**Avis sur une notification en vue d'un contrôle préalable transmise par le délégué à la protection des données de l'Agence européenne des médicaments ("EMEA")**

Bruxelles, le 7 septembre 2009 (dossier 2008-402)

## 1. Procédure

Le 25 juin 2008, le Contrôleur européen de la protection des données (ci-après dénommé "le CEPD") a reçu du délégué à la protection des données (ci-après dénommé "le DPD") de l'EMEA une notification en vue d'un contrôle préalable (ci-après dénommée "la notification") concernant un traitement de données à effectuer dans le cadre de la base de données EudraVigilance, placée sous la responsabilité directe de l'EMEA.

Le 18 septembre 2008, il a demandé à l'EMEA un complément d'informations, et lui a ensuite posé une autre série de questions le 10 octobre 2008.

Entre-temps, parallèlement à l'évaluation d'EudraVigilance aux fins du présent contrôle préalable, le CEPD a entamé une analyse de la proposition de la Commission visant à adapter le cadre légal actuel de la pharmacovigilance dans la Communauté européenne, qui porte également sur le rôle de l'EMEA à propos d'EudraVigilance.

Le 23 janvier 2009, des membres du personnel de l'EMEA et du CEPD se sont rencontrés pour discuter, entre autres, de la manière dont l'EMEA traite les questions relatives aux données à caractère personnel, en particulier dans le contexte de la gestion d'EudraVigilance.

Le 29 janvier 2009, l'EMEA a répondu à une partie de la première série de questions posées par le CEPD le 18 septembre 2008. Vu la complexité du traitement, le CEPD a prolongé de deux mois, le 30 janvier 2009, le délai dont il dispose pour rendre un avis. Le 12 février 2009, il a procédé à un examen des informations complémentaires que l'EMEA lui avait transmises dans sa réponse du 29 janvier et au cours de la réunion du 23 janvier2009.

Le 22 avril 2009, le CEPD a publié un avis sur les propositions de la Commission visant à adapter le cadre légal actuel de la pharmacovigilance.

Le 14 mai 2009, l'EMEA a transmis le reste des informations manquante: celles qui avaient été demandées le 12 février et celles qui manquaient dans le premier complément demandé. Le 20 juillet, le CEPD a transmis à l'EMEA le projet d'avis pour qu'elle fasse part de ses observations, qu'il a reçues le 4 septembre 2009.

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 63
E-mail : edps@edps.europa.eu - Site Internet : www.edps.europa.eu
Tél.: 02-283 19 00 - Fax : 02-283 19 50

## 2. Examen du dossier

### 2.1 Les faits

La ***finalité*** globale *du traitement de données* est de permettre aux autorités nationales compétentes (ci-après dénommées "les ANC") et à l'EMEA de notifier et d'évaluer respectivement les effets indésirables présumés des médicaments à usage humain (dénommés "les rapports de sécurité concernant des cas particuliers", ou plus simplement "les rapports de sécurité"), que ce soit durant la phase de développement desdits médicaments ou après leur mise sur le marché dans l'Espace économique européen.

L'objectif final de cette notification et de l'évaluation qui s'ensuit est double: *i)* détecter des signaux de sécurité éventuels concernant des médicaments à usage humain, et *ii)* être à même de prendre des décisions à partir d'une meilleure compréhension des effets indésirables des médicaments. EudraVigilance contribue ainsi à la protection et à la promotion de la santé publique dans l'EEE.

C'est l'unité "Post-autorisation et évaluation des médicaments à usage humain" de l'EMEA qui est le premier ***responsable du traitement des données***.

En résumé, le ***traitement*** comprend les ***activités*** suivantes:

*1) collecte des rapports de sécurité et envoi de ceux-ci à l'EMEA:* les ANC collectent les rapports de sécurité auprès des professionnels de la santé, des titulaires d'autorisations de mise sur le marché ("TAMM"), des promoteurs des essais cliniques et autres promoteurs. Actuellement, ce sont les ANC qui envoient à l'EMEA des rapports de sécurité se rapportant à des cas (effets indésirables graves présumés) qui se sont produits sur leur territoire, tandis que les TAMM signalent à l'EMEA des effets indésirables graves présumés (inattendus) qui se sont produits en dehors de l'EEE. Quant aux promoteurs d'essais cliniques, ils signalent les effets indésirables graves présumés inattendus à EudraVigilance conformément aux "lignes directrices détaillées sur la collecte, la vérification et la présentation de rapports sur des effets indésirables constatés à la suite d'essais cliniques de médicaments à usage humain" et à la législation nationale.

