Avis sur la notification d'un contrôle préalable reçue du Délégué à la protection des données de la Commission européenne à propos du dossier "Traitement des demandes de levée de l'immunité de juridiction et d'inviolabilité des locaux et archives de la Commission"

Bruxelles, le 25 mars 2009 (Dossier 2008-645)

1. Procédure

Par e-mail en date du 31 octobre 2008, le Délégué à la protection des données (DPD) de la Commission européenne a soumis au Contrôleur européen de la protection des données (CEPD) une notification dans le sens de l'article 27.3 du règlement (CE) 45/2001 (ci-après "le règlement"), concernant le dossier "Traitement des demandes de levée de l'immunité de juridiction et d'inviolabilité des locaux et archives de la Commission".

Le 3 décembre 2008, des informations complémentaires ont été demandées au DPD. Ces dernières ont été reçues le 9 février 2009. Le 6 mars 2009, le projet d'avis du CEPD a été envoyé au DPD afin de lui permettre d'apporter ses commentaires. Ces derniers ont été reçus le 23 mars 2009.

2. Les faits

Le Protocole sur les Privilèges et Immunités des Communautés européennes ("PPI")[1] établit un certain nombre d'immunités au profit des fonctionnaires et agents des Communautés, telles que notamment (i) l'immunité de juridiction, (ii) l'inviolabilité des locaux, et (iii) l'inviolabilité des archives des Communautés, comme suit:

i. En vertu de l'article 12 du PPI, les fonctionnaires et autres agents des Communautés jouissent de l'immunité de juridiction *"pour les actes accomplis par eux, y compris leurs paroles et écrits, en leur qualité officielle (...). Ils continueront à bénéficier de cette immunité après la cessation de leurs fonctions"*.

ii. En vertu de l'article 1er du PPI, *"les locaux et les bâtiments des Communautés sont inviolables. Ils sont exempts de réquisition, confiscation ou expropriation"*.

iii. En vertu de l'article 2 du PPI, *"les archives des Communautés sont inviolables."*

[1] Protocole (n°36) sur les privilèges et immunités des Communautés européennes (1965), *Journal officiel n° C 321 E du 29/12/2006 p. 0318 - 0324.*

En vertu de l'article 18, paragraphe 2 du PPI, *"chaque institution des Communautés est tenue de lever l'immunité accordée à un fonctionnaire ou autre agent dans tous les cas où elle estime que la levée de cette immunité n'est pas contraire aux intérêts des Communautés"*. L'article 19 du PPI pose un principe de coopération loyale entre les autorités responsables des Etats membres concernés et les institutions en vertu duquel une institution européenne est tenue de lever l'immunité en question sauf à démontrer que cela constituerait une entrave aux intérêts des Communautés ou, dans le cas de demande de levée de l'inviolabilité des archives, que cela porterait atteinte aux droits légitimes des tiers (voir CJCE, C-275/00, *First and Franex*).

A cette fin, la Commission a mis en place un traitement de données ayant pour finalité, en réponse à la demande d'une juridiction nationale, ou de toute autre entité nationale ayant autorité pour procéder à une enquête, à autoriser, ou non, la comparution d'un fonctionnaire ou d'un agent en justice, et/ou l'accès aux locaux et/ou aux archives de la Commission européenne.

Les ***personnes concernées*** sont les fonctionnaires et les anciens fonctionnaires ainsi que le personnel soumis et ayant été soumis au Régime applicable aux autres agents (RAA) pour lesquels une instruction judiciaire requiert (i) qu'ils fassent état en justice des constatations faites en raison de leur fonction, et/ou (ii) qu'une autorité compétente perquisitionne les locaux qu'ils occupent ou qu'ils ont occupé, et/ou (iii) qu'une autorité compétente accède aux archives les concernant.

