Avis sur la notification d'un contrôle préalable reçue du délégué à la protection des données du service européen pour l'action extérieure sur les enquêtes en matière de sécurité

Bruxelles, le 1er février 2013 (2011-1059)

1. Procédure

Le 21 novembre 2011, le Contrôleur européen de la protection des données («**CEPD**») a reçu du délégué à la protection des données («DPD») du service européen pour l'action extérieure («SEAE») la notification d'un contrôle préalable concernant les enquêtes en matière de sécurité menées par la division de la sécurité et de la politique de sécurité du SEAE. La notification était accompagnée d'une déclaration de confidentialité.

Des questions ont été transmises le 20 décembre 2011, auxquelles le SEAE a répondu le 14 juin 2012. D'autres questions ont été posées les 21 juin et 9 août, et les réponses ont été fournies respectivement les 23 juillet et 31 août. Dans l'intervalle, une notification révisée a été envoyée le 23 juillet 2012. Le 10 septembre, conformément à l'article 27, paragraphe 4, le CEPD a prolongé de deux semaines (jusqu'au 24 septembre) le délai qui lui est imparti pour rendre son avis sur le contrôle préalable, lequel délai a été de nouveau prolongé jusqu'au 8 octobre en raison de la complexité du dossier. Des demandes d'informations/d'éclaircissements complémentaires ont été transmises le 8 octobre et les réponses fournies le 14 décembre 2012. Le CEPD a de nouveau prolongé le délai d'un mois le 17 décembre 2012. Le projet d'avis a été adressé au DPD pour observations le 16 janvier 2013. Le CEPD a reçu la réponse du SEAE le 31 janvier 2013.

2. Faits

2.1 Finalités

Eu égard à la notification, le traitement des données a pour principale finalité de mener des enquêtes sur les infractions à la sécurité, la compromission ou la perte d'informations classifiées de l'UE («ICUE»), les incidents de sécurité et les menaces pesant sur les intérêts du SEAE en matière de sécurité, réels ou présumés. Cette finalité générale se divise en plusieurs traitements de données qui sont expliqués ci-dessous.

Le responsable du traitement est le SEAE, représenté par le directeur de la sécurité du QG et de la politique de sécurité du SEAE.

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 30
E-mail: edps@edps.europa.eu - Site Internet: www.edps.europa.eu
Tél.: 02-283 19 00 - Fax: 02-283 19 50

La base juridique des traitements de données visés par cette finalité se compose des actes législatifs suivants:

1. Décision du Conseil du 26 juillet 2010 fixant l'organisation et le fonctionnement du service européen pour l'action extérieure, article 10, paragraphe 2 sur la sécurité (2010/427/UE).
2. Décision du Conseil du 31 mars 2011 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'UE, et notamment ses articles premier, 7, 12 et 13 (2011/292/UE)[1].
3. Décision de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité du 15 juin 2011 relative aux règles de sécurité applicables au service européen pour l'action extérieure, et notamment ses articles premier, 7, 8, 9 et 10[2] (2011/C 304/05).
4. Décision de la Commission de l'UE du 08.09.1994.
5. Décision nº 844 de la Commission de l'UE du 29.11.2001[3] et règlement Euratom nº 3 du 31.07.1958[4].
6. Information administrative nº 45/2006 de la Commission européenne du 15.09.2006.

De plus, à la date de rédaction du présent avis, le SEAE élaborait une version consolidée[5] de la «décision de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité [...] relative aux règles de sécurité applicables au service européen pour l'action extérieure» (le «projet de décision consolidée»). Cette décision, ainsi que l'affirme le responsable du traitement, clarifie les évènements prévisibles devant faire l'objet d'une enquête et recouvre les faits suivants:
- infractions à la sécurité, réelles ou présumées (article 8);
- compromission ou perte d'informations classifiées de l'UE («ICUE»), réelles ou présumées (article 8);
- incidents de sécurité ou menaces pesant sur les intérêts du SEAE en matière de sécurité, réels ou présumés (article 2).

Finalité et types de traitements

Conformément à la finalité générale exposée ci-dessus, la procédure du SEAE recouvre diverses activités de traitement:

2.1.1) Enquête sur les incidents de sécurité, les infractions à la sécurité ou les menaces pesant sur les intérêts du SEAE en matière de sécurité.
L'article 9 du projet de décision consolidée apporte des précisions quant aux enquêtes menées sur les incidents de sécurité, les infractions à la sécurité et/ou la compromission d'informations classifiées, ainsi que sur les mesures correctives à prendre.

[1] Cette décision énonce les principes de base et les normes minimales de sécurité pour la protection des ICUE.
[2] Cette décision arrête les règles en matière de sûreté et de sécurité applicables au SEAE. Elle définit le cadre réglementaire général permettant à ce dernier de gérer efficacement les risques menaçant son personnel, ses biens matériels et les informations qu'il détient et de s'acquitter des responsabilités qui lui incombent en ce qui concerne l'obligation de vigilance à cet égard.
[3] La décision de la Commission du 29 novembre 2001 prévoit une structure 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.
[4] Le règlement nº 3 du Conseil Euratom 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.
[5] Les premières règles adoptées par le SEAE sont arrêtées par la décision de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité du 15 juin 2011 relative aux règles de sécurité applicables au service européen pour l'action extérieure (2011/C 304/05).

Ainsi, des enquêtes ou des vérifications peuvent être menées:
(I) lorsqu'il est avéré ou qu'il existe des motifs raisonnables de supposer que des informations classifiées concernant le SEAE ont été compromises ou perdues,
(II) sur toute infraction à la sécurité, réelle ou présumée, ou tout autre incident de sécurité ou menace pesant sur les intérêts du SEAE en matière de sécurité.

Dans tous les cas susmentionnés, un dossier est créé pour collecter tous les éléments susceptibles de contribuer à la manifestation de la vérité, à la détermination du préjudice subi et à l'éventuelle identification de l'auteur de l'infraction présumée. Ceci comprend notamment la déclaration des plaignants, des témoins, des éventuels auteurs des faits, mais aussi tout élément probant. Le but est l'établissement d'un rapport transmis à l'autorité compétente selon le cas traité. L'article 9 dispose également que: «*Lorsque l'accès aux informations concerne des données privées contenues dans des systèmes de communication et d'information, ledit accès est conforme au règlement (CE) nº 45/2001*».