Depuis sa création en 1995, l'EMEA n'accepte de rapports de sécurité relatifs à des médicaments autorisés que s'ils sont transmis par voie électronique, conformément à l'article 29, point f, de la législation communautaire. Ce n'est que dans des circonstances exceptionnelles - comme une défaillance du système de transmission électronique - qu'elle accepte des transmissions par télécopieur; dès que le système fonctionne, les rapports sont introduits dans EudraVigilance et la copie papier est détruite;

*2) réception des rapports de sécurité par l'EMEA:* les rapports de sécurité, envoyés par voie électronique sous une forme cryptée à l'EMEA , sont placés dans la passerelle d'EudraVigilance. Les expéditeurs des rapports font l'objet d'une vérification d'identité et les rapports sont ensuite décryptés et transférés dans EudraVigilance, où ils sont validés au regard d'un ensemble de règles préétablies;

*3) partage des informations:* la base de données EudraVigilance est totalement accessible aux utilisateurs identifiés des ANC, tandis que les TAMM n'ont accès qu'aux informations qu'ils ont eux-mêmes soumises à l'EMEA.

Le 19 décembre 2008, l'EMEA a publié un projet de "lignes directrices sur l'accès" sur son site web, en vue d'une consultation publique. Ce document montre comment l'Agence envisage d'élargir l'accès au contenu de la base de données aux TAMM et aux professionnels des soins de santé;

*4) analyse par l'EMEA:* conformément à sa mission de protection de la santé publique, l'EMEA peut, après avoir reçu les rapports de sécurité, rédiger des avis, en consultation avec ses comités scientifiques, sur les mesures qui devraient être prises.

***Les personnes concernées*** sont: *i)* les patients (identifiés par un nom générique ou des initiales) et les familles des patients dont les données figurent dans les rapports de sécurité; *ii)* les professionnels de la santé et les juristes dont les données figurent dans les rapports de sécurité; *iii)* les personnes ayant un lien avec les organisations reconnues qui font partie de la communauté des utilisateurs d'EudraVigilance. Cette communauté se compose de personnes reconnues comme possédant les qualifications appropriées en matière de pharmacovigilance ou comme responsables d'EudraVigilance (ci-après dénommées "les personnes qualifiées"), qui sont désignées ou nommées par les TAMM ou les promoteurs.

Les ***données à caractère personnel*** relèvent des ***catégories*** suivantes:

**Pour ce qui concerne les patients et les professionnels de la santé:** *i)* des données d'identification (généralement, les patients sont identifiés par des initiales ou un numéro personnel, comme la date de naissance); *ii)* les coordonnées des sources premières des informations, comme des professionnels de la santé, rarement le patient; *iii)* les caractéristiques physiques des personnes; *iv)* les antécédents médicaux, qui peuvent inclure les résultats d'essais de laboratoire et dans certains cas l'histoire de la famille; et *iv)* d'autres catégories spéciales de données pouvant être traitées, notamment des données relatives à la vie sexuelle (par exemple, si les antécédents médicaux mentionnent la situation par rapport au VIH). Les données stockées peuvent dater du 1er janvier 1995 à actuellement.

**Pour ce qui concerne les personnes travaillant pour les ANC ou les TAMM fournissant les informations à la base de données et les personnes qualifiées:** données d'identification, comprenant le nom complet, l'adresse et les autres coordonnées, un document d'identification (comme un passeport, entre autres).

Les données sont **conservées** en ligne dans EudraVigilance pour une période indéterminée, afin de pouvoir procéder à leur évaluation scientifique complète.

Le responsable du traitement **met** le contenu en ligne de EudraVigilance **à la disposition** des types de destinataires suivants: *i)* les ANC; *ii)* les TAMM (uniquement les données qu'ils ont transmises eux-mêmes); *iii)* des autorités des USA (FDA), du Canada (Santé Canada) et du Japon (ministère de la santé, du travail et du bien-être) reçoivent des données d'EudraVigilance sur une base **ponctuelle**. Elles n'ont pas accès à la base de données même; leur accès ponctuel au contenu d'EudraVigilance se fait selon les règles figurant dans l'échange de lettres et concernant, entre autres, la manière de traiter les informations échangées.

En ce qui concerne le ***droit à l'information des personnes*** dont les données figurent dans EudraVigilance, la notification explique que, puisque les informations ne sont pas collectées directement auprès des personnes, l'EMEA ne donne pas d'informations à celles-ci.

La notification ne parle pas non plus des droits ***d'accès et de rectification*** des personnes concernées, ni des procédures permettant de les exercer (parce que, selon l'EMEA, l'Agence n'a pas de contacts directs avec les personnes concernées).

Au niveau des ***mesures de sécurité***, il importe de relever que, selon la notification, EudraVigilance est hébergée par le centre de données de l'EMEA et est accessible aux utilisateurs autorisés via un

réseau interne ainsi que via Internet, en utilisant le Hypertext Transfer Protocol et un protocole cryptographique.