La procédure d'examen de la requête donne lieu au ***traitement de données*** suivant:

i. Dans le cadre d'une instruction judiciaire, l'autorité judiciaire nationale transmet sa demande de levée d'immunité de juridiction, d'inviolabilité des locaux, et/ou d'inviolabilité des archives de la Commission à un service de contact de la Commission (Directeur général du personnel et de l'administration, Secrétaire Générale, Directeur général de l'OLAF, et/ou un service de la Commission en cas de demande de levée de l'inviolabilité des locaux).

ii. Dans la plupart des cas, les autorités nationales demandent expressément à la Commission de ne pas informer la ou les personne(s) concernée(s) de la demande faite par l'autorité nationale ni de la décision prise par la Commission pour y donner suite, ceci afin de ne pas entraver le déroulement de l'instruction.

iii. Dès leur arrivée, les demandes reçoivent un numéro d'enregistrement dans le "Case Management System" ("CMS") de l'Office d'investigation et de discipline de la Commission ("IDOC"). Les demandes de levée de l'inviolabilité des locaux et/ou de levée de l'inviolabilité des archives qui sont introduites concomitamment à une demande de levée de l'immunité de juridiction font l'objet d'un même numéro d'enregistrement.

iv. L'IDOC instruit les demandes en collaboration avec l'OLAF, le Secrétariat général et le Service juridique de la Commission. L'IDOC prépare le projet de décision de la Commission, qui est transmis pour avis et accord à l'OLAF, au Secrétariat général et au Service juridique.

v. Lorsque le secret de l'instruction a été demandé par l'autorité nationale, une version nominative du projet de décision est déposée au Secrétariat général dans un lieu sécurisé dont l'accès est strictement réglementé, et seule une version anonyme du projet de décision est diffusée par le Secrétariat général.

vi. La décision de levée de l'immunité est adoptée selon un processus différent en fonction de l'immunité en cause, comme suit:

- Concernant la procédure de demande de levée de l'immunité de juridiction, le dossier de la procédure écrite est transmis au Directeur général et au cabinet du Président et du membre chargé du personnel pour signature. La décision est adoptée par la Secrétaire Générale, et envoyée au demandeur soit par le Secrétariat général soit par l'intermédiaire de l'OLAF.

- En cas de demande de levée de l'inviolabilité des locaux de la Commission, la décision est transmise à la DG chargée du personnel pour signature. La décision est adoptée par le Directeur chargé du personnel et de l'administration en accord avec la Secrétaire Générale et envoyée au demandeur soit par l'IDOC soit par l'OLAF. La Direction Sécurité de la DG ADMIN est informée de la décision pour faciliter l'accès aux locaux lors de la perquisition.

- En cas de demande de levée de l'inviolabilité des archives de la Commission, la décision est transmise à la DG chargée du personnel pour signature. La décision est adoptée par le Directeur chargé du personnel et de l'administration en accord avec la Secrétaire Générale et envoyée au demandeur soit par l'IDOC soit par l'OLAF. Le(s) service(s) dépositaire(s) des documents demandés est informé de la décision de levée de l'inviolabilité des archives en vue de la transmission desdits documents. La Direction Sécurité de la DG ADMIN est également informée de la décision afin d'assurer l'exécution de la décision.

vii. Lorsque le secret n'est pas expressément demandé par les autorités nationales, la personne concernée est informée par l'IDOC de la décision de la Commission ou de l'AIPN compétente dans les jours qui suivent l'adoption de cette décision, dont elle reçoit copie. En cas de demande de maintien du secret de la procédure, la décision prise soit par la Commission (levée de l'immunité de juridiction) soit par l'AIPN compétente (levée de l'inviolabilité des locaux ou des archives) n'est communiquée à la personne concernée qu'une fois la Commission informée du fait que le secret de la procédure ne s'impose plus.

Le traitement des données est à la fois ***manuel et automatisé***. Les éléments nécessaires à la gestion du dossier (demande de l'autorité nationale, information des autres services, décision de la Commission, archivage du dossier) sont placés dans des dossiers papiers. Les documents émis par l'IDOC sont conservés électroniquement.