2.1.2) Base de données de dossiers
Il est précisé dans la notification qu'il sera procédé à l'établissement d'une base de données des dossiers (en cours et classés) reprenant des informations utiles issues de chaque dossier et permettant à la fois de retrouver facilement et d'extraire certaines données afin d'orienter des actions préventives et d'établir des statistiques anonymisées. Selon les informations fournies par le responsable du traitement, la base de données a pour finalité de faire en sorte que les enregistrements conservés soient pris en charge par un outil automatisé permettant de retrouver/d'extraire aisément des fichiers à des fins d'enquêtes autorisées (rechercher des dossiers similaires, leur modus operandi, des infractions à la sécurité commises à plusieurs reprises par la même personne, faciliter les contrôles de sécurité du personnel par les services autorisés, etc.).

2.1.3) Liste d'accès
Un autre traitement consiste en l'établissement, l'entretien et la mise à jour d'une liste des personnes dont l'accès aux locaux du SEAE est interdit, sur la base de preuves provenant des dossiers concernés. L'article 11 du projet de décision consolidée prévoit que: «Tant qu'une enquête sur l'infraction et/ou la compromission est en cours, le chef de la direction de la sécurité du SEAE peut suspendre l'accès de la personne concernée aux ICUE et aux locaux du SEAE».

Cette liste est établie de la façon suivante: lorsqu'une enquête autorisée sur la compromission des ICUE est en cours, la personne suspectée d'être à l'origine de l'infraction peut, selon les règles en vigueur, se voir retirer l'autorisation d'accéder aux ICUE par l'autorité de sécurité du SEAE. En conséquence, la personne concernée se verra refuser l'accès aux locaux du SEAE (zones sécurisées et/ou éventuellement l'ensemble des locaux).

2.1.4) Contrôle des communications électroniques
Le SEAE a indiqué dans la notification que, en ce qui concerne les recherches effectuées sur les cas spécifiques d'utilisation d'ordinateurs et/ou de communications (e-mail, Internet, téléphones fixes ou portables, fax, par exemple), l'utilisation acceptable, les mesures de contrôle et les enquêtes sont décrites dans l'information administrative nº 45/2006 du 15.09.2006 relative aux règles applicables à l'utilisation des services de TIC. Cette information administrative porte sur le contrôle des communications électroniques liées aux activités du personnel.

En accord avec cette information administrative, le SEAE a précisé que, dans le cadre de l'enquête, l'anonymat de données spécifiques et limitées (trafic et/ou contenu d'une boîte de

messagerie électronique, accès aux pages Internet, appels depuis un téléphone portable/fixe, télécopies, etc.) peut être levé.

2.2 Catégories de personnes concernées

Les personnes concernées comprennent tous les membres du personnel et les autres agents du SEAE, les agents contractuels, les fonctionnaires retraités, les prestataires de services, les sous-traitants, les visiteurs et les tiers qui s'adressent spontanément au SEAE ou à son personnel (par courrier, e-mail, téléphone, fax, etc.) ou qui sont victimes, témoins ou auteurs d'une infraction ou d'un événement préjudiciable aux intérêts du SEAE ou de son personnel.

2.3 Catégories de données

Les données traitées dans le cas d'incidents de sécurité dépendront des faits établis au cours de l'enquête. En principe, les données à caractère personnel comportant les noms, prénoms, éventuellement le lieu et la date de naissance, l'adresse, les numéros de téléphone fixe et portable peuvent également être traitées, de même que la nature et les circonstances du dossier (ce qui s'est passé, quand et où, etc.), les éléments de preuve recueillis ou le lien entre ces éléments et les personnes concernées.

Les données contenues dans la base de données des dossiers sont énumérées ci-dessous:
numéro du dossier; date de création du dossier; prénom/nom de famille/données relatives à la naissance de la personne à l'origine du signalement; prénom/nom de famille/données relatives à la naissance de la victime; ville de l'évènement; municipalité de l'évènement; lieu de l'évènement; date de l'évènement; partie de la journée; type d'évènement (éventuellement par catégories); champ séparé pour les infractions à la sécurité; champ séparé pour la compromission d'ICUE; champs séparés pour la perte de cartes d'accréditation/de stationnement, clés, PC, appareils portables ou autres du SEAE; résumé du modus operandi; si l'infraction a été signalée ou non à la police fédérale belge; résultats de l'enquête; champ visant à signaler tout comportement/acte suspect de personnes/véhicules/personnel; mesures prises.

Le responsable du traitement a indiqué que les données à caractère personnel traitées sont celles qui sont nécessaires pour permettre une recherche visant à trouver le bon dossier dans la base de données à l'aide de mots-clés. Le responsable du traitement a en outre précisé, à propos de la recherche dans la base de données, que le SEAE utilise les mots-clés[6] pour «*trouver une affaire donnée dans le futur ou pour catégoriser les dossiers présentant le même "modus operandi" ou commis au même endroit, par la même personne, le même jour de la semaine, etc.*». De plus, tous les incidents de sécurité pour lesquels un fichier a été créé sont inclus dans la base de données une fois connus.

En ce qui concerne la liste des accès et le contrôle des communications électroniques, la procédure implique la consultation des bases de données Sysper, Sysper2, Gestel et IOLAN, cartes de service et titres d'accès – photographies comprises -, pensionnés, fichiers-tiers[7], habilitations, consultation, copie et conservation des images enregistrées par les caméras équipant les immeubles, requêtes adressées à DIGIT (trafic e-mails et logs internet, numéros de téléphone appelés au départ des lignes des locaux et des bâtiments dans lesquels le SEAE exerce ses activités) selon une procédure définie.

[6] Le responsable du traitement définit un mot-clé comme tout champ de données listé dans la notification et pouvant servir à des fins d'identification.

[7] Chaque membre du personnel doit indiquer une personne à prévenir en cas d'accident. Les nom et coordonnées de la personne à prévenir sont conservés dans les fichiers de données à caractère personnel du service des ressources humaines.