L'EMEA a précisé ce qui suit à propos des mesures spécifiques qu'elle a adoptées afin de satisfaire aux exigences des articles 22 et 23 du règlement (CE) nº 45/2001:

*i)* l'accès à la base de données repose sur une identification de l'utilisateur et un mot de passe donnés à l'issue du processus d'inscription à EudraVigilance. Cet aspect est réglementé conformément au projet de lignes directrices sur l'accès à EudraVigilance susmentionné, qui était joint à la notification;

*ii)* l'EMEA a un agent responsable de la sécurité des TI dont les tâches couvrent la protection des données à caractère personnel du point de vue de la sécurité des systèmes d'information;

*iii)* tâches et obligations des utilisateurs ayant accès à des données et informations à caractère personnel: toutes les responsabilités des agents de l'EMEA sont clairement définies dans leur description des tâches. De plus, ils reçoivent une formation sur la protection des données à caractère personnel, visant à leur faire mieux comprendre les principes de la protection des données et les obligations qui leur incombent à cet égard;

*iv)* pour le personnel des ANC autorisé à utiliser EudraVigilance, le mémorandum d'accord sur le partage des données d'EudraVigilance (et d'autres documents et informations confidentiels ayant trait à la sécurité et à la pharmacovigilance dans le domaine des médicaments à usage humain) conclu entre l'EMEA et ces institutions comporte une clause ainsi rédigée: "*Les participants affirment qu'ils respecteront les principes énoncés dans la directive 95/46/CE et le règlement (CE) nº 45/2001 sur la protection des personnes à l'égard du traitement de données à caractère personnel et la libre circulation de ces données. Les participants affirment en outre qu'ils s'abstiendront de traiter des données à caractère personnel en vue de finalités non légitimes ou de transmettre ces données à des personnes non autorisées"*;

*v)* mesures adoptées pour veiller à ce que les utilisateurs n'aient accès qu'aux ressources nécessaires pour exécuter leurs tâches et mécanismes utilisés pour assurer l'identification sûre et personnalisée des utilisateurs: chaque utilisateur doit suivre une procédure d'inscription au cours de laquelle il donne une série de données à caractère personnel. Une fois inscrit, il reçoit un mot de passe et un identifiant. Les promoteurs et les TAMM ont un accès limité, qui ne leur permet de voir que les données que leur société a transmises;

*vi)* toujours à ce propos, l'EMEA a signalé que les profils d'utilisateurs étaient fondés sur une inscription de groupe. Toutes les demandes sont conservées et journalisées dans le "Service Desk System". Par conséquent, toutes les informations ne sont accessibles que sur la base du "privilège moindre", afin d'empêcher et de minimiser les risques d'accès non autorisés. Les profils actuellement attribués à EudraVigilance (publiés sur son site) sont les suivants: "parcourir EudraVigilance", "créer et envoyer des rapports de sécurité", "envoyer un rapport sur un médicament", "parcourir et envoyer un rapport de sécurité et un rapport sur un médicament", "pas de droit d'accès". Ce dernier statut sera attribué à un utilisateur par l'EMEA pour donner suite à une demande en ce sens d'une organisation (par exemple, si l'utilisateur n'est plus autorisé à accéder à EudraVigilance parce qu'il n'est plus un employé de l'organisation ou a changé de service);

*vii)* en termes de contrôle de l'accès aussi, l'EMEA utilise actuellement dans le site EVWEB un schéma d'accès qui repose sur l'utilisation du protocole de sécurité hypertext transport (HTTPS). Des certificats sont utilisés pour vérifier l'identité des organisations au niveau de la passerelle

d'EudraVigilance, ainsi que pour signer des messages en vue du processus d'échange électronique. Les certificats sont délivrés via une société qui intervient en tant qu'autorité de certification;

*viii)* l'EMEA a procédé à un examen de la sécurité des TI axé sur EudraVigilance avec l'aide d'un consultant extérieur en 2003 et la sécurité des TI de l'EMEA a aussi été vérifiée par une société extérieure en 2009;

*ix)* il n'y a pas de procédure pour le signalement et la gestion d'incidents susceptibles d'affecter des données à caractère personnel;

*x)* journalisation des opérations d'accès à EudraVigilance: selon les informations fournies, un journal est tenu pour les accès obtenus via le web ainsi que pour les accès à EudraVigilance Data Warehouse (EVDAS). Pour le web, deux types de journaux existent actuellement: a) journalisation des opérations d'accès au système, reprenant des éléments comme le nom d'utilisateur, l'adresse ip, première et dernière connexion des utilisateurs accédant au système; b) journalisation des événements dans la base de données, reprenant les opérations effectuées par les utilisateurs connectés. Ces journaux sont actuellement conservés selon la capacité de stockage dont dispose le système, soit trois mois environ. Dans le cas d'EVDAS, des informations sont journalisées à propos des rapports, mais elles ne comprennent pas les paramètres exacts associés aux rapports. Ces informations sont conservées indéfiniment;

*xi)* utilisation de dossiers temporaires ou d'exemplaires de travail des documents: l'EMEA a indiqué que les versions imprimées des informations stockées dans la base de données, de même que les rapports et les documents de travail concernant EudraVigilance, étaient considérées comme confidentielles conformément au règlement (CE) nº 1049/2001;

*xii)* lignes directrices en matière de sécurité: l'EMEA a fait savoir qu'elle était en train d'élaborer des documents à ce sujet. Le premier de ces documents en est au stade de la révision et de l'approbation par la direction. Les documents à élaborer sont intitulés: violations, reconnaissance de responsabilité, accès aux systèmes informatiques, à Internet et aux courriels, matériel informatique, gestion des données, utilisation de logiciels, signalement des incidents de sécurité;

*xiii)* l'EMEA applique actuellement des lignes directrices sur la gestion de la sécurité informatique qui s'inspirent de la norme ISO 27001/2.