Les ***données personnelles*** traitées concernent (i) des données relatives à l'identité de la personne en cause telles que nom, adresse, situation familiale, carrière, fonctions à la Commission; (ii) des données relatives au comportement, à l'action ou à l'inaction

alléguée à son encontre; et (iii) des données relatives aux procédures judiciaires dont elle fait l'objet ou dans lesquelles elle se trouve impliquée.

Les dossiers sont gérés par les gestionnaires responsables de l'unité IDOC. Les données sont ***transmises*** aux services de la Commission associés dans le processus décisionnel (Secrétariat Général, Service Juridique, OLAF, AIPN). La Direction Sécurité de la DG ADMIN, et/ou le(s) service(s) dépositaire des documents en cas d'accès aux archives, sont informés de la décision prise par la Commission pour assurer la bonne exécution de cette décision le moment venu. Seules les personnes ayant un besoin d'information aux fins d'accomplissement de leurs tâches sont destinataires de ces informations.

Les demandes de levée de l'immunité de juridiction, de l'inviolabilité des locaux et/ou des archives de la Commission bénéficient des mesures applicables aux enquêtes et procédures disciplinaires dont l'IDOC est en charge afin d'en garantir la ***confidentialité***. [...]

Les données nécessaires à la gestion du dossier (demande des autorités nationales, échanges avec les services consultés, et décision de la Commission) sont ***conservées*** dans les archives de l'IDOC jusqu'à la clôture de la procédure nationale ou, à défaut d'information à cet égard, pendant une période maximale de vingt ans. En cas d'ouverture d'une procédure disciplinaire à l'encontre de la personne, les documents relatifs à l'immunité de juridiction sont versés au dossier disciplinaire de l'intéressé et conservés pour une période de vingt ans à compter de la clôture de la procédure disciplinaire.

Les ***droits d'accès et de rectification*** sont garantis à la personne concernée. La clause de confidentialité du traitement expose leur limite. Le droit d'accès peut être limité et différé à la demande expresse de l'autorité nationale qui a introduit la requête lorsque celle-ci invoque le secret de l'instruction. Dans un tel cas, la personne ne peut exercer sont droit d'accès au dossier CMS contenant l'ensemble des données la concernant qu'à partir du moment où l'exception d'enquête n'est plus applicable. La personne est également informée de son droit de saisir le CEPD, dans les circonstances prévues à l'article 20.4 du règlement (CE) 45/2001. En l'absence d'invocation du secret de l'instruction, la personne est informée, sans retard, de la demande faite à la Commission et des suites que celle-ci entend lui réserver, et elle peut accéder au dossier CMS contenant l'ensemble des données la concernant à tout moment sur simple demande écrite adressée au Directeur de l'IDOC.

La personne est **informée** de la procédure relative à la levée d'immunité par la ***clause de confidentialité***. Cette clause de confidentialité est remise à l'intéressé en annexe à la lettre par laquelle celui-ci est informé de la demande des autorités judiciaires nationales le concernant; cette information intervient dès que possible lorsque le secret de la procédure ne s'applique pas ou ne s'applique plus. Cette clause sera en outre prochainement accessible sur le site intranet de l'IDOC.

La clause de confidentialité reprend les informations suivantes: identité du responsable du traitement; finalité du traitement; base juridique; catégories de données traitées; les destinataires des données; les mesures de sécurité; la durée de

conservation des données; le droit d'accès, de rectification et de suppression des données et ses modalités; le droit de recours auprès du CEPD.