2.4 Collecte et conservation des données
Les données à caractère personnel sont traitées à la fois manuellement et automatiquement dans des dossiers papier et/ou électroniques. Les documents papier sont conservés dans un coffre-fort et les fichiers électroniques sont stockés dans un système de stockage sécurisé.

2.5 Transferts de données
Les données traitées dans le cadre de l'opération de traitement peuvent être divulguées aux destinataires suivants:

- au sein du SEAE, la liste des personnes interdites d'accès est interdit sera communiquée aux responsables du SEAE ayant besoin d'en connaître dans le cadre de l'exercice de leurs activités professionnelles;

- au sein des autres institutions ou organes communautaires, aux particuliers autorisés, sur la base stricte du besoin d'en connaître (IDOC, OLAF, etc.) dans le cadre de leurs compétences;

- au sein des États membres de l'UE, aux personnes autorisées, aux autorités judiciaires, à la police ou à des entreprises sous-traitantes sur la base stricte du besoin d'en connaître ;

- à des pays tiers ou à des organisations internationales en vertu d'accords ou d'arrangements spécifiques relatifs à la protection réciproque des informations classifiées. Le responsable du traitement a précisé qu'il existe des pays tiers et des organisations internationales (OI) avec lesquels l'UE a mis en place des accords en matière de sécurité des informations ou autres dispositifs similaires. Le responsable du traitement a fourni au CEPD une note d'information du Conseil de l'Union européenne sur «l'échange d'informations classifiées de l'UE (ICUE) avec ceux-ci ("version actuelle du SEAE du 22 juin 2012 - 11766/12")». Cette note énumère les pays tiers et les organisations internationales avec lesquels de tels accords et arrangements ont été conclus[8]. Tous les échanges d'informations se produisant dans ce contexte ne concerneraient que les infractions à la sécurité et/ou les compromissions de la sécurité liées à la gestion d'informations classifiées échangées entre l'UE (et le SEAE en particulier), d'un côté, et le pays tiers ou l'OI concerné, de l'autre. Ces échanges s'inscriront dans le cadre des dispositions pertinentes prévues dans l'accord concerné à propos de la collaboration entre les parties concernant les enquêtes de sécurité.

Compte tenu des informations fournies par le responsable du traitement, ces échanges ne seront effectués qu'après une décision au cas par cas, et feront l'objet d'une vérification afin de s'assurer que la contrepartie et le système et les procédures en place sont fiables, et qu'il existe un besoin d'en connaître adéquat de la part de l'autre partie.

Dans ce cadre, la divulgation de données à caractère personnel ne serait envisagée que dans des cas exceptionnels, lorsque

1. cette divulgation est absolument nécessaire pour collaborer avec le tiers dans le cadre de l'enquête de sécurité concernée;
2. le caractère adéquat du niveau de protection assuré par le tiers a été dûment évalué et est considéré comme suffisant au regard des intérêts en cause en matière de sécurité.

[8] La liste actuellement en vigueur comprend les États suivants: Australie, Bosnie-Herzégovine, Croatie, Ancienne République yougoslave de Macédoine, Islande, Israël, Liechtenstein, Monténégro, Norvège, Suisse, Ukraine et États-Unis d'Amérique. D'autres États sont engagés dans des négociations. Pour ce qui est des organisations internationales, la liste comprend: l'OTAN, la CPI et l'ASE. Il existe également des arrangements administratifs permanents avec les Nations Unies.

Si ces évaluations sont positives, le responsable du traitement affirme qu'elles conduiraient à la divulgation des données à caractère personnel en cause, sur le fondement de l'article 9, paragraphe 6, point d), du règlement (CE) nº 45/2001.

- Le responsable du traitement a également précisé que l'échange de données à caractère personnel peut être nécessaire avec des pays tiers et des organisations internationales avec lesquels il n'existe pas d'accords ou d'arrangements de sécurité, afin de protéger les intérêts du SEAE en matière de sécurité. Là encore, la divulgation de données à caractère personnel serait uniquement envisagée dans des cas exceptionnels, après une évaluation minutieuse du caractère adéquat du niveau de protection assuré par le tiers au regard:
    1. des intérêts vitaux de la personne concernée; ou
    2. des intérêts en cause en matière de sécurité.

Le responsable du traitement affirme que, si elles sont positives, ces évaluations conduiraient à la divulgation des données à caractère personnel en cause, conformément à l'article 9, paragraphe 6, point e) et/ou d) du règlement (CE) nº 45/2001 respectivement.

Enfin, il a été indiqué que, pour chaque destinataire, la finalité sera de satisfaire aux obligations découlant des règlements communautaires, des accords internationaux et/ou des arrangements administratifs et des lois nationales, le cas échéant, afin de permettre l'exécution des missions relevant de la compétence du Haut Représentant de l'Union pour les affaires étrangères et la politique de sécurité et/ou du SEAE.

2.6 Conservation des données

La politique de conservation suivante est applicable. Les données à caractère personnel conservées dans des dossiers papier et/ou électroniques, ainsi que dans la base de données, peuvent être conservées par l'administration pour une durée maximale de dix ans à compter de la clôture du dossier. Cette période correspond aux délais de prescription généralement admis en droit à l'égard des dossiers pénaux. Les agents chargés de la gestion des dossiers peuvent être appelés à témoigner par les organes compétents.

Les données à caractère personnel figurant dans la liste des personnes dont l'accès aux locaux du SEAE est interdit sont conservées pendant la durée strictement nécessaire à l'application de l'interdiction d'accès, et, en tout état de cause, au maximum cinq ans à compter de la mise en œuvre de la mesure.

2.7 Information des personnes concernées

Une déclaration de confidentialité sera publiée dans l'onglet Sécurité du site intranet du SEAE. Ce document contient des informations sur l'identité du responsable du traitement, la finalité de l'enquête de sécurité, la base juridique du traitement, les destinataires des données, l'existence des droits d'accès et de rectification, la durée de conservation et le droit de saisir le CEPD à tout moment.