## 2.2 Aspects juridiques

### 2.2.1 Aspects préliminaires

Dans le présent avis, le CEPD examine si l'EMEA se conforme au règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (ci-après dénommé "le règlement") lorsqu'elle traite des données dans le cadre de la gestion d'EudraVigilance. Cet examen et les recommandations qui en découlent ont pour toile de fond les éléments qui suivent.

En premier lieu, le traitement de données par EudraVigilance se fait conformément aux règles en vigueur sur la pharmacovigilance, y compris celles qui ont été élaborées dans des instruments ultérieurs (décisions et lignes directrices, par exemple) par l'EMEA ou par la Commission et l'EMEA conjointement. Certaines de ces règles font actuellement l'objet d'un réexamen de la part des décideurs. Le CEPD a rendu le 22 avril 2009 un avis sur les propositions de la Commission visant à adapter les règles en matière de pharmacovigilance, y compris le contrôle des effets

indésirables de médicaments. Bien que les observations présentées à cette occasion l'aient été "*de lege ferenda*", elles sont parfaitement applicables au traitement de données effectué actuellement par EudraVigilance. C'est pourquoi le présent avis reproduit en partie, dans le contexte du traitement ici visé, des arguments et recommandations identiques ou similaires à ceux qui figurent dans l'avis du 22 avril 2009.

En deuxième lieu, EudraVigilance est une base de données gérée par l'EMEA mais dont le contenu provient des ANC, des TAMM et des promoteurs d'essais cliniques, qui transmettent ces informations à l'EMEA. Chacun de ces acteurs est tenu de respecter des cadres juridiques différents en matière de protection des données: l'EMEA doit se conformer au règlement, tandis que les ANC, les TAMM et les promoteurs doivent se conformer au droit national mettant en oeuvre la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après dénommé "la directive").

En troisième lieu, les ANC, les TAMM et les promoteurs sont responsables du traitement des données qu'eux-mêmes traitent en tant que fournisseurs d'informations et utilisateurs du système. L'EMEA joue le même rôle dans le cadre de sa gestion d'EudraVigilance, parce que, outre sa tâche de vérification des informations reçues, il lui appartient de faire fonctionner le système, d'en assurer la maintenance technique et d'en garantir la sécurité globale. Par conséquent, tous les acteurs partagent des responsabilités au regard des droits des personnes concernées, en vertu de cadres juridiques différents et dans la limite de leurs fonctions. C'est pourquoi tous les acteurs peuvent être considérés comme des "responsables conjoints du traitement" pour la partie du traitement qui relève directement de leur compétence. Comme cela est développé plus loin, les différentes entités doivent, en tant que "co-responsables du traitement", coordonner leurs efforts afin de respecter leurs obligations.

Le présent contrôle préalable a pour objet de vérifier si l'EMEA se conforme au règlement, et non d'examiner si les entités nationales respectent leur législation nationale en matière de protection des données. Toutefois, le respect par l'EMEA des obligations qui lui incombent en vertu du règlement dépend jusqu'à un certain point du respect de leurs règles par les ANC, les TAMM et les promoteurs lorsqu'ils collectent et transmettent les informations. **C'est pourquoi il est de la plus grande importance que les co-responsables du traitement se concertent pour assurer le respect de leurs obligations.** Dans ce contexte, ils doivent mettre en place une coordination effective. Le droit des particuliers à la protection de leurs données et au respect de leur vie privée peut être compromis si les différents co-responsables du traitement ne veillent pas à ce que, tant au stade de la collecte des informations qu'à celui de leur introduction dans EudraVigilance, les personnes concernées soient informées du traitement. On ne s'étonnera dès lors pas si, dans le présent avis, le CEPD recommande à diverses reprises à l'EMEA de coordonner ses efforts avec ceux des entités nationales pour assurer le respect des règles en vigueur.

### 2.2.2 Contrôle préalable

Le présent contrôle préalable porte sur la gestion d'EudraVigilance par l'EMEA conformément à l'article 57, paragraphe 1, point d), du règlement (CE) nº 726/2004. Ainsi que nous l'avons indiqué précédemment, EudraVigilance est un réseau centralisé de traitement de données et un système de gestion permettant de signaler et d'évaluer des effets indésirables présumés durant la phase de développement des médicaments et après leur mise sur le marché dans la CE et l'EEE.

***Applicabilité du règlement.*** Le 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 dans un fichier"* ainsi qu'au traitement de données *"par toutes les*

*institutions et tous les organes communautaires, dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire*". Pour les raisons exposées ci-dessous, tous les éléments justifiant l'application du règlement sont réunis en l'espèce.