3. Les aspects légaux

3.1. Contrôle préalable

Le contrôle préalable porte sur le traitement de données à caractère personnel ("*toute information concernant une personne physique identifiée ou identifiable*" - article 2.a du règlement (CE) 45/2001) dans le contexte du traitement des demandes de 1) levée de l'immunité de juridiction des fonctionnaires et autres agents de la Commission, et/ou 2) levée de l'inviolabilité des locaux de la Commission, et/ou 3) levée de l'inviolabilité des archives de la Commission.

Le traitement de données est effectué par une institution et est mis en œuvre pour l'exercice d'activités relevant du champ d'application du droit communautaire (article 3.1 du règlement). Le traitement de données est à la fois manuel et automatisé. L'article 3.2 du règlement est donc applicable en l'espèce. Dès lors, ce traitement tombe sous le champ d'application du règlement (CE) 45/2001.

L'article 27.1 du règlement soumet au contrôle préalable du CEPD tous "*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 27.2 contient une liste des traitements susceptibles de présenter de tels risques.

L'article 27.2.a du règlement présente comme traitements susceptibles de présenter de tels risques "les traitements de données relatives à la santé et les traitements de données relatives à des suspicions, infractions, condamnations pénales ou mesures de sûreté". Le traitement "demandes de levée de l'immunité de juridiction et d'inviolabilité des locaux et archives de la Commission" traite plus particulièrement des données relatives à des suspicions, infractions, condamnations pénales et tombe dès lors dans le champ d'application de l'article 27.2.a.

En principe, le contrôle effectué par le CEPD est préalable à la mise en place du traitement. A défaut, le contrôle devient par la force des choses "a posteriori". Ceci n'enlève rien à la mise en place souhaitable des recommandations présentées par le CEPD.

La notification du DPD a été reçue le 31 octobre 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. En raison des 68 jours jours de suspension pour informations complémentaires, le CEPD rendra son avis pour le 27 mars 2009 au plus tard.

3.2. Base légale et licéité du traitement

La licéité du traitement doit être examinée à la lumière de l'article 5.a du règlement. Cet article prévoit que le traitement 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 relevant de l'exercice légitime de l'autorité publique dont est investie l'institution".

La Commission ne peut entraver le cours de la justice et doit donc, lorsque les intérêts des Communautés ne l'exigent pas, lever les immunités prévues dans le Protocole sur les Privilèges et Immunités des Communautés Européennes. Il s'agit bien d'une mission effectuée dans l'intérêt public sur la base des traités. Il s'agit en outre d'une obligation légale telle que prévue à l'article 5.b du règlement. La licéité du traitement est donc respectée.

La base légale est dans le cas présent particulièrement importante, les données traitées pouvant en effet être sensibles. La base légale du traitement repose sur l'article 18, paragraphe 2, du PPI qui dispose que *"chaque institution des Communautés est tenue de lever l'immunité accordée à un fonctionnaire ou autre agent dans tous les cas où elle estime que la levée de cette immunité n'est pas contraire aux intérêts des Communautés."* La base légale est conforme et vient à l'appui de la licéité du traitement.

D'après la description du traitement, le CEPD constate que le traitement peut également porter sur des données sensibles dans le sens de l'article 10 du règlement.

3.3. Traitement portant sur des catégories particulières de données

L'article 10.5 du règlement 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 (...)"*. En l'espèce, la levée d'immunité est spécifiquement prévue à l'article 18 du Protocole sur les Privilèges et Immunités des Communautés européennes, protocole qui figure en annexe du Traité instituant la Communauté européenne. L'article 19 du PPI pose également un principe de coopération entre les autorités nationales et les institutions concernant le traitement des demandes de levée d'immunité, ce qui induit notamment la communication par les autorités nationales, et leur traitement par la Commission, d'informations justifiant la levée d'une telle immunité telle que notamment des suspicions d'infractions et allégations à l'encontre de la personne concernée. Le traitement concerné s'inscrit dans le cadre du PPI et respecte par conséquent l'article 10.5 du règlement.