De plus, des informations spécifiques supplémentaires sont fournies par différents canaux, en fonction des particuliers concernés:

- **Personne faisant l'objet d'une enquête (personne concernée)**

Lorsqu'il est possible de contacter la personne concernée, la fourniture d'informations s'effectue au moment de la collecte de la déclaration écrite de la personne concernée, laquelle se voit remettre immédiatement une copie de la déclaration de confidentialité. Dans d'autres cas, la personne concernée sera informée lors du premier contact après l'enregistrement. Le

SEAE considère que si l'information de la personne concernée éventuelle est susceptible de nuire à l'enquête menée par les organes compétents du SEAE ou par les autorités judiciaires, cette information doit être différée jusqu'à ce que ce ne soit plus le cas.

- **Informateurs, témoins et dénonciateurs**

La personne signalant un fait est automatiquement informée de la déclaration de confidentialité, si le contact se fait par e-mail. Si la déclaration est enregistrée par écrit en présence de la personne, une copie de la déclaration de confidentialité lui est immédiatement remise. Si le signalement est effectué par téléphone, la personne sera informée verbalement. Le responsable du traitement affirme que ces appels téléphoniques seront enregistrés afin de garantir l'authenticité du signalement (la capacité technique d'enregistrement n'était toutefois pas encore disponible à la date de l'analyse du contrôle préalable).

Les témoins interrogés sont informés de la déclaration de confidentialité au cours de l'interrogatoire et reçoivent aussi une copie de leur déclaration.

Comme l'explique le responsable du traitement, les dénonciations[9] peuvent également survenir dans le cadre d'enquêtes de sécurité et relèveraient de la catégorie d'informateur. Le responsable du traitement a en outre précisé que ces cas sont prévus par l'article 8 relatif aux infractions à la sécurité et à la compromission d'informations classifiées de la décision de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité du 15 juin 2011 relative aux règles de sécurité applicables au service européen pour l'action extérieure (2011/C 304/05), qui dispose que «toute infraction à la sécurité, réelle ou présumée, est immédiatement signalée à la direction de la sécurité du SEAE, qui en informe les autorités compétentes de la Commission, du secrétariat général du Conseil ou des États membres, si nécessaire».

- **Personnes dont l'accès aux locaux du SEAE est interdit**

Sur la base des informations fournies par le responsable du traitement, les personnes suspectes faisant l'objet d'une enquête de sécurité ne peuvent pas être informées préalablement de leur présence sur la liste, en raison du fait que cela pourrait entraver la procédure d'enquête. Elles ne seraient informées que si elles se présentent à un point d'accès. Le responsable du traitement indique qu'au terme de la procédure d'enquête, 1) la personne serait informée du fait que l'accès lui est interdit dans le cadre des mesures administratives éventuellement prises et que 2) si aucun élément de preuve n'a été trouvé contre le suspect à l'issue de l'enquête, les données de la personne seront immédiatement supprimées de la liste d'exclusion. D'après le responsable du traitement, il est considéré comme justifié de ne pas informer la personne concernée qu'elle a été suspectée, étant donné qu'elle n'aura pas été confrontée au fait qu'elle avait fait l'objet d'une enquête et que l'enquête sera clôturée sans aucune conséquence pour la personne concernée.

[9] Conformément à l'article 22 du statut des fonctionnaires, le fonctionnaire qui, dans l'exercice ou à l'occasion de l'exercice de ses fonctions, a connaissance de faits qui peuvent laisser présumer une activité illégale éventuelle, notamment une fraude ou une corruption, préjudiciable aux intérêts des Communautés, ou une conduite en rapport avec l'exercice de ses fonctions pouvant constituer un grave manquement aux obligations des fonctionnaires des Communautés, en informe immédiatement son supérieur hiérarchique direct ou son directeur général ou encore, s'il le juge utile, le secrétaire général, ou toute personne de rang équivalent, ou l'Office européen de lutte antifraude (OLAF).

2.8 Droits d'accès et de rectification
Les personnes concernées ont le droit de corriger les informations qu'elles ont fournies, soit immédiatement, soit ultérieurement, en remplissant et en envoyant une déclaration supplémentaire qui sera consignée dans le dossier. Cette possibilité est toujours communiquée lors de l'entretien avec les personnes concernées, mais elle est également énoncée dans la déclaration de confidentialité consultable dans l'onglet Sécurité du site intranet du SEAE.

Le responsable du traitement a également affirmé que lorsque l'accès aux données peut être préjudiciable à l'enquête ou aux droits et libertés d'autrui, l'accès à ces données peut être refusé, limité ou différé en vertu des exceptions mentionnées à l'article 20 du règlement 45/2001. Toute personne concernée peut alors saisir le CEPD, qui peut vérifier les données la concernant et, si nécessaire, les corriger ou les supprimer pour un motif légitime.

2.9 Sécurité

[...]

3. Aspects juridiques

3.1. Contrôle préalable

Applicabilité du règlement nº 45/2001 (ci-après le «règlement»): en premier lieu, le traitement de données constitue un traitement de données à caractère personnel [*«toute information concernant une personne physique identifiée ou identifiable»* - article 2, point a), du règlement]. En effet, comme l'indique la notification, les données à caractère personnel des 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 de données effectués ou non à l'aide de procédés automatisés», tels que définis à l'article 2, point b), du règlement (CE) nº 45/2001. Par exemple, lorsque l'on établit un rapport sur la base d'informations extraites de bases de données, d'enregistrements de vidéosurveillance, etc., qui sont ensuite conservées dans une base de données électronique, des données à caractère personnel font l'objet d'un traitement. Enfin, le traitement est effectué par un organe communautaire, en l'occurrence le SEAE, dans le cadre d'enquêtes de sécurité et dans l'exercice d'activités qui relèvent du droit communautaire. Dès lors, le CEPD considère que tous les éléments qui déclenchent l'application du règlement sont présents dans les traitements de données mis en œuvre par le SEAE.