Premièrement, les données figurant dans EudraVigilance comportent des *données à caractère personnel* telles que définies à l'article 2, point a), du règlement. Il s'agit en particulier de données de patients comportant des informations sensibles, comme ses antécédents médicaux et des données d'identification émanant des personnes qualifiées. Deuxièmement, les données à caractère personnel collectées font l'objet de *traitements automatisés*, tels que définis à l'article 2, point b), du règlement. En fait, les données à caractère personnel sont introduites dans EudraVigilance, où divers destinataires y ont accès en ligne. Enfin, le traitement est effectué par une agence (l'EMEA) qui fait partie de l'Union européenne, dans le cadre du droit communautaire (article 3, paragraphe 1, du règlement). Par conséquent, tous les éléments justifiant l'application du règlement sont réunis en l'espèce.

***Justification du contrôle préalable.*** L'article 27, paragraphe 1, du règlement soumet au contrôle préalable du CEPD "*les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités*". Le paragraphe 2 énumère les traitements susceptibles de présenter de tels risques; la liste inclut, au point a), "les traitements de données relatives à la santé". La plupart des données traitées dans EudraVigilance sont des données relatives à la santé, comprenant notamment les antécédents médicaux des patients, les réactions à des médicaments, etc. C'est pourquoi leur traitement doit soumis à un contrôle préalable du CEPD.

***Contrôle préalable effectué a posteriori.*** Étant donné que le contrôle préalable vise à faire face à des situations susceptibles de présenter certains risques, l'avis du CEPD devrait être rendu avant le début du traitement concerné. Or, en l'espèce, le traitement a déjà été mis en œuvre. Cela ne devrait cependant pas constituer un problème insurmontable à condition que toutes les recommandations formulées par le CEPD soient pleinement prises en compte et que le traitement soit adapté en conséquence.

***Notification et délai pour rendre l'avis du CEPD.*** La notification a été reçue le 25 juin 2008. En raison de la complexité du système, le délai dans lequel le CEPD doit rendre son avis a été prolongé de deux mois. Conformément à l'article 27, paragraphe 4, du règlement, ce délai a été suspendu pendant 223 jours au total afin d'obtenir des informations complémentaires et de permettre au responsable du traitement d'examiner le projet d'avis. Le mois d'août n'étant pas pris en compte dans ces calculs, l'avis doit donc être adopté au plus tard le 7 septembre 2009.

### 2.2.3 Licéité du traitement

Le traitement de données à caractère personnel ne peut être effectué que s'il est justifié par un ou plusieurs des motifs visés à l'article 5 du règlement. Le motif justifiant le traitement est énoncé au point a) de l'article 5, selon lequel le traitement de données peut être effectué 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*".

Pour déterminer si le traitement est conforme à l'article 5, point a), du règlement, il convient de répondre aux deux questions qui suivent. Premièrement, le traité ou d'autres actes législatifs prévoient-ils une mission qui est d'intérêt public? Deuxièmement, le traitement effectué par l'EMEA est-il effectivement nécessaire à l'exécution de cette mission?

***Base juridique.*** Parmi les fondements juridiques qu'offrent le traité ou d'autres instruments législatifs qui justifient le traitement, le CEPD relève les éléments suivants:

1) l'article 22 et l'article 57, paragraphe 1, point d), du règlement (CE) nº 726/2004 du Parlement européen et du Conseil du 31 mars 2004 établissant des procédures communautaires pour l'autorisation et la surveillance en ce qui concerne les médicaments à usage humain et à usage vétérinaire, et instituant une Agence européenne des médicaments;

2) divers articles de la directive 2001/83/CE du Parlement européen et du Conseil du 6 novembre 2001 instituant un code communautaire relatif aux médicaments à usage humain;

3) les lignes directrices sur la pharmacovigilance pour les médicaments à usage humain;

4) la directive 2001/20/CE du Parlement européen et du Conseil du 4 avril 2001 concernant le rapprochement des dispositions législatives, réglementaires et administratives des États membres relatives à l'application de bonnes pratiques cliniques dans la conduite d'essais cliniques de médicaments à usage humain.

La législation susmentionnée non seulement crée l'EMEA, mais aussi exige la mise en place d'un système de pharmacovigilance dans lequel sont collectées les informations "*nécessaires à la surveillance de la sécurité des médicaments et à la protection de la santé publique*". Elle attribue en outre clairement à l'EMEA la tâche d'assurer la diffusion dans la Communauté, au moyen d'une base de données, des informations sur les effets indésirables de médicaments autorisés, l'objectif final étant que l'EMEA prenne les mesures appropriées. EudraVigilance a été créée pour exécuter ces missions. Compte tenu de ce qui précède, le CEPD a toutes les raisons de penser que le cadre juridique susmentionné légitime et justifie la collecte des informations sur les effets indésirables et leur traitement ultérieur dans EudraVigilance.