3.4. Qualité des données

L'article 4 du règlement énonce certaines obligations en ce qui concerne la qualité des données à caractère personnel. "*Les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement*" (article 4.1.c). Il convient donc de vérifier que les données sont en relation avec la finalité du traitement pour lequel elles sont traitées.

Le CEPD considère que les données traitées qui sont décrites au début du présent avis doivent être considérées comme satisfaisant à ces conditions en liaison avec les finalités du traitement expliquées ci-dessus. Les données collectées paraissent être

nécessaires pour la gestion des demandes de levée des immunités émises par des autorités nationales dans le cadre d'une information ou d'une instruction judiciaire. Le CEPD estime que l'article 4.1.c du règlement (CE) 45/2001 est respecté à cet égard.

De plus, les données doivent être traitées "*loyalement et licitement*" (article 4.1.a du règlement). La licéité du traitement a déjà fait l'objet d'une analyse (voir supra, point 3.2). Quant à la loyauté du traitement, dans le cadre d'un sujet aussi sensible, elle doit faire l'objet d'attention spécifique. Elle est en relation avec l'information donnée aux personnes concernées (voir infra, point 3.8).

Enfin, les données doivent être "*exactes et, si nécessaire, mises à jour: 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*" (article 4.1.d du règlement). Dans les limites de l'article 20 du règlement, les droits d'accès et de rectification sont à la disposition de la personne concernée afin de rendre le dossier le plus complet possible. Ils représentent la possibilité d'assurer la qualité des données. Concernant ces deux droits d'accès et de rectification, voir point 3.7 ci-après.

3.5. Conservation des données

L'article 4.1.e du règlement pose le principe que les données 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*".

Les données nécessaires à la gestion du dossier, ainsi que la décision de la Commission/AIPN, sont conservées dans les archives de l'IDOC jusqu'à la clôture de la procédure nationale ou, à défaut d'information à cet égard, pendant une période maximale de vingt ans. En cas d'ouverture d'une procédure disciplinaire à l'encontre de la personne par la Commission, les documents relatifs à l'immunité de juridiction sont versés au dossier disciplinaire de l'intéressé et conservés pour une période de vingt ans à compter de la clôture de la procédure disciplinaire.

Le CEPD estime que cette durée de conservation sur le long terme doit être accompagnée de garanties appropriées. Le fait que les données soient archivées pour une conservation sur le long terme ne leur ôte pas le caractère de données personnelles.

Par ailleurs, la durée de conservation doit être réévaluée en fonction de l'évolution du dossier, notamment du fait de l'abandon des procédures disciplinaires et/ou contentieuses, ou de l'acquittement de la personne en justice.

En outre, la Commission doit veiller à définir les catégories exactes de personnes qui ont droit d'accéder à ces données/archives et les finalités pour lesquelles elles ont accès à ces données.

3.6. Transferts des données

Les données à caractère personnel collectées dans le cadre du traitement examiné font l'objet de transferts (i) entre institutions ou organes communautaires ou en leur sein (article 7 du règlement), et (ii) à des destinataires autres que les institutions et organes communautaires (articles 8 et 9 du règlement).

(i) Transferts vers des institutions ou organes communautaires ou en leur sein

En vertu de l'article 7.1 du règlement, les transferts de données vers des institutions communautaires ou en leur sein peuvent être effectuées "*si nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire*".

Nous sommes dans le cas de transferts au sein d'une même institution. Les destinataires du traitement sont notamment le Secrétariat Général, le Service Juridique, l'IDOC, l'AIPN en charge de la gestion des dossiers, et le service de la Commission en contact avec l'autorité nationale (ADMIN, OLAF, SG, etc.) afin de lui transmettre la décision prise par la Commission. Certains services spécifiques reçoivent communication de la décision de l'AIPN: c'est le cas de la direction sécurité de la DG ADMIN et/ou du service dépositaire des documents en cas d'accès aux archives, ceci afin de faciliter l'accès le moment venu par les autorités compétentes aux locaux et/ou aux archives concernés.