Le «projet de décision de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité relative aux règles de sécurité applicables au service européen pour l'action extérieure» (ci-après «**le projet de décision»**) prévoit en son article 9, paragraphe 3, que «lorsque l'accès aux informations concerne des données privées contenues dans des systèmes de communication et d'information, ledit accès est conforme au règlement (CE) nº 45/2001». Le CEPD relève que cette limitation de l'applicabilité du règlement est contraire au règlement en tant que tel. En effet, l'article 3 du règlement nº 45/2001 prévoit que «[ce] règlement 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». L'applicabilité du règlement nº 45/2001 n'est donc pas limitée au traitement de données à caractère personnel par des systèmes de communication et d'information. Le projet de décision devrait ainsi être modifié de façon à en tenir compte.

Évaluation visant à établir si les traitements de données relèvent de l'article 27 du règlement. Le CEPD considère que le traitement de données relève clairement du cas prévu à l'article 27, paragraphe 2, du règlement (CE) nº 45/2001.

En premier lieu, de l'avis du CEPD, ces traitements de 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 infractions à la sécurité, des vols ou des accès non autorisés, le SEAE traitera des informations susceptibles d'être liées à des présomptions d'infractions ou de délits et à 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 responsable du traitement a également présenté la notification prévue à l'article 27, paragraphe 2, point d), concernant les traitements de données visant à exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat. Toutefois, le CEPD considère que seul le traitement visant à exclure des personnes de l'accès aux locaux du SEAE entre dans le champ d'application de cet article. De l'avis du CEPD, les autres traitements de données se rapportant à l'élaboration d'un rapport et à l'enregistrement dans des bases de données n'ont pas, en eux-mêmes, pour finalité d'exclure des personnes d'un droit, d'une prestation ou d'un contrat, même si cela est une conséquence potentielle. Par conséquent, l'article 27, paragraphe 2, point d) ne s'applique qu'à certains traitements de données.

La notification du DPD a été reçue le 21 novembre 2011. Conformément à l'article 27, paragraphe 4, du règlement, le présent avis doit être rendu dans un délai de deux mois. Une notification révisée limitant la portée de l'analyse a été envoyée le 23 juillet 2012. La procédure a été suspendue pendant une durée totale de 297 jours pour demander des informations complémentaires, puis pendant 15 jours pour permettre aux responsables du traitement de présenter des observations. La procédure a également été prolongée de deux mois au total en raison de la complexité du dossier. Dès lors, le présent avis doit être rendu avant le 1er février 2013.

3.2. Licéité du traitement

Le traitement des données à caractère personnel ne peut être effectué qu'en application des motifs visés à l'article 5 du règlement (CE) nº 45/2001.

La notification envoyée par le SEAE cite les articles 5, points a), b), d), et e) du règlement comme fondements juridiques. Toutefois, parmi les différents motifs énoncés à l'article 5 du règlement (CE) nº 45/2001, le CEPD considère que le traitement notifié en vue d'un contrôle préalable ne relève que du champ d'application de l'article 5, point a), en vertu duquel les données peuvent être traitées 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 de données sont conformes à l'article 5, point a), du règlement (CE) nº 45/2001, trois éléments doivent être pris en considération. Premièrement, si le traité ou d'autres actes législatifs prévoient les traitements de données effectués par le SEAE; deuxièmement, si les traitements de données sont réalisés dans l'intérêt public; et

troisièmement, si les traitements de données sont nécessaires. Bien entendu, ces trois conditions sont étroitement liées.

Motifs pertinents prévus dans le traité ou d'autres actes législatifs. Le CEPD prend note de l'éventail d'instruments juridiques décrits dans les faits, 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 de la réalisation d'enquêtes.

En ce qui concerne la décision du Conseil du 26 juillet 2010 fixant l'organisation et le fonctionnement du service européen pour l'action extérieure, article 10, paragraphe 2, sur la sécurité (2010/427/UE), le CEPD remarque que cet article prévoit que, dans l'attente de l'adoption de son propre règlement de sécurité en 2011, le SEAE a appliqué les mesures de sécurité prévues à l'annexe de la décision 2001/264/CE relative à la protection des informations classifiées, ainsi que les dispositions de la Commission en matière de sécurité définies dans l'annexe pertinente du règlement intérieur de la Commission concernant d'autres aspects liés à la sécurité.

Comme indiqué au point 2 ci-dessus, en présentant le projet de décision au CEPD, le responsable du traitement a fourni des informations supplémentaires concernant la base juridique. D'après les informations reçues, cette décision consolidée devrait porter sur les aspects pertinents des enquêtes et remplacer la base juridique utilisée aujourd'hui. L'article 9 relatif aux enquêtes menées sur les incidents de sécurité, les infractions à la sécurité et/ou les compromissions et les mesures correctives, et l'article 12 sur l'organisation de la sécurité au sein du SEAE, entre autres, sont jugés pertinents pour l'analyse de la licéité du traitement.

Le CEPD considère que les fondements juridiques énoncés plus haut, tant d'un point de vue général que d'un point de vue plus spécifique, prévoient l'existence du service de sécurité du SEAE et les pouvoirs dont il est investi concernant la conduite d'enquêtes et de vérifications. Ces fondements juridiques prévoient également, d'une manière générale, le type de traitements décrits dans la notification. Les actes juridiques susmentionnés permettent au bureau de sécurité du SEAE d'effectuer des traitements visant à obtenir des informations dans le but d'assurer des conditions de sécurité dans le fonctionnement des services du SEAE 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 le SEAE.

Les traitements de données sont effectués dans l'intérêt du public. Le CEPD remarque que le SEAE effectue les traitements dans l'exercice légitime de l'autorité publique dont il est investi. Comme l'indique l'énoncé de mission du SEAE, ce service est habilité à mener des enquêtes et est tenu de le faire avec l'objectif général de protéger le personnel, les biens physiques et les informations au sein du SEAE et dans le cadre des missions visées au titre V, chapitre 2 du TUE. Compte tenu de la nature de ces activités, il est clair 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 faits 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 SEAER, il apparaît nécessaire de traiter des données à caractère personnel. S'il ne procède pas au traitement de ces données, le SEAE 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 analysée in 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 d'informations relatives à des incidents (tels que décrits dans les faits ci-dessus) 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.

