Avis de contrôle préalable
concernant la fourniture de services de conseil externes
à l'Agence européenne des médicaments («EMA»).

Bruxelles, le 15 octobre 2015
(Dossier 2013-0627)

1. Procédure

Le 11 juin 2013, le Contrôleur européen de la protection des données («CEPD») a reçu une notification de contrôle préalable sur la base de l'article 27, paragraphe 2, du règlement (CE) nº 45/2001 («le règlement») concernant le traitement de données à caractère personnel dans le cadre de services de conseil externes du délégué à la protection des données («DPD») de l'Agence européenne des médicaments («EMA»). À la demande du CEPD, l'EMA a fourni des informations supplémentaires.

Dans la mesure où il s'agit d'une **notification ex post**, le délai de deux mois pour l'adoption d'un avis par le CEPD ne s'applique pas. Ce dossier a été traité dans les meilleurs délais.

2. Le traitement

L'EMA a conclu un contrat avec une clinique (ci-après «le contractant») pour la fourniture aux membres du personnel de services médicaux, qui comprennent également des **services de conseil**. Ces derniers sont les seuls services couverts par la notification envoyée par l'EMA. La fourniture de ces services a pour finalité d'apporter une aide au personnel affecté par un stress émotionnel pendant et après un incident de continuité d'activité. Ces services de conseil sont également disponibles pour faire face à des situations de type comportements d'intimidation, harcèlement sexuel, conflits au travail, ou pour soutenir le personnel souffrant de stress pour d'autres raisons dans leur vie, ainsi que pour l'anxiété, la dépression, les relations humaines, les litiges judiciaires et familiaux, les traumatismes, la gestion du stress et l'évaluation psychologique.

La relation juridique entre l'EMA et le contractant est régie par un contrat-cadre de services («FSC», *Framework Service Contract*) et un accord de niveau de services («SLA», *Service Level Agreement*).

La procédure concerne deux types de traitement de données: les traitements réalisés directement par l'EMA et les traitements réalisés directement par le contractant pour ce qui est des consultations.

Les données à caractère personnel traitées directement par l'EMA sont les suivantes:

- la demande de consultations formulée par la personne concernée,
- un rapport sommaire du contractant indiquant que les six consultations auxquelles la personne concernée a droit ont été conduites – rapport qui ne contient aucune information se rapportant au contenu des consultations ou au diagnostic, mais qui peut contenir une recommandation pour d'autres consultations,
- les factures pour les services fournis sur lesquelles figurent un numéro de référence et la date de naissance de la personne concernée, et
- «les copies de documents non médicaux d'un membre du personnel effectuées à partir des fichiers» (selon le SLA).

Les données à caractère personnel traitées par le contractant sont les suivantes:

- toutes les données susmentionnées, et
- toutes les données à caractère personnel résultant des consultations et liées à celles-ci.

Le responsable des ressources humaines et un ordonnateur ont accès aux données traitées directement par l'EMA.

Une réunion verbale et informelle se tient entre le responsable des ressources humaines et le membre du personnel concerné avant l'établissement d'une demande de consultation. La demande de six consultations est alors envoyée au contractant par le département des ressources humaines de l'EMA. La prise de rendez-vous se fait directement entre le membre du personnel et le prestataire de services. Le rapport sommaire et la facture, qui contiennent un numéro de dossier attribué au lieu du nom de la personne concernée, sont envoyés à l'EMA une fois les consultations achevées.

3. Analyse juridique

3.1. Champ d'application de l'avis

Champ d'application Le présent avis couvre le traitement des données par l'EMA et son contractant externe lors de la fourniture de **services de conseil**. Il ne couvre pas le traitement des données à caractère personnel par le contractant externe lorsque celui-ci fournit des services médicaux *stricto sensu*. Par conséquent, l'EMA doit envoyer une notification distincte à cet égard.

Lignes directrices Le traitement relève du champ d'application des **lignes directrices** du CEPD sur le traitement **des données relatives à la santé** sur le lieu de travail par les institutions et les organes de l'Union Européenne (les «lignes directrices»)[1].

Le DPD a souligné que le traitement des données concerné diffère de celui lié aux consultations relatives à des situations de harcèlement. Ce dernier a déjà fait l'objet d'un avis de contrôle préalable par le CEPD[2].