***Critère de la nécessité.*** Selon l'article 5, point a), du règlement, le traitement des données doit être "*nécessaire à l'exécution d'une mission*", comme indiqué ci-dessus. Cette nécessité est ainsi directement liée à la finalité dudit traitement. En l'espèce, les finalités globales d'EudraVigilance sont de détecter les signaux de sécurité associés à des médicaments et d'être à même de prendre les mesures appropriées.

Le CEPD est conscient que, pour exécuter la mission décrite ci-dessus, l'EMEA doit nécessairement traiter des données à caractère personnel. Dans ce contexte, l'article 5, point a), du règlement est respecté. Cela dit, comme il l'explique plus en détails au point 2.2.5 ("qualité des données"), il n'est pas convaincu que *toutes* les données à caractère personnel et *tous* les traitements effectués dans le cadre d'EudraVigilance soient effectivement nécessaires au regard de la finalité poursuivie. Même s'il comprend parfaitement les raisons sous-tendant la nécessité de collecter et de traiter ensuite certaines données à caractère personnel, il se demande si toutes les possibilités ont été examinées, par l'EMEA avec les ANC et d'autres partenaires intéressés, pour ramener le traitement de données à caractère personnel à ce qui est véritablement nécessaire. De surcroît, si toutes les informations sont effectivement nécessaires, à tous les stades, le CEPD estime que l'EMEA devrait examiner dûment la possibilité d'utiliser des pseudonymes dans les informations figurant dans les rapports de sécurité et lui en rendre compte. À cet égard, il souhaite que l'EMEA et les ANC explorent cette possibilité et s'entendent sur une approche harmonisée applicable à la collecte et au traitement ultérieur des données à caractère personnel.

Compte tenu de ce qui précède, le CEPD est d'avis que, si le traitement est d'une façon générale conforme à l'article 5, point a), du règlement, cette conclusion doit être nuancé en tenant compte des observations ci-dessus, qui sont développées au point 2.2.5.

### 2.2.4 Traitement portant sur des catégories particulières de données

Le traitement de données à caractère personnel relatives à la santé est interdit sauf s'il est justifié pour l'un des motifs énoncé à l'article 10, paragraphes 2 et 3, du règlement. Selon le paragraphe 2, point a), cette interdiction ne s'applique pas lorsque "*la personne concernée a donné son consentement explicite à un tel traitement*" et, selon le paragraphe 3, lorsque "*le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, (…) et que le traitement de ces données est effectué par un praticien de la santé soumis au secret professionnel ou par une autre personne également soumise à une obligation de secret équivalente*". On trouve des règles similaires dans les législations nationales qui mettent en œuvre la directive. En outre, ces textes législatifs et l'article 10, paragraphe 3, du règlement prévoient que des données relatives à la santé peuvent être traitées dans le cadre de la médecine préventive: "*aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé et lorsque le traitement de ces données est effectué par un praticien de la santé soumis au secret professionnel ou par une autre personne également soumise à une obligation de secret équivalente*".

EudraVigilance comporte des données relatives à la santé de patients qui sont collectées par les ANC et les TAMM. L'EMEA, les ANC et les TAMM sont co-responsables au regard du critère de la nécessité d'avoir des motifs prévus par la loi pour traiter ces données. Selon les législations nationales qui mettent en œuvre la directive, la collecte et le traitement ultérieur dans le cadre d'EudraVigilance de données relatives à la santé au niveau national peuvent être justifiés par la nécessité de ce traitement aux fins de la médecine préventive, afin d'éviter que les effets indésirables de certains médicaments ne se multiplient. Pour autant qu'il joue le même rôle, le traitement effectué par l'EMEA pourrait aussi être justifié par le même motif, tiré de l'article 10, paragraphe 3, du règlement.

Pour appliquer l'article 10, paragraphe 3, du règlement et les exceptions similaires figurant dans les législations nationales, il faut que toutes les données relatives à la santé à fournir soient nécessaires "*aux fins de la médecine préventive*". Il s'agit là d'un critère strict: si les données provenant de patients ne sont pas nécessaires ni indispensables, l'exception ne s'applique pas. Par conséquent, il faut que tous les responsables du traitement concernés vérifient que les données relatives à la santé figurant dans les rapports de sécurité sont absolument nécessaires. Cet argument confirme la position qui est développée au point 2.2.5 sur la nécessité de veiller à l'adéquation des données.

Si l'EMEA et les responsable du traitement au niveau national souhaitent introduire des informations qui ne sont pas nécessaires aux fins de la médecine préventive, sur la base tant de l'article 10, paragraphe 2, point a), du règlement que des législations nationales qui mettent en œuvre la directive, il leur faut trouver des base juridiques supplémentaires. Des autres justificatifs prévus par la loi, seul le consentement de la personne concernée apparaît comme adéquat. Dès lors, pour collecter et traiter ensuite des informations qui ne sont pas nécessaires aux fins de la médecine préventive, il faut obtenir le *consentement explicite* du patient. Ce consentement ne doit évidemment pas être donné deux fois (lors de la collecte des données et lors de leur introduction dans EudraVigilance): lorsque les ANC et les TAMM demandent le consentement pour collecter les informations, ils peuvent aussi demander de consentir au transfert desdites informations à l'EMEA, à leur introduction dans EudraVigilance et à leur diffusion ultérieure aux personnes qui disposent d'un accès à EudraVigilance.

