Avis sur la notification d'un contrôle préalable reçue du délégué à la protection des données (DPD) de la Commission européenne à propos du dossier "Autorisations de témoigner en justice"

Bruxelles, le 28 mars 2008 (Dossier 2007-721)

1. Procédure

Par e-mail reçu le 4 décembre 2007, une notification dans le sens de l'article 27 (3) du règlement (CE) n° 45/2001 a été effectuée par le Délégué à la Protection des données (DPD) de la Commission au Contrôleur européen de la protection des données (CEPD), concernant le dossier "autorisations de témoigner en justice". Etait joint à la notification la déclaration spécifique de confidentialité du traitement en question.

Par e-mail en date du 20 décembre 2007, des questions sont transmises au DPD de la Commission. La réponse a été adressée au CEPD le 7 février 2008. Le projet d'avis a été envoyé pour commentaires le 17 mars 2008 mars au DPD. Les commentaires ont été reçus le 27 mars 2008.

2. Examen de l'affaire

L'article 19 du Statut des fonctionnaires des Communautés européennes (articles 11 et 54 du Régime applicable aux autres agents) stipule que "*le fonctionnaire ne peut faire état en justice, à quelque titre que ce soit, des constatations qu'il a faite en raison de ses fonctions, sans l'autorisation de l'autorité investie du pouvoir de nomination. Cette autorisation ne peut être refusée que si l'intérêt des Communautés l'exigent et si ce refus n'est pas susceptible d'entraîner des conséquences pénales pour le fonctionnaire intéressé. Le fonctionnaire reste soumis à cette obligation même après la cessation de ses fonctions.* (...) La Commission a mis en place un traitement de données visant, en réponse à la demande d'une juridiction nationale, ou de toute autre entité nationale ayant autorité pour procéder à une enquête, à autoriser la comparution d'un fonctionnaire ou d'un agent en justice.

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) qui doivent faire état en justice des constatations faites en raison de leurs fonctions.

L'autorité nationale transmet sa demande d'audition à un service de contact de la Commission (ADMIN, OLAF, Secrétariat Général, etc.) ou directement au fonctionnaire. Cette demande doit être transmise au service compétent (ADMIN.B.3) pour être traitée. Un projet de décision est préparé par ADMIN.B.3 puis adopté par l'AIPN après accord du Service juridique. La décision est alors envoyée au demandeur : soit le service de contact de la Commission qui a

reçu la demande de l'autorité nationale (et qui transmet la décision à cette même autorité), soit le fonctionnaire si c'est lui qui a reçu la demande. Le cas échéant, la décision n'est pas transmise au fonctionnaire si l'autorité nationale a exigé la confidentialité. C'est alors cette autorité qui informe le fonctionnaire en le convoquant.

La procédure est manuelle et automatisée. Les éléments nécessaires à la gestion du dossier (demande de l'autorité nationale, copie de l'autorisation, échanges d'e-mails) sont placés dans des classeurs et sur un disque réseau.

La décision est classée au dossier personnel du fonctionnaire dès qu'elle peut être communiquée au fonctionnaire. Pour ce faire, l'ADMIN.B.3 demande au service de contact une information explicite sur le moment à partir duquel la décision peut être placée dans le dossier personnel. Après 6 mois, l'unité ADMIN.B.3 vérifie l'état du dossier pour éviter toute omission.

Les données traitées reprennent les données suivantes : nom, prénom, numéro de personnel, grade, affectation, lien statutaire, raison de la comparution et référence à la convocation de l'autorité national.

Les données nécessaires à la gestion du dossier (demande de l'autorité nationale, copie de l'autorisation, échanges d'e-mails) sont conservées cinq années. La décision de l'AIPN est conservée dans le dossier personnel et dès lors suit les règles de conservation de ce dernier (jusqu'à l'extinction des droits de la personne concernée, de ses ayants droit et des possibilités de recours).