[1] *Lignes directrices concernant le traitement des données relatives à la santé sur le lieu de travail par les institutions et organes communautaires*, adoptées en septembre 2009 et disponibles sur le site web du CEPD https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/09-09-28_Guidelines_Healthdata_atwork_FR.pdf

[2] Voir l'avis émis dans le dossier 2010-0598 (Points d'écoute/procédures informelles à l'EMA), en février 2011.

Le présent avis porte sur les aspects qui ne semblent pas être complètement conformes au règlement, tel que souligné dans les lignes directrices susmentionnées, qui nécessitent d'être améliorés ou qui méritent par ailleurs une explication.

3.2. Motifs de contrôle préalable

Dans la mesure où les services de conseil peuvent comporter le traitement de données relatives à la santé, ils sont soumis à contrôle préalable conformément à l'article 27, paragraphe 2, point a), du règlement.

3.3. Licéité

En vertu de l'article 5, point a), du règlement, le traitement est licite s'il 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*».

Le fondement juridique du traitement évalué est l'article 1er sexies du statut des fonctionnaires aux termes duquel «*les fonctionnaires en activité ont accès aux mesures à caractère social, y compris aux mesures spécifiques destinées à concilier vie professionnelle et vie familiale, adoptées par les institutions*». Il est également conforme au considérant 27 du règlement aux termes duquel le traitement des données à caractère personnel effectué pour l'exécution de missions d'intérêt public «*comprend le traitement de données à caractère personnel nécessaires pour la gestion et le fonctionnement de ces institutions et organes*». Par ailleurs, la note de service interne du 19 juin 2008[3] mentionne que les services sont disponibles pour des situations telles que les «conflits au travail», les «comportements d'intimidation», ou «pour soutenir le personnel souffrant de stress pour d'autres raisons dans leur vie».

Compte tenu de la nature sensible du traitement des données considéré et étant donné que le fondement juridique spécifique pour les conseils au personnel n'est détaillé que dans une note de service interne, l'EMA devrait décrire plus avant les modalités de la procédure de services de conseil dans le cadre de règles plus spécifiques à valeur normative (politique, communication, décision), applicables à son personnel interne[4]. Une telle démarche permettra non seulement d'assurer la clarté et la transparence des procédures mais également d'aider les membres du personnel en décrivant en détails ce traitement de données sensibles.

Le traitement mis en œuvre par l'EMA semble nécessaire pour résoudre des problèmes liés à l'emploi et contribuer à l'amélioration générale de l'environnement de travail[5] au sein de l'EMA.

À la lumière de cette évaluation, le traitement est licite aux termes de l'article 5, point a), du règlement, à la condition que le fondement juridique soit renforcé par une politique/décision adoptée par l'EMA.

---

[3] Note de service (réf.: EMEA/312151/2008 310) envoyée par le responsable administratif au secrétariat de l'EMA concernant les services de conseil.

[4] Voir à ce titre les *Lignes directrices relatives au traitement de données à caractère personnel dans le cadre de la sélection de conseillers confidentiels et des procédures informelles de traitement des cas de harcèlement au sein des institutions et organes de l'Union Européenne,* adoptées en février 2011 (disponible à l'adresse suivante:https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/11-02-18_Harassment_Guidelines_FR.pdf), p. 4

3.4. Traitement de catégories particulières de données

Les données à caractère personnel traitées par l'EMA (et par le contractant pour le compte de l'EMA) dans le cadre des services de conseil comprennent les données relatives à la santé.

De fait, comme établi par le CEPD dans les lignes directrices[6], les données relatives à la santé comprennent:
- les données médicales (par exemple, orientations d'un malade par un généraliste vers un spécialiste et prescriptions médicales, rapports d'examens médicaux et psychologiques) - en l'espèce, ces données sont traitées par le contractant, et
- les données administratives et financières relatives à la santé (par exemple, calendrier des rendez-vous médicaux, factures de prestation de services de santé, indication du nombre de jours de congé de maladie, gestion des congés maladie) - en l'espèce, ces données sont traitées par l'EMA et le contractant.

