dernier ne peut mener une enquête sur une question de sécurité sans l'autorisation préalable du Secrétaire général/Haut représentant ou du Secrétaire général adjoint.*

L'article 15 établit : *Le Bureau de sécurité peut établir des contacts avec:*
les Autorités nationales de sécurité compétentes des États membres, pour obtenir leur aide concernant les informations dont il a besoin pour évaluer les risques et les menaces auxquels pourraient être exposés le Secrétariat général, son personnel, ses activités, ses biens et ressources et ses informations classifiées dans les lieux où se déroulent normalement ses travaux;
les services nationaux compétents des États membres ou des États d'accueil sur le territoire desquels le Secrétariat général peut exercer ses activités, en ce qui concerne toute question liée à la protection, sur leur territoire, de son personnel, de ses activités, de ses biens et ressources et de ses informations classifiées;
les services de sécurité des autres institutions européennes et organismes internationaux en vue d'assurer toute coordination utile.

Compte tenu de cette base juridique, il y a lieu d'examiner la licéité du traitement. Selon l'article 5, point a) du règlement 45/2001, 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 instruments précités indiquent que les enquêtes menées par le Bureau de Sécurité sont des missions d'intérêt public (gestion et prévention des infractions à la sécurité, des compromissions d'information classifiée de l'UE, etc.) sur la base d'actes législatifs adoptés sur la base des traités. En outre, le Bureau de Sécurité 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.

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

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

Le type de données décrites à l'article 10, paragraphe 1, ne fera pas l'objet d'un traitement systématique mais peut certainement apparaître dans le cadre des certaines enquêtes. Dans ce cas, il convient de respecter l'interdiction générale établie à l'article 10, paragraphe 1, ou d'examiner de façon restrictive s'il est nécessaire d'appliquer une exception. Quoi qu'il en soit, le personnel du BdS chargé 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 une des circonstances prévues à l'article 10, paragraphe 2, ne soit présente dans l'affaire en cause ou qu'il ne soit nécessaire d'appliquer l'article 10, paragraphe 4 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), 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 les dossiers d'enquêtes, le contenu exact de ces dossiers diffèrera naturellement selon les cas. Ainsi, c'est au cas par cas que la qualité des données devra être appréciée. Il y a 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.

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 (la base de données spécialisée des enquêtes permet la mise à jour de celles-ci) 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 3.7 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 que cela soit en qualité de témoin, informateur, etc.) et la rapidité avec laquelle ces informations lui sont transmises, afin que le droit de défense puisse être respecté (voir le point 3.8 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 contenues dans la base de données informatique ainsi que dans les dossiers physiques sont conservées pendant une durée de trente ans à partir de la constitution du dossier. Pour rappel, le BdS évoque trois raisons pour justifier la fixation de ce délai de conservation. D'une part le délai de prescription généralement admis par la loi belge pour les crimes grave est de 20 ans, les agents traitant les dossiers peuvent en effet être appelés à témoigner devant les instances compétentes. D'autre part certains dossiers de renseignement et de contre-espionnage ne peuvent s'apprécier que sur le long ou le très long terme, et, enfin, la durée moyenne de la carrière d'un fonctionnaire s'étale sur plus ou moins une durée de trente ans.

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 sont 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".

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

3.6. Transfert de données

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

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

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

Si des données sont transférées à la suite d'une demande du destinataire, tant le BdS que le destinataire assument la responsabilité de la légitimité du transfert, conformément à l'article 7 paragraphe 2. Le BdS 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, le BdS 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, le BdS doit inclure dans le dossier une note faisant état du transfert des données.

3.6.2. Transfert de données à caractère personnel aux États membres

Deux scénarios peuvent être observés dans les États membres :

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

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

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

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

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 du BdS, 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 le BdS 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. Le BdS doit procéder à cette évaluation chaque fois qu'il transfère des données à caractère personnel de sa propre initiative et établir une décision motivée exposant la nécessité du transfert.