Les dossiers sont gérés par les gestionnaires responsables de l'unité ADMIN.B.3 Les données sont transmises à l'autorité nationale, au service juridique (pour accord) et au service de la Commission en contact avec l'autorité nationale (ADMIN, Secrétariat Général, OLAF). Sur demande individuelle, certains services peuvent avoir accès à la décision de l'AIPN, conservée dans le dossier personnel (service juridique, IDOC, OLAF, Inspection des délégations, direction sécurité). Le responsable ressources humaines de la DG d'appartenance de la personne concernée peut également avoir accès à la décision de l'AIPN.

Les droits d'accès et de rectification sont garantis à la personne concernée. La déclaration spécifique de confidentialité du traitement expose leur limite. Le droit d'accès peut-être limité et différé à la demande de l'autorité nationale qui a demandé la levée du devoir de réserve. Dans un tel cas, la personne concernée est informée qu'elle peut saisir le Contrôleur européen de la protection des données dans le cadre de l'article 20 du règlement (CE) n° 45/2001. Le verrouillage et l'effacement des données sont effectués dans les 15 jours qui suivent une demande justifiée de la personne concernée.

Un lien vers la déclaration spécifique de confidentialité se trouve sur la page intranet de la Commission expliquant la procédure et les règles en la matière. Cette déclaration reprend plus précisément les informations suivantes : le responsable du traitement, les finalités, les catégories de données concernées, la base juridique, le droit d'accès et de rectification, les destinataires des données et la durée de conservation des données.

Les demandes d'autorisation, si elles doivent rester confidentielles, sont transmises par le service demandeur sous double enveloppe. Dans ce cas, le circuit des signataires est suivi par les gestionnaires et non par les huissiers. Toutes les expéditions de courrier sont faites sous double enveloppe. Les éléments nécessaires à la gestion du dossier sont placés dans des classeurs dans des armoires fermées à clé et/ou sur le disque réseau. Les documents ne sont pas

attachés lors de leur enregistrement dans ADONIS (registre du courrier) et sont au niveau de confidentialité 2. La consultation du service juridique se fait par voie électronique uniquement; les e-mails sont cryptés si la demande requiert la confidentialité.

3. Les aspects légaux

3.1. Contrôle préalable

L'opération décrite par la notification reçue le 4 décembre 2007 représente un traitement de données à caractère personnel ("toute information concernant une personne identifiée ou identifiable" - article 2.a). Le traitement de données présenté 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).

Le traitement "autorisations de témoigner en justice" est partiellement automatisé, en ce sens que les listes des données nécessaire à gérer les dossiers des autorisations sont enregistrées sur le disque réseau. Les données sont également conservées sur support papier dans des classeurs et dans le dossier personnel en ce qui concerne la décision de l'AIPN. 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 du règlement (CE) 45/2001, soumet au contrôle préalable du CEPD, les traitements présentant des risques particuliers au regard des droits et libertés des personnes concernées. L'article 27.2 contient une liste de traitements susceptibles de présenter semblables risques. L'article 27.2.a. 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 sureté". Le traitement "autorisation de témoigner en justice" traite plus particulièrement des données relatives à des suspicions, infractions, condamnations pénales et tombe dès lors sous 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. Dans ce cas précis, le traitement a été mis en place avant de consulter le CEPD, 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 officielle a été reçue par courrier en date du 4 décembre 2007. Conformément à l'article 27.4 du règlement, le CEPD devait rendre son avis pour le 5 février 2008. Le délai dans lequel le CEPD doit rendre son avis ayant été suspendu de 49 jours (+ 10 jours pour commentaires), le CEPD rendra son avis au plus tard pour le 4 avril 2008 (5 février + 59 jours de suspension).

3.2. Licéité du traitement

La licéité du traitement doit être examinée à la lumière de l'article 5.a du règlement 45/2001 qui prévoit que "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 le devoir de réserve du fonctionnaire et l'autoriser à faire état de ses constatations. Il s'agit bien ici d'une mission effectuée dans l'intérêt public.