Le traitement des données à caractère personnel relatives à la santé ou à la vie sexuelle est interdit, sous réserve de motifs visés à l'article 10, paragraphe 2, du règlement. Selon l'article 10, paragraphe 2, point b), une telle exception est prévue lorsque le traitement est nécessaire afin de respecter les droits et obligations du responsable du traitement en matière de droit du travail. Dans ce cas, la justification du traitement de données relatives à la santé peut être trouvée dans le statut des fonctionnaires (article 1er sexies), qui doit être complété par une politique/décision se rapportant aux services de conseil, à adopter par l'EMA (voir section 3.3 ci-dessus).

Du fait de la nature sensible des données à caractère personnel traitées en l'espèce, des mesures organisationnelles spécifiques doivent être prises conformément à l'article 22 du règlement (cf. ci-après section 3.6).

3.5. Droits de la personne concernée

1) Information

Selon la notification, les membres du personnel de l'EMA reçoivent une notification générale de protection des données pour tous les traitements liés aux procédures de ressources humaines, tandis qu'un avis général de confidentialité figure sur le site web externe. Aucun avis de protection des données spécifique complémentaire n'est communiqué aux membres du personnel. Le membre du personnel concerné reçoit une copie des communications entre le responsable des ressources humaines et la société de services de conseil extérieure.

La «déclaration de protection des données» fournie par l'EMA ne satisfait pas aux exigences imposées par les articles 11 et 12 du règlement. Par exemple, les finalités du traitement et les destinataires ou les catégories de destinataires des données ne figurent pas dans la déclaration. L'EMA doit communiquer des informations aux personnes concernées par le biais d'un avis de protection des données spécifique sur les services de conseil. L'avis doit être publié sur le site web ou sur l'intranet[7].

Par ailleurs, la politique ou la décision de l'EMA sur la procédure de services de conseil (voir ci-dessus section 3.3.) doit prévoir que des informations spécifiques, dans le cas d'une demande de services de conseil, soient fournies à la personne concernée, lors de la réunion

[6] Voir *lignes directrices sur les données relatives à la santé* citées ci-dessus, page 2.
[7] Voir à cet égard les *Lignes directrices sur les cas de harcèlement citées ci-dessus*, au point 1.

initiale entre le responsable des ressources humaines et la personne concernée. À cet égard, l'EMA a déjà mis en œuvre un système d'information dans le cadre de la procédure informelle en matière de harcèlement. Le CEPD a indiqué que celui-ci constituait une bonne pratique[8]. L'EMA doit mettre en œuvre le même système pour la procédure en question.

2) Exercice de leurs droits par les personnes concernées

Outre le fait de devoir demander à son contractant de donner accès aux personnes concernées à leurs données à caractère personnel (voir ci-dessous section 3.7.), l'EMA doit également donner accès aux données à caractère personnel qu'elle traite et fournir les moyens d'exercer les droits de rectification et d'effacement. À cet égard, l'avis de protection des données doit fournir des informations précises sur la manière dont la personne concernée peut exercer ses droits vis-à-vis de l'EMA et du contractant. La notification (section 8) doit être actualisée en conséquence.

3.6. Sécurité

[...]

3.7. Sous-traitance

Conformément à l'article 23, paragraphe 1, du règlement, *lorsque le traitement est effectué pour son compte, le responsable du traitement choisit un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation prévues par l'article 22 et veille au respect de ces mesures.* Par ailleurs, conformément à l'article 23, paragraphe 2, du règlement, *la réalisation de traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que:*
a) le sous-traitant n'agit que sur instruction du responsable du traitement;
b) les obligations visées aux articles 21 [confidentialité] *et 22* [sécurité] *incombent également au sous-traitant, à moins que, en vertu de l'article 16 ou de l'article 17, paragraphe 3, deuxième tiret, de la directive 95/46/CE, le sous-traitant soit déjà soumis à des obligations de confidentialité et de sécurité énoncées dans la législation nationale de l'un des États membres*.

En l'espèce, un contrat (FSC et SLA) a été conclu entre l'EMA et le sous-traitant.

1) Obligation du sous-traitant de n'agir que sur instruction de l'EMA.