3.3. Traitement portant sur des catégories particulières de données

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 (CE) nº 45/2001, 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 3.2 ci-dessus.

En ce qui concerne les catégories particulières de données, l'article 10, paragraphe 1, du règlement nº 45/2001 dispose que «*le traitement des 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 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 nº 45/2001 soient traitées dans le cadre des enquêtes. Compte tenu de l'objectif général poursuivi par le SEAE lorsqu'il effectue des traitements de données, le CEPD croit comprendre que la collecte de catégories particulières de données n'est pas l'objectif principal du SEAE.

Le CEPD estime toutefois que, dans le cadre des enquêtes, le SEAE peut collecter et traiter, peut-être involontairement, des catégories particulières de données. La collecte et le traitement ultérieur de données sensibles ne sont autorisés que si celles-ci sont *nécessaires* dans le cas spécifique au regard de l'une des finalités visées à l'article 10, paragraphe 2. Étant donné que le traitement de données sensibles doit être considéré comme une exception plutôt que comme la règle, il y a lieu d'appliquer ici le critère de nécessité de manière restrictive.

À cet égard, le CEPD rappelle le principe de la qualité des données (aussi analysé de façon plus spécifique ci-dessous), 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.

3.4. 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 pour lesquelles elles sont 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, l'adresse, etc. figurent 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 devrait définir l'objet et l'étendue de l'enquête. Cela contribuerait à limiter les informations collectées à celles qui relèvent de l'enquête. Deuxièmement, 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 une enquête et à établir un rapport 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 3.7 ci-après).

3.5. 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 à la réalisation des finalités pour lesquelles elles sont collectées [et/]ou pour lesquelles elles sont traitées ultérieurement*».

Le CEPD accepte la durée de conservation de cinq ans pour les données à caractère personnel figurant dans la liste des personnes dont l'accès aux locaux du SEAE est interdit.

Le CEPD prend également note de la durée de dix ans à compter de la clôture du dossier applicable aux données à caractère personnel conservées par l'administration dans des dossiers papier et/ou électroniques ainsi que dans la base de données.

3.6. Transfert des 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 95/46/CE ou, au titre de l'article 9, vers d'autres types de destinataires.

Au vu des informations fournies par le responsable du traitement, les données ne peuvent être communiquées à des personnes autorisées au sein des institutions ou organes communautaires et des États membres de l'UE, des autorités judiciaires ou de police ou des entreprises sous-traitantes concernées que si nécessaire et sur la base du besoin d'en connaître. Les données peuvent également être transférées à des pays tiers et des organisations internationales conformément à des accords ou des arrangements spécifiques relatifs à la protection réciproque des informations classifiées, lorsque cela est nécessaire et que ledit pays tiers ou organisation internationale est impliqué dans le dossier.

Par conséquent, les articles 7, 8 et 9 sont applicables et doivent être analysés.

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 peuvent être communiquées à des institutions ou organes communautaires. En l'occurrence, ces organes sont l'OLAF, l'IDOC, le CEPD ou le Médiateur dans le cadre de leurs compétences respectives.

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»*.

D'après 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 ces transferts de données 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 au sein de l'institution ou de l'organe communautaire 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 nationale 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; et b) les États membres dans lesquels la législation nationale 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 95/46/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.

Transfert de données à caractère personnel aux pays tiers et organisations internationales
Pour les destinataires qui ne sont pas soumis à la directive 95/46/CE, l'article 9, paragraphe 1, du règlement nº 45/2001 dispose que «*le transfert de données à caractère personnel à des destinataires autres que les institutions et organes 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*». Dès lors, en principe, les données ne peuvent pas être transférées à des destinataires situés dans des pays non membres de l'EEE qui n'assurent pas un niveau de protection adéquat. Des dérogations peuvent toutefois s'appliquer aux termes de l'article 9, paragraphe 6, et de l'article 9, paragraphe 7.

Sur la base des informations reçues du responsable du traitement, le CEPD remarque que des accords ont été signés entre le Conseil européen et les pays tiers et organisations internationales concernant les échanges d'informations classifiées. Ces accords sont également mis en œuvre par le SEAE. Ils prévoient uniquement le transfert d'informations ICUE, qui peuvent contenir ou non des données à caractère personnel. Par conséquent, dans le cas où les ICUE à transférer contiennent des données à caractère personnel, le CEPD invite le SEAE à se conformer à l'article 9 du règlement.

En outre, l'article 9 devrait également être appliqué dans le cas où un transfert est effectué vers des pays tiers ou des organisations internationales avec lesquels le SEAE n'a pas conclu d'accord concernant l'échange d'informations classifiées.

En ce qui concerne l'applicabilité de l'article 9, paragraphe 6, points d) / e), dans de tels cas, le CEPD accepte provisoirement l'exception proposée, mais cette décision est prise sans préjudice de sa conclusion sur l'analyse de la question dans un «document d'orientation sur l'application de l'article 9 du règlement (CE) 45/2001: transfert de données à caractère personnel vers des pays tiers ou des organisations internationales», qui est actuellement en cours de rédaction.

3.7. 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 ou, dans certaines circonstances, indirectement par 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 le SEAE. 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 généralement conforme à l'article 13 du règlement (CE) nº 45/2001.

Si la déclaration de confidentialité ne prévoit pas la possibilité, dans certains cas, de reporter l'obligation de prévoir un accès/une rectification afin de préserver l'enquête, cette possibilité est prévue dans la notification, dans laquelle il est précisé que certaines données peuvent faire l'objet des exceptions visées à l'article 20 du règlement (CE) n° 45/2001 [notamment l'article 20, paragraphe 1, point a), et l'article 20, paragraphe 1, point c)]. Cela peut notamment être le cas si le SEAE 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 s'il doit se prévaloir d'une exception, le SEAE doit réaliser une évaluation au cas par cas des circonstances qui entourent le traitement des données en jeu.

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 dénonciateurs, 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 (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).