La base légale est dans le cas présent particulièrement importante; les données traitées peuvent en effet être très sensibles. Elle repose sur l'article 19, du Statut et sur les articles 11 et 54 du Régime applicable aux autres agents qui prévoit que "le fonctionnaire ne peut faire état en justice, à quelque titre que ce soit, des constatations qu'il a faite en raison de ses fonctions, sans l'autorisation de l'autorité investie du pouvoir de nomination. Cette autorisation ne peut être refusée que si l'intérêt des Communautés l'exigent et si ce refus n'est pas susceptible d'entraîner des conséquences pénales pour le fonctionnaire intéressé. Le fonctionnaire reste soumis à cette obligation même après la cessation de ses fonctions (...)". Dès lors, la base légale, relevant du Statut, est conforme et vient à l'appui de la licéité du traitement.

D'après la description du traitement en tant que tel, le CEPD conclut que 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 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, l'article 19 du statut, adopté sur la base des traités autorise le traitement : "autorisation de témoigner en justice". L'article 10 est donc bien respecté.

3.4. Qualité des données

Conformément à l'article 4.1.c du règlement, les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement. Les données traitées qui sont décrites au début du présent avis doivent être considérées comme satisfaisant à ces conditions en l'espèce. Les données requises sont nécessaires pour la gestion des autorisations de témoigner en justice. Le CEPD estime que l'article 4.1.c du règlement 45/2001 semble respecté à cet égard.

Par ailleurs les données doivent être traitées "*loyalement et licitement"* (article 4.1.a du règlement (CE) 45/2001. La licéité du traitement a déjà fait l'objet d'une analyse (voir supra, point 3.2). Quant à la loyauté, elle est en relation avec l'information donnée aux personnes concernées. Sur ce point voir ci-dessous point 3.9.

Selon l'article 4.1.d du dit règlement, les "*données doivent être exactes et, si nécessaire, mises à jour"*. Le système lui même fait que les données sont exactes et mises à jour. En effet, le traitement ne porte que sur les autorisations elles-mêmes et le fait que, dans certains cas, l'autorité nationale demande que le fonctionnaire ne soit pas informé directement de la levée de son devoir de réserve. La décision n'est pas alors directement stockée dans le dossier personnel de la personne concernée. Afin de vérifier l'état des dossiers, l'unité ADMIN.B.3 vérifie son état après 6 mois. Dans les limites de l'article 20, 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 deuxième possibilité d'assurer la qualité des données. Concernant ces deux droits d'accès et de rectification, voir point 3.8 ci-après.

3.5. Conservation des données

Le principe général énoncé dans le règlement 45/2001 est 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"*.(article 4.1.e du règlement).

Pour mémoire, les données nécessaires à la gestion des dossiers sont conservées pendant une période de 5 ans à partir de la clôture du dossier. La décision de l'AIPN est conservée dans le dossier personnel et suit donc les règles de conservation de ce dernier.

Le CEPD estime que cette durée de 5 ans semble raisonnable au regard de la réalisation des finalités pour lesquelles les données ont été collectées (autorisation de témoigner en justice) ainsi que pour lesquelles elles sont traitées ultérieurement (gestion des dossiers).

Par ailleurs, en ce qui concerne la décision conservée dans le dossier personnel, cette conservation des données sur le long terme devra être accompagnée de garanties appropriées. Les données conservées sont personnelles. Le fait qu'elles soient archivées pour une conservation sur le long terme ne leur ôte pas le caractère de données personnelles.

3.6. Transfert des données

Le traitement doit être aussi examiné à la lumière de l'article 7.1 du règlement 45/2001. Le traitement au regard de l'article 7.1 concerne les transferts de données à caractère personnel entre institutions ou organes communautaires ou en leur sein "*si nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire*".