Le FSC ne comprend qu'un seul article consacré à la protection des données (article II.7), qui ne fait aucune référence à l'obligation du sous-traitant *de n'agir que sur instruction du responsable du traitement*, comme le prévoit l'article 23, paragraphe 2, point a), du règlement. La seule référence au règlement incluse dans le FSC ne suffit pas à indiquer clairement la condition légale du traitement des données. Par conséquent, le contrat doit être modifié pour inclure cette obligation.

[8] Voir avis relatif au dossier 2010-0598 cité ci-dessus, point 3.8.

2) Confidentialité

Le contractant est enregistré dans un État membre de l'UE (à savoir le Royaume-Uni); il est donc soumis aux obligations visées dans la directive 95/46/CE et dans sa loi de transposition, notamment les obligations de confidentialité et de sécurité. La clause de confidentialité prévue par le FSC (article II.9) doit également faire référence aux règles de protection des données nationales applicables[9].

3) Mesures de sécurité

[...]

4) Exercice par les personnes concernées de leurs droits au titre du traitement par le contractant

Afin d'assurer l'efficacité du droit d'accès de la personne concernée, le point 14 du SLA relatif aux «fichiers» doit être complété par des dispositions indiquant clairement que la personne concernée a accès à son propre fichier conformément à l'article 13 du règlement, et non pas seulement en vertu de l'article 26 bis du statut des fonctionnaires (point 14.1 du SLA). De même, le point 14.2 du SLA doit être complété par des dispositions indiquant que le contractant doit respecter les demandes d'effacement et de rectification présentées par les membres du personnel de l'EMA, conformément à l'article 14 du règlement.

Le CEPD souligne qu'en matière de droit d'accès de la personne concernée aux données de santé traitées directement par le contractant, la règle générale reste l'accès direct. Toutefois, *en vertu de* l'article 20, paragraphe 1, point c), du règlement, l'accès aux données à caractère psychologique ou psychiatrique peut être donné *indirectement* si une évaluation faite au cas par cas révèle que l'accès indirect est nécessaire pour protéger la personne concernée, au vu des circonstances[10].

Conclusion:

Il n'existe aucune raison de conclure à une violation des dispositions du règlement (CE) 45/2001, pour autant que les recommandations énoncées dans le présent avis soient pleinement prises en compte. L'EMA doit, en particulier:

- adopter des règles spécifiques à valeur normative (politique, communication, décision) détaillant les modalités de la procédure de services de conseil
- établir et publier une déclaration de confidentialité exhaustive concernant le traitement lié aux services de conseil, qui soit conforme aux exigences des articles 11 et 12 du règlement, notamment fournir des informations sur la manière dont la personne concernée peut exercer ses droits; la politique/décision sur les services de conseil devrait prévoir que la personne concernée reçoive la déclaration de confidentialité pendant la réunion initiale avec le responsable des ressources humaines;
- préparer des déclarations de confidentialité spécifiques à signer par le personnel chargé du traitement effectué directement par l'EMA au titre du traitement des données de santé dans le cadre des services de conseil;

[9] Voir l'avis relatif au dossier 2007-0489 (données traitées par le conseiller social de la BCE) du 6 décembre 2007, point 3.9.
[10] Voir *Lignes directrices*, point 6.

- modifier le contrat et le SLA avec le prestataire de services de conseil, de manière à:
    - inclure l'obligation du prestataire de services *de n'agir que sur instruction du responsable du traitement*, prescrite à l'article 22, paragraphe 2, point a), du règlement ;
    - faire référence aux règles de protection des données nationales applicables dans la clause de confidentialité;
    - [...];
    - [...];
    - compléter le point 16 du SLA sur les «Fichiers» conformément aux articles 13 et 14 du règlement, garantissant les droits de la personne concernée;
    - inclure l'obligation pour le contractant de faire signer par chaque membre de son personnel une déclaration de confidentialité spécifique se rapportant au traitement des données relatives à la santé des membres du personnel de l'EMA dans le cadre du contrat;
- [...]
- actualiser la notification pour y inclure des procédures concernant l'exercice des droits des personnes concernées, tant au regard des données traitées par le contractant qu'au regard des données traitées directement par l'EMA;
- notifier au CEPD le traitement des données relatives à la santé par le contractant lors de la fourniture des services médicaux *stricto sensu*.

15 octobre 2015

(signé)

Wojciech WIEWIÓROWSKI
Contrôleur européen adjoint de la protection des données