De plus, compte tenu des informations fournies dans la déclaration de confidentialité et la notification, le CEPD considère que, dans le cas d'enquêtes, si le SEAE se prévaut d'une exception pour reporter la fourniture d'informations, il ne devrait pas perdre de vue que les limitations d'un droit fondamental ne peuvent être appliquées de manière systématique. Le SEAE doit évaluer dans chaque cas si les conditions sont réunies pour appliquer une des exceptions prévues à l'article 20, paragraphe 1, point a) ou c). Par ailleurs, comme l'indique l'article 20 du règlement, la mesure doit être «nécessaire». Pour ce faire, il faut que le «test de nécessité» soit réalisé au cas par cas. Si le SEAE fait valoir une exception, il 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, le SEAE peut reporter la fourniture de ces informations en se prévalant de l'article 20, paragraphe 5, aux termes duquel «*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*».

Eu égard à ce qui précède, et contrairement à ce qui est stipulé dans la notification du SEAE, seuls les reports temporaires sont autorisés. Le SEAE ne peut pas définitivement «refuser» l'accès aux données. Dès lors, le mot «refuser» doit être supprimé de la déclaration de confidentialité.

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.

3.8. Information de la personne concernée

Le règlement dispose que la personne concernée doit être informée de la collecte des données la concernant, et il énumère plusieurs éléments qui doivent obligatoirement figurer dans les informations afin de garantir la transparence du traitement de données à caractère personnel.

Dans le présent dossier, les données pourraient être collectées directement auprès de la personne concernée ou indirectement, par exemple par l'intermédiaire d'informateurs.

Il convient de tenir compte du fait que toutes les exigences visées 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 qui seraient normalement traitées dans le cadre des activités de traitement analysées, les personnes concernées doivent avoir connaissance de toutes les garanties auxquelles elles ont droit.

Pour évaluer si le responsable du traitement des données fournit bien, en l'espèce, les informations en question à la personne concernée, deux questions doivent être examinées: tout d'abord dans quelle la mesure les informations ont été effectivement fournies et, deuxièmement, dans quelle mesure les informations fournies et leur contenu sont conformes au règlement (CE) nº 45/2001.

La voie de communication: selon la notification, la voie de communication par laquelle les personnes sont informées est une déclaration de confidentialité publiée dans l'onglet Sécurité du site intranet du SEAE. En outre, toujours selon la notification, les personnes, y compris la personne signalant des faits, les personnes concernées, le (les) témoin(s) et le (les) dénonciateur(s), en cas de déclarations écrites ou orales, sont automatiquement informées de la déclaration de confidentialité, par écrit ou verbalement. Tel ne sera pas le cas, a fortiori, lorsque ces personnes ne sont pas entendues ou ne fournissent pas de déclarations écrites[10].

Le CEPD estime que la pratique de la publication d'informations dans l'onglet Sécurité du site intranet du SEAE est positive au regard de l'information des personnes concernées. Mais ceci ne saurait être considéré comme suffisant dans le cas d'espèce. Le CEPD recommande donc que le SEAE adopte une procédure permettant de fournir la déclaration de confidentialité à chacune des personnes concernées au sujet desquelles des données à caractère personnel sont collectées.

En ce qui concerne les informateurs, les témoins et les dénonciateurs, le CEPD recommande que les informations soient également fournies individuellement à chaque personne concernée, indépendamment du fait qu'elle soit ou non interrogée.

Toutefois, le CEPD remarque que si le SEAE reçoit des informations par le biais d'appels téléphoniques, il est prévu que ceux-ci soient enregistrés afin de garantir l'authenticité du rapport. Cette possibilité technique n'était pas encore disponible à la date de rédaction du présent avis mais elle est prévue dans la notification. Dans ce cas, les personnes concernées doivent également être informées du fait que l'appel est enregistré. Or, cela n'est pas mentionné dans les informations transmises au CEPD. Le CEPD invite le SEAE à prendre des mesures appropriées pour informer correctement les personnes concernées dont les appels peuvent être enregistrés.

Quant à l'applicabilité de l'article 20 du règlement, qui permet au SEAE de reporter la fourniture d'informations, le CEPD renvoie aux observations formulées ci-dessus à propos du droit d'accès et du fait que la limitation d'un droit fondamental ne peut être appliquée de manière systématique. Dans ce cas, le SEAE doit réaliser une évaluation au cas par cas des circonstances qui entourent le traitement des données en jeu.

[10] Comme indiqué dans la notification, si la (les) personne(s) concernée(s) n'est (ne sont) pas joignables, elle(s) sera (seront) informée(s) lors du premier contact après l'enregistrement.

Enfin, si le SEAE fait valoir une exception, il 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, le SEAE peut reporter la fourniture de ces informations en se prévalant de l'article 20, paragraphe 5, aux termes duquel «*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 le droit de la personne concernée 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).

En conséquence, le CEPD ne partage pas le point de vue du SEAE concernant l'absence d'information de la personne concernée lorsqu'aucune preuve n'a été trouvée contre le suspect au terme de l'enquête. Dès lors, conformément au raisonnement exposé ci-dessus, le CEPD ne peut accepter l'argument du SEAE selon lequel «*il est justifié de ne pas informer la personne concernée qu'elle a été suspectée, étant donné qu'elle n'aura pas été confrontée au fait qu'elle avait fait l'objet d'une enquête et que l'enquête sera clôturée sans aucune conséquence pour la personne concernée*».

L'application d'une telle procédure sans informer la personne concernée serait contraire au règlement n° 45/2001 et au droit d'information des personnes concernées, dans le cadre d'un traitement de données à caractère personnel effectué par l'institution, et pourrait à terme conduire au dépôt de plaintes contre l'institution. Le SEAE doit donc modifier cet aspect de la procédure.

Le contenu de la déclaration de confidentialité: il est indiqué dans la notification, dans le chapitre relatif aux informations à fournir aux personnes concernées et aux moyens de communication utilisés, que «l'existence des bases de données et du processus permettant de faire vérifier les données qui y sont stockées par le CEPD, et, le cas échéant, de les rectifier si elles sont incorrectes, fait l'objet d'une déclaration publiée dans l'onglet Sécurité du site intranet du SEAE». Le CEPD considère que ce libellé est incomplet au regard des exigences prévues aux articles 11 et 12. Le libellé devrait donc être modifié afin de tenir compte de cette situation.