Le respect de l'article 8, point a), du règlement exige que les destinataires des informations utilisent les données pour exécuter une mission dans l'intérêt public. Le CEPD estime que l'envoi de données à caractère personnel dans le cadre des échanges relevant de l'assistance mutuelle peut être considéré en théorie comme remplissant les conditions de l'article 8, point a). Les autorités compétentes des États membres utiliseront les données pour exécuter des missions d'intérêt public en menant des activités dans les domaines du renseignement.

Pour les pays qui n'ont pas étendu l'application de la directive 95/46/CE aux autorités judiciaires, il convient de prendre en considération l'article 9 du règlement. Dans le cas de ces pays, la Convention 108 du Conseil de l'Europe, qui, pour ce qui concerne la question étudiée, peut être considérée comme fournissant un niveau de protection adéquat, est en tout état de cause applicable aux autorités judiciaires.

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

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

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

Une autre forme de dérogation est prévue à l'article 9.7 qui stipule que le transfert peut être autorisé par le CEPD "*lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants; ces garanties peuvent notamment résulter de clauses contractuelles appropriées*".

En vertu de l'article 9.8, le BdS 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 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 2001/264/CE a prévu à sa section XII les principes régissant la communication d'informations classifiées de l'UE à des Etats tiers ou à des organisations internationales. L'article 3 de la section XII 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 Conseil*". Le CEPD relève ce point car il se réjouit que de tels transferts soient soumis aux conditions strictes de sécurité établies par la décision 2001/264/CE, mais il précise que ces transferts doivent aussi, comme expliqué ci-dessus, répondre aux conditions de protection des données prévues par le règlement 45/2001.

3.7. Droit d'accès et de rectification

Selon l'article 13 du règlement, la personne concernée a le droit d'obtenir, sans contrainte, du responsable du traitement la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données.

Le droit d'accès est le droit de la personne concernée d'être informée de tout renseignement la concernant traité par le responsable du traitement. Par principe, ce droit doit être interprété en liaison avec la notion de données à caractère personnel. En effet, une vision large des données à caractère personnel a été adoptée dans le règlement, et le Groupe de l'article 29 a également donné une large interprétation à ce concept[3]. 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, le Conseil a adopté la décision du 13 septembre 2004 portant adoption de dispositions d'application en ce qui concerne le règlement (CE) no 45/2001 du Parlement européen et du Conseil 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, dont la Section 5 décrit la procédure permettant au personnes concernées d'exercer leur droit.

Le CEPD se réjouit du fait que les droits d'accès et de rectification de la personne concernée soient garantis. 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". 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 compromettre l'enquête (voir le point 3.8 ci-dessous).

[3] 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 "prédisciplinaire" ou "prépénale". L'intérêt de l'autorité qui est censée suivre l'enquête (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 le BdS : *"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 3.8 ci-dessous).

En outre, il y a lieu de tenir compte également du paragraphe 4 de l'article 20 : *"Si une limitation prévue au paragraphe 1 est invoquée pour refuser l'accès à la personne concernée, le contrôleur européen de la protection des données lui fait uniquement savoir, lorsqu'il examine la réclamation, si les données ont été traitées correctement et, dans la négative, si toutes les corrections nécessaires ont été apportées"*. Le droit d'accès indirect devra alors être garanti. En effet, cette disposition jouera un rôle, par exemple, dans les cas où la personne concernée a été informée de l'existence du traitement, ou en a connaissance, mais où son droit d'accès reste limité eu égard à l'article 20.

L'article 20, paragraphe 5, dispose que *"L'information visée aux paragraphes 3 et 4 peut être reportée aussi longtemps qu'elle prive d'effet la limitation imposée sur la base du paragraphe 1"*. Il peut se révéler nécessaire pour le BdS 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[4].