Si le consentement à la collecte initiale et au traitement ultérieur des données dans le cadre d'EudraVigilance n'a pas été obtenu lorsque les ANC ou les TAMM procèdent à leur collecte, l'EMEA devra l'obtenir ensuite, à moins d'invoquer l'exception de l'article 10, paragraphe 3, du

règlement. Tout dépendra alors des informations figurant dans le rapport de sécurité, qui feront l'objet d'un examen au cas par cas. Le CEPD sait que l'EMEA n'a pas de lien direct avec les patients et qu'il lui serait difficile, parfois même impossible, de les contacter pour obtenir leur consentement. Pour résoudre ce problème, il est essentiel que l'EMEA coopère avec les ANC et les TAMM de manière à s'assurer que ces derniers ne lui transmettent que des données relatives à la santé de patients qui ont déjà donné leur consentement ou des données qui sont nécessaires aux fins de la prévention médicale et qui peuvent donc être traitées sans consentement explicite.

Il convient de lire ce qui précède avec les observations présentées au point 2.2.5 concernant la nécessité d'utiliser un pseudonyme. La nécessité d'obtenir le consentement du patient sera moindre si les informations figurant dans les rapports de sécurité sont traitées dans l'anonymat ou le pseudo-anonymat.

### 2.2.5 Qualité des données

***Adéquation, pertinence et proportionnalité.*** Selon l'article 4, paragraphe 1, point c), du règlement, 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; c'est ce qu'on appelle le "principe de la qualité des données".

**Informations contenues dans EudraVigilance qui concernent des personnes travaillant pour des ANC ou des TAMM:** le CEPD n'a aucune raison de penser que les informations d'identification (nom, date de naissance, carte d'identité, passeport), l'adresse et le numéro de téléphone sont excessifs. Compte tenu de la nécessité d'assurer une identification sûre et personnalisée des utilisateurs, le type d'informations demandées semble approprié. Néanmoins, des informations comme la taille, la couleur des yeux, un pseudonyme et le nombre d'enfants semblent excessives au regard de la finalité du traitement, à savoir l'inscription des utilisateurs d'EudraVigilance . Le CEPD sait que ces informations figurent sur certaines cartes d'identité nationales et que l'EMEA les enregistre pour cette raison et les garde au motif que "*c'est l'unique identification de l'utilisateur inscrit dans EV et que nous devons empêcher les accès non autorisés à EV dans EVPM et EVCTM. Nous conservons les enregistrements aussi longtemps que l'organisation est inscrite*". Si le CEPD accepte que ces données soient enregistrées, il estime que, dès que la procédure d'inscription de l'utilisateur est terminée, y compris l'identification et la vérification des informations figurant sur la carte d'identité ou dans le passeport, l'EMEA a la possibilité de renvoyer, détruire ou cacher les informations excessives.

***Données relatives à la santé des patients:*** comme l'indique la notification, le rapport de sécurité ne mentionne pas les patients par leur nom. Dans certains cas, toutefois, un numéro spécifique est attribué à chaque patient et il est dès lors possible de retrouver l'identité de la personne concernée dans l'ensemble du système. Même sans ce numéro, le patient peut rester identifiable si l'on recoupe plusieurs informations figurant dans les rapports.

L'EMEA a précisé à diverses occasions que la collecte d'informations à caractère personnel et leur introduction dans EudraVigilance étaient nécessaires au regard d'une série de finalités, notamment la traçabilité (vérifier que le patient ou l'auteur du rapport existent réellement), le souci d'éviter les répétitions inutiles dans les rapports, un suivi éventuel et l'évaluation clinique des rapports.

Le CEPD comprend parfaitement les raisons précitées, qui sont tout à fait légitimes. Cependant, il n'est pas convaincu que les efforts adéquats ont été faits pour a) analyser les informations et veiller à ce que seules celles qui sont nécessaires soient collectées et ensuite traitées et, **plus particulièrement, pour b) étudier les possibilités de recourir à l'anonymisation ou à la**

**pseudonymisation dans les rapports de sécurité, notamment au moment de leur transfert vers EudraVigilance.**

La question a déjà été soulevée dans l'avis du 22 avril 2009 sur les propositions de la Commission visant à adapter le cadre relatif à la pharmacovigilance, où le CEPD demandait s'il était *nécessaire* de traiter les données relatives à la santé de personnes physiques identifiables à tous les stades du système de pharmacovigilance, en particulier au moment où l'EMEA doit introduire ces données dans EudraVigilance.