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 saisir le Contrôleur européen de la protection des données. Le CEPD estime toutefois que la description des délais prévus pour la conservation 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. Par conséquent, il demande au SEAE de compléter la déclaration de confidentialité à cet égard (voir point 3.5 ci-dessus). En outre, le CEPD considère que la finalité devrait être décrite de façon plus détaillée. En effet, la déclaration actuelle se limite à préciser que «ce traitement a pour finalité de mener des enquêtes de sécurité».

3.9. Confidentialité des communications

L'article 36 du règlement dispose que «*[l]es institutions et organes communautaires garantissent la confidentialité des communications réalisées au moyen de réseaux de*

télécommunications et des équipements de terminaux dans le respect des principes généraux du droit communautaire». Le concept de «principes généraux du droit communautaire» renvoie également à la notion de droits fondamentaux de la personne, tels qu'établis notamment par la Convention européenne des droits de l'homme. Toute limitation de la confidentialité des communications doit donc être conforme à l'article 8, paragraphe 2, dudit instrument: *«Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui»*.

Cette disposition doit être respectée lorsque des contrôles des communications électroniques sont réalisés, notamment lors de l'inspection de messages électroniques. Le SEAE se réfère à l'information administrative nº 45/2006 de la Commission du 15.09.2006 qui est appliquée par le SEAE. Toutefois, le fait de se référer à l'information administrative de la Commission ne permet pas de déterminer si le SEAE effectuerait les «recherches» lui-même ou si, comme l'indique la note d'information, cette mission serait également exécutée par les services de l'IDOC de la Commission. De plus, le projet de décision consolidée qui a été remis au CEPD se borne à préciser que c'est la direction de la sécurité du SEAE qui mène les enquêtes ou les vérifications et qui met en œuvre toutes les mesures correctives qui s'imposent dans le cadre des enquêtes[11].
Le CEPD invite donc le SEAE à adopter une procédure spécifique portant sur les contrôles de communications électroniques qui peuvent être effectués.

En tout état de cause, après avoir pris en considération les exigences visées à l'article 8, paragraphe 2, de la Convention européenne des droits de l'homme et des libertés fondamentales, il convient dès lors d'examiner les limitations du principe de confidentialité à la lumière des critères suivants[12]:

- La limitation est-elle autorisée par une disposition juridique ou une mesure équivalente?

- Est-elle nécessaire? Le même résultat pourrait-il être obtenu sans enfreindre le principe de confidentialité? La surveillance de l'utilisation personnelle de la messagerie électronique (pour une raison autre que la détection de virus) ou de

[11] L'article 9 du projet de décision prévoit précisément:

> 1. La direction de la sécurité du SEAE, assistée d'experts issus des États membres et/ou d'autres institutions communautaires, selon le cas, et après autorisation du directeur général administratif, le cas échéant, doit:
>
> a) mener des enquêtes ou des vérifications, selon le cas:
>
> i) lorsqu'il est avéré ou qu'il existe des motifs raisonnables de supposer que des informations classifiées concernant le SEAE ont été compromises ou perdues;
>
> ii) sur toute infraction à la sécurité, réelle ou présumée, ou tous autres incidents de sécurité ou menaces pesant sur les intérêts du SEAE en matière de sécurité;
>
> b) mettre en œuvre toutes les mesures correctives qui s'imposent, le cas échéant, dans le cadre des enquêtes.
>
> 2. Les enquêteurs ont accès à toutes les informations nécessaires pour mener lesdites enquêtes et bénéficient du soutien total de l'ensemble des services du SEAE à cet égard.
>
> Les enquêteurs peuvent prendre des mesures appropriées pour protéger l'ensemble de preuves de manière proportionnelle à la gravité de l'affaire examinée.

[12] Il convient de remarquer à cet égard que la question du contrôle ou de l'inspection des communications électroniques («e-monitoring») sera traitée séparément par le CEPD dans le cadre de lignes directrices horizontales.

l'Internet par un agent ne peut être considérée comme nécessaire que dans des circonstances exceptionnelles.

- Est-elle proportionnée aux préoccupations qui la motivent? Le principe de proportionnalité signifie que l'application de limitations à la confidentialité des communications diffèrera selon qu'il s'agisse de communications personnelles ou de communications professionnelles. Il signifie également que, s'il est nécessaire de vérifier la messagerie électronique de travailleurs en leur absence, cette vérification devrait en principe être limitée aux messages électroniques qui ne sont pas marqués comme étant privés ou personnels ou qui sont adressés à l'institution.

En ce qui concerne le contrôle des communications électroniques, le CEPD élabore actuellement des lignes directrices portant sur le traitement des données de communications électroniques par les institutions et organes européens.

3.9. Mesures de sécurité

Conformément aux 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 CEPD n'a aucune raison de croire que le SEAE n'a pas mis en œuvre des mesures techniques et organisationnelles appropriées permettant d'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, et qui correspondent aux mesures mises en place dans les autres institutions communautaires.

Conclusion:

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

- Le SEAE devrait modifier le projet de décision de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité relative aux règles de sécurité applicables au service européen pour l'action extérieure lorsqu'il décrit le champ d'application du règlement nº 45/2001 qui est actuellement mentionné en son article 9;
- 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, à des autorités nationales (de police et judiciaires), ainsi qu'à des pays tiers ou organisations internationales, 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;
- Le SEAE devrait documenter les procédures dans le cas d'un transfert de données à caractère personnel vers des pays tiers ou des organisations internationales faisant l'objet d'accords relatifs aux ICUE. Le CEPD se réserve le droit d'apporter des précisions à sa position concernant ces transferts après l'adoption d'un document stratégique sur le transfert;
- Le SEAE devrait établir des procédures permettant d'informer les différentes catégories de personnes concernées, de prendre des mesures appropriées au regard du contenu des informations fournies et de modifier sa notification à la lumière des observations formulées ci-dessus;
- La déclaration de confidentialité devrait être modifiée de la manière suggérée dans différents points du présent avis.
- [...]

Fait à Bruxelles, le 1er février 2013

(**signé**)

Giovanni BUTTARELLI