L'article 14 du règlement accorde à la personne concernée le droit à la rectification des données inexactes ou incomplètes. Compte tenu de la sensibilité de la plupart des enquêtes menées par le BdS, ce droit revêt une importance cruciale pour garantir la qualité des données

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

utilisées, laquelle est, en l'espèce, liée au droit de défense. Le droit de 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.

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

3.8. Information de la personne concernée

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

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

Comme indiqué au point 2, lorsque qu'un fonctionnaire ou agent du SGC est impliqué dans une affaire, il en est rapidement informé par le BdS à moins que cette information ne compromette l'enquête ou dans les cas où le secret absolu est de rigueur aux fins de l'enquête et où il faut recourir à des procédures d'enquête relevant de la compétence d'une autorité judiciaire nationale. En tout état de cause, une fois l'enquête terminée, des conclusions faisant nommément référence à la personne concernée ne peuvent être tirées sans que l'intéressé n'ait eu la possibilité d'exprimer son point de vue sur tous les faits qui le concernent (article 6.3 de la décision 198/03). La décision 198/03 elle-même est accessible à tous sur l'intranet du SGC.

Le CEPD accueille favorablement le fait que cette information se situe à deux niveaux, l'un plus général via la publication de la décision et un personnalisé lorsque le BdS informe personnellement la personne concernée.

Cependant, bien que la teneur des informations fournies puisse parfois correspondre partiellement aux informations qui doivent être communiquées en vertu des articles 11 et 12, il ressort de l'analyse par le CEPD que les informations visées dans ces dispositions ne sont pas toutes effectivement données. Il convient de tenir compte du fait que toutes les exigences prévues au paragraphe 1 des articles 11 et 12 doivent être respectées, y compris celles mentionnées au point f), puisque, compte tenu de la sensibilité des affaires, les personnes concernées doivent avoir connaissance de toutes les garanties auxquelles elles ont droit. Ainsi, une déclaration de confidentialité spécifique serait la bienvenue.

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 le BdS 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, autorités nationales), le BdS 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 (voir le point 3.8 ci-dessus).

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

3.9. 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 19 mars 2001 adoptant le règlement de sécurité du Conseil (2001/264/CE). De manière générale, les accès physiques et informatiques sont limités aux personnels disposant du besoin d'en connaître et des habilitations de sécurité / autorisations d'accès à l'information classifiée correspondantes.

Au regard de l'ensemble des mesures de sécurité prises, le CEPD estime que celles-ci peuvent être considérées comme 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, le SGC doit:

- évaluer la proportionnalité des activités de traitement au cas par cas ;
- établir une recommandation générale adressée aux personnes qui gèrent les dossiers d'enquête, en vue de leur rappeler le principe de qualité des données et de les inviter à veiller au respect de celui-ci, conformément à l'article 4.1.c ;
- 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 la compétence du destinataire et à titre provisoire la nécessité du transfert lorsque le destinataire fait au BdS une demande de transfert de données, conformément à l'article 7, paragraphe 2 ;
- inclure dans le dossier d'enquête une note faisant état du transfert des données ;

- établir la nécessité d'un transfert de sa propre initiative aux autorités judiciaires dans une décision motivée, à la lumière de l'article 8 du règlement ;
- mettre en place un registre des transferts occasionnels effectués en vertu de la dérogation de l'article 9.6 et 9.7 et en informer le CEPD ;
- 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 (article 12) ;
- 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 ;
- établir des règles afin que, dès que l'enquête est terminée, la personne concernée puisse rectifier les données à caractère personnel la concernant, en vue de leur mise à jour à la lumière des faits ultérieurs ;
- respecter le contenu des informations qui doivent être fournies à la personne concernée, conformément au paragraphe 1 des articles 11 et 12 du règlement (y compris le point f).

Fait à Bruxelles, le 12 décembre 2008.

(signé)

Peter HUSTINX
Contrôleur Européen de la Protection des Données