Nous sommes dans le cas d'un transfert au sein d'une même institution. Notamment, les destinataires du traitement sont le service juridique, l'AIPN, l'unité ADMIN.B.3 en charge de la gestion des dossiers et le service de la Commission en contact avec l'autorité nationale (ADMIN, OLAF, SG, etc.). Sur demande individuelle, certains services peuvent avoir accès à la décision de l'AIPN, conservée dans le dossier personnel. C'est le cas du service juridique, de l'IDOC, de l'OLAF, de l'Inspection des délégations, de la direction sécurité. Le responsable ressources humaines de la DG d'appartenance a également accès à la décision de l'AIPN. Enfin, le CEPD souligne que lui-même, le Médiateur européen et la Cour de Justice peuvent être considérés comme destinataires de données, en cas de plaintes ou de recours par exemple. Il s'ensuit que le transfert est 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 (CE) 45/2001 dispose 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 d'accorder les autorisations de témoigner en justice.

Dans le cas sous analyse, les données (la décision de l'AIPN) sont également communiquées à l'autorité nationale qui demande la levée du devoir de réserve. 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 sous-analyse, ce sont les autorités judiciaires qui ont fait la demande de l'autorisation de témoigner en justice 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 95/49/CE aux autorités judiciaires, il convient de prendre en considération l'article 9 du règlement. Dans le cas de ces pays, la Convention 108 du Conseil de l'Europe, qui, pour ce qui concerne la question étudiée, peut être considérée comme fournissant un niveau de protection adéquat, est en tout état de cause applicable aux autorités judiciaires.

Si l'autorité nationale se trouve dans un pays ne relevant pas de la directive (CE) 45/96, 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, (...) ".

3.7 Traitement incluant le numéro de personnel ou le numéro identifiant

Le Commission utilise le numéro de personnel pour la gestion des autorisations de témoigner en justice. L'utilisation d'un identifiant n'est, en soi, qu'un moyen -légitime, en l'espèce- de faciliter le travail du responsable du traitement des données à caractère personnel; toutefois, cette utilisation peut avoir des conséquences importantes. C'est d'ailleurs ce qui a poussé le législateur européen à encadrer l'utilisation de numéros identifiants par l'article 10.6 du règlement, qui prévoit l'intervention du CEPD. En l'espèce, l'utilisation du numéro de personnel peut avoir pour conséquence de permettre l'interconnexion de données traitées dans des contextes différents. Il ne s'agit pas ici d'établir les conditions dans lesquelles la Commission peut traiter le numéro personnel, mais de souligner l'attention qui doit être portée à ce point du règlement. En l'espèce, l'utilisation du numéro personnel par la Commission est raisonnable car l'utilisation de ce numéro est un moyen de faciliter le travail du traitement, en particulier son archivage.

3.8 Droit d'accès et de rectification

L'article 13 du règlement (CE) 45/2001 dispose du droit d'accès - et de 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 (CE) 45/2001 dispose du droit de rectification pour la personne concernée. De la même façon que la personne concernée dispose du droit d'accès, cette dernière peut aussi faire modifier les données personnelles si nécessaire.

Pour rappel, les droits d'accès et de rectification sont garantis à la personne concernée. Ces deux droits peuvent être limités et différés à la demande de l'autorité nationale qui a demandé la levée du devoir de réserve, conformément à l'article 20.1. Dans un tel cas, la Commission a informé de manière général la personne concernée du fait qu'elle peut saisir le CEPD conformément aux articles 20.3, 20.4. Cependant, L'article 20, paragraphe 5, dispose que *"l'information visée aux paragraphes 3 et 4 peut être reportée aussi longtemps qu'elle prive d'effet la limitation imposée sur la base du paragraphe 1"*. Il peut se révéler nécessaire de différer cette information conformément à cette disposition, afin de protéger l'enquête. De plus, comme il est précisé dans les faits du présent avis ces limitations sont temporaires.