Au vu des éléments fournis dans la notification, il apparaît que de tels transferts sont en conformité avec l'article 7.1, puisque les données collectées sont nécessaires à la réalisation du traitement et que par ailleurs les données sont "*nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire*".

L'article 7.3 du règlement dispose en outre que "*le destinataire traite les données à caractère personnel uniquement aux fins qui ont motivé leur transmission*". Compte tenu de la sensibilité des données traitées, il doit être rappelé aux destinataires que les données ne doivent être traitées que dans le but de traiter les demandes de levée d'immunités aux fins d'autoriser une personne à comparaître en justice et/ou une perquisition des lieux ou archives la concernant.

(ii) Transferts vers des destinataires autres que les institutions communautaires

Dans le cas d'espèce, la décision de la Commission/AIPN est communiquée à l'autorité nationale qui demande la levée de l'immunité. 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, (...)".* Dans le cas d'espèce, ce sont les

autorités judiciaires qui ont fait la demande de levée de l'immunité et qui ont à cette occasion, démontré la nécessité du transfert de données puisque ces données sont nécessaires afin de rendre la justice.

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.

Si l'autorité nationale se trouve dans un pays ne relevant pas de la directive 95/46/CE, l'article 9 du règlement est également d'application. En vertu de cette disposition, le transfert ne peut avoir lieu que vers un pays offrant un niveau de protection adéquat. Si tel n'est pas le cas, le traitement devra se fonder sur les exceptions prévues à l'article 9.6, par exemple l'article 9.6.d : "*le traitement est nécessaire ou rendu juridiquement obligatoire pour des motifs d'intérêts public important ou pour la constatation, l'exercice ou la défense d'un droit en justice, (...)* ".

En tout état de cause au vu de la nature des données échangées dans le cas d'espèce, le CEPD recommande que tout transfert de données vers des destinataires autres que les institutions communautaires soit enregistré par la Commission ainsi que la justification légale en vertu de laquelle un tel transfert a été effectué.

3.7. Droit d'accès et de rectification

L'article 13 du règlement prévoit le droit d'accès - et ses modalités - à la demande de la personne concernée par le traitement. En application de l'article 13 du règlement, la personne concernée a notamment 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.

L'article 14 du règlement prévoit également le droit de rectification de ses données par la personne concernée. De la même façon que la personne concernée dispose du droit d'accès, cette dernière peut aussi faire modifier ses données personnelles si nécessaire.

Pour rappel, les droits d'accès et de rectification sont garantis à la personne concernée. Ces droits, et les modalités de leur exercice, sont indiqués dans la clause de confidentialité (cf section 3.8 ci-dessous). Ces deux droits peuvent être limités et différés à la demande de l'autorité nationale qui invoque le secret de la procédure, conformément à l'article 20.1 du règlement.

L'article 20, paragraphe 5, dispose en outre 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 de différer cette information conformément à cette disposition, afin de protéger l'enquête. Le CEPD rappelle toutefois que cette mesure dérogatoire doit rester temporaire, et que la personne doit pouvoir exercer son droit d'accès dès que le secret de la procédure n'est plus justifié.

Dans les cas où l'information de la personne et l'exercice de ses droits sont différés, la personne est informée par la clause de confidentialité, lorsque celle-ci lui est remise, du fait qu'elle peut saisir le CEPD afin de vérifier si les données ont été traitées, ce qui respecte les dispositions de l'article 20.4 du règlement.

L'article 14 du règlement accorde à la personne concernée le droit à la rectification des données inexactes ou incomplètes. 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. Si aucune limitation découlant de l'article 20.1 n'est d'application - notamment s'il n'y a pas de demande de secret de la procédure de la part de l'autorité nationale - le CEPD rappelle que la personne concernée doit avoir la possibilité de s'exprimer sur l'affaire qui la concerne avant que la décision de la Commission/AIPN ne soit prise. Les commentaires faits par la personne concernée doivent être consignés dans son dossier personnel. Cette recommandation mise à part, le CEPD estime que les articles 13 et 14 du règlement sont respectés.

3.8. Information des personnes concernées

Les articles 11 et 12 du règlement portent sur les informations à fournir à la personne concernée afin de garantir un traitement transparent de ses données à caractère personnel. Ces articles énumèrent une série de mentions obligatoires et facultatives. Ces dernières sont applicables dans la mesure où, compte tenu des circonstances particulières du traitement en l'espèce, elles sont nécessaires afin d'assurer un traitement loyal des données à l'égard de la personne concernée.

Dans le cas présent, les données relatives à la demande de levée d'une immunité ne sont pas collectées directement auprès de la personne concernée, mais sont transmises par l'autorité nationale au service de la Commission avec laquelle elle est en contact. Les dispositions de l'article 12 (*Informations à fournir lorsque les données n'ont pas été collectées auprès de la personne concernée)* sont par conséquent applicables en l'espèce.

Une information générale est prévue pour les personnes concernées via la clause de confidentialité spécifique aux demandes de levée d'immunité de juridiction et d'inviolabilité des locaux et archives de la Commission, disponible sur intranet. La clause de confidentialité contient toutes les mentions, obligatoires et facultatives, prescrites à l'article 12 du règlement.

En ce qui concerne l'information spécifique, c'est à dire lorsqu'une personne concernée fait l'objet d'une demande de levée d'immunité, elle doit être informée du traitement au plus tard à la première communication des données si la demande a été faite via un des services de la Commission. Ceci est le cas en l'espèce toutes les fois que l'autorité nationale n'invoque pas le secret de la procédure.

Il se peut par ailleurs que cette information soit différée, conformément à l'article 20.1 du règlement, à la demande de l'autorité nationale. La Commission informera la personne concernée dès que l'autorité nationale lui aura indiqué que le secret de la procédure ne s'impose plus. Cette limitation du droit à l'information de la personne concernée est en conformité avec l'article 20.1 règlement.

3.9. Sécurité

Des mesures techniques et organisationnelles ont été prises afin 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.

Sur base des informations disponibles, le CEPD n'a pas de raison de croire que la Commission n'a pas respecté les mesures de sécurité requises à l'article 22 du règlement.

Conclusion

Le traitement proposé ne paraît pas entraîner de violations des dispositions du règlement (CE) 45/2001 pour autant qu'il soit tenu compte des observations faites ci-dessus. Cela implique, en particulier, que la Commission doit assurer :

- que la conservation sur le long terme des dossiers soit accompagnée de garanties appropriées;
- que la durée de conservation soit réévaluée en fonction de l'évolution du dossier, notamment du fait de l'abandon des procédures disciplinaires et/ou contentieuses, ou de l'acquittement de la personne en justice;
- que soient définies précisément les catégories exactes de personnes qui ont droit d'accéder à ces données/archives et les finalités pour lesquelles elles ont accès à ces données;
- que soient enregistrés tout transfert de données vers des destinataires autres que les institutions communautaires ainsi que la justification légale en vertu de laquelle un tel transfert a été effectué;
- qu'il soit rappelé aux gestionnaires en charge des dossiers au sein de la Commission que les données ne doivent être traitées que dans le but de traiter les demandes de levée d'immunités aux fins d'autoriser une personne à comparaître en justice et/ou une perquisition des lieux ou archives la concernant;
- que la personne concernée puisse s'exprimer sur l'affaire qui la concerne avant que la décision de l'AIPN ne soit prise et cela si aucune limitation découlant de l'article 20.1 n'est d'application, et que ses commentaires soient consignés dans son dossier personnel.

Fait à Bruxelles, le 25 mars 2009

(signé)

Giovanni BUTTARELLI
Contrôleur Adjoint