L'article 14 du règlement accorde à la personne concernée le droit à la rectification des données inexactes ou incomplètes. Compte tenu de la sensibilité du traitement, ce droit revêt une importance cruciale pour garantir la qualité des données utilisées, laquelle est, en l'espèce, liée au droit de défense. 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 confidentialité venant de l'autorité nationale - la personne concernée doit avoir la possibilité de s'exprimer sur l'affaire qui la concerne avant que la décision de l'AIPN ne soit prise. Cette possibilité de s'exprimer devra par exemple être assurée à la personne concernée lorsque la Commission est citée comme témoin en tant qu'institution et que le service concerné désigne la personne qui paraît la plus compétente pour répondre, en tant que témoin, au juge. Cette disposition s'appliquera également lorsque le fonctionnaire ou agent demande de sa propre initiative la levée du devoir de réserve. Le CEPD recommande que cette possibilité soit introduite dans la procédure régissant les autorisations à témoigner en justice. Cette recommandation mise à part, le CEPD estime que les articles 13 et 14 du règlement sont respectés.

Le verrouillage et l'effacement des données sont effectués dans les 15 jours qui suivent une demande justifiée de la personne concernée; les articles 15 et 16 sont donc bien respectés.

3.9 Information des personnes concernées

Les articles 11 et 12 du règlement 45/2001 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, une partie des données (la demande d'autorisation) est transmise par le biais de la personne elle-même ou par celui du service de la Commission en contact avec l'autorité nationale.

Les dispositions de l'article 11 (*Informations à fournir lorsque les données sont collectées auprès de la personne concernée*) sur l'information de la personne concernée sont applicables en l'espèce. En effet, dans certains cas, la personne concernée transmet elle-même la demande d'autorisation qu'elle a reçu de l'autorité nationale au service ADMIN.B.3 ; elle fournit donc elle-même les données.

Les dispositions de l'article 12 (*Informations à fournir lorsque les données n'ont pas été collectées auprès de la personne concernée)* sont également applicables en l'espèce. En effet, dans d'autres cas, l'autorité nationale transmet la demande d'autorisation via un service de la Commission.

Dans le cas sous analyse, une information générale est prévue pour les personnes concernées via la Déclaration spécifique de confidentialité disponible sur intranet. La Déclaration reprend toutes les mesures des articles 11 et 12 à l'exception du droit de saisir, à tout moment, le Contrôleur européen de la protection des données. Le CEPD demande que cette mention soit inclue dans la Déclaration.

En ce qui concerne l'information spécifique, c'est à dire lorsqu'une personne concernée fait l'objet d'une demande d'autorisation, elle doit être informée du traitement au plus tard à la première communication des données si l'autorisation a été demandée via un des services de la Commission et directement si la demande d'autorisation a été fournie par la personne concernée. C'est le cas en l'espèce. Il se peut par ailleurs que cette information soit différée, conformément à l'article 20.1, à la demande de l'autorité nationale. C'est l'autorité nationale qui informera alors la personne concernée. Cette limitation du droit à l'information de la personne concernée est en conformité avec le règlement.

3.10. 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.

Après une analyse attentive de ces mesures, le CEPD considère qu'elles sont, de manière générale, adéquates à la lumière de l'article 22 du règlement (CE) 45/2001. Cependant, en terme de gestion des accès et au vu de la sensibilité des données traitées, le CEPD recommande que les gestionnaires de l'unité ADMIN.B.3 ainsi que ceux du service juridique n'aient accès qu'aux dossiers dont ils sont spécifiquement en charge. Seul le gestionnaire d'un dossier, son remplaçant éventuel et leur supérieur hiérarchique doivent avoir accès à ce dossier particulier, de même pour le service juridique.

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 soit introduite la possibilité pour la personne concernée de 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;
- l'ajout dans le Déclaration spécifique de confidentialité l'information relative au droit de saisir à tout moment le Contrôleur européen de la protection des données;
- les gestionnaires du service ADMIN.B.3 et du service juridique et leurs remplaçants éventuels n'aient accès qu'aux dossiers dont ils ont la charge.

Fait à Bruxelles, le 28 mars 2008

(signé)

Joaquín BAYO DELGADO
Le Contrôleur Adjoint