Cette préoccupation trouve écho dans l'extrait suivant des orientations en matière d'accès à EudraVigilance, qui prévoit explicitement l'utilisation des données du système en recourant à l'anonymisation ou à la pseudonymisation: "*Selon le projet de document concernant les orientations en matière d'accès à EudraVigilance, le système "devrait fonctionner sur la base de rapports anonymisés, de manière à ce qu'il ne soit pas possible d'identifier le patient. Des règles appropriées concernant l'anonymisation des données devraient être adoptées afin d'assurer une approche harmonisée de toutes les parties intervenantes (…). Cela concerne en particulier les informations sur les patients (nom, date de naissance, cause du décès) ou d'autres éléments permettant une identification, spécialement dans la synthèse du cas et les informations additionnelles figurant dans les rapports sur les effets indésirables*". Ce qui précède est également corroboré par la pratique actuelle de certaines ANC qui, se fondant sur les lois nationales mettant en œuvre la directive, n'incorporent pas de données d'identification personnelle dans les rapports de sécurité. Toutefois, on ne sait pas si cette pratique a créé des problèmes pour le fonctionnement général d'EudraVigilance.

Le CEPD admet que, au cours des premières phases du traitement telles que la collecte des données, il peut être impossible de ne pas traiter des données identifiables. Il concède que, dans certains cas précis, la nécessité de disposer de données à caractère personnel existe aussi à des stades ultérieurs, notamment lorsque les données sont introduites dans EudraVigilance; mais ensuite, lorsque les données doivent être enregistrées dans EudraVigilance et en particulier lorsqu'elles sont partagées avec d'autres parties prenantes, cette nécessité est beaucoup moins évidente dans la plupart des cas. Dans ce contexte, on peut se demander s'il ne suffirait pas de disposer de données ayant subi une pseudonymisation.

Pour satisfaire à l'exigence de qualité des données prévue dans les législations nationales sur la protection des données et dans le règlement, l'EMEA devrait, avec les ANC et d'autres co-responsables du traitement, examiner ces questions en profondeur. Le CEPD estime en particulier qu'il convient d'évaluer jusqu'à quel point on pourrait limiter la collecte et le traitement de données à caractère personnel aux différents stades. En outre, l'EMEA devrait, en collaboration avec les ANC et d'autres co-responsables du traitement, faire le nécessaire pour évaluer si l'utilisation de données pseudonymisées dans les rapports de sécurité serait suffisante pour atteindre les mêmes finalités. Le CEPD pense que, en appliquant les principes de la qualité des données et de leur utilisation minimale dans le cadre de procédures bien définies, il serait possible dans de nombreux cas d'obtenir, si pas une anonymisation totale, au moins une pseudonymisation. L'application de ces principes et la mise en place de procédures appropriées ne devraient pas incomber à l'EMEA seule, mais également aux ANC et aux TAMM dans le cadre de la collecte initiale des données. À ce sujet, le CEPD invite l'EMEA à prendre en considération, en coordination avec les ANC, les recommandations suivantes:

premièrement, rechercher quelles sont les données à caractère personnel qui sont nécessaires aux fins des rapports de sécurité, en tenant compte des principes de la minimisation et de la qualité des données; ce faisant, il faudrait viser à ne collecter que les données qui sont nécessaires. Le

formulaire de rapport de sécurité qui en résultera devrait être accompagné de recommandations sur la manière de le remplir afin d'utiliser un minimum de données à caractère personnel;

deuxièmement, étudier en même temps les possibilités d'anonymisation ou pseudonymisation des informations à caractère personnel. L'EMEA devrait, avec les ANC et les TAMM, évaluer la manière et la mesure dans laquelle ces mécanismes pourraient être appliqués aux données figurant dans les rapports de sécurité. Dans le cas où il est véritablement nécessaire de traiter des données identifiables ou lorsque les données ne peuvent rendues anonymes, l'EMEA devrait faire tout ce qui est en son pouvoir pour exploiter des solutions techniques permettant une identification indirecte des personnes concernées, par exemple en recourant à des mécanismes de pseudnonymisation; troisièmement, veiller à ce que, aux différents niveaux, les responsables du traitement procèdent à un "contrôle de la qualité" des données. Tout comme ils vérifient l'exactitude des informations (voir le point "exactitude" ci-dessous), les différents responsables du traitement devraient aussi inclure dans leur procédure la vérification de la qualité des données avant d'être à même d'introduire les rapports de sécurité dans EudraVigilance.

Rappelons ici que le traitement de données relatives à la santé est soumis à un critère strict pour satisfaire au principe de l'exactitude: seules les données véritablement nécessaires pour réaliser la finalité recherchée doivent être collectées, ce qui est encore plus évident dans le cas (signalé plus haut) où ce traitement ne repose pas sur un consentement, mais sur l'exception prévue à l'article 10, paragraphe 3, qui exige expressément que les données ne soient traitées que lorsque c'est "nécessaire". En résumé, l'utilisation de données identifiables devrait être limitée autant que possible et empêchée ou arrêtée le plus vite possible dans les cas où elle n'est pas considérée comme nécessaire. La seule conclusion possible à ce stade est que le respect des exigences de nécessité et de proportionnalité inscrites à l'article 4, paragraphe 1, point c), et à l'article 10, paragraphe 3, du règlement dépend du résultat de m'application des mesures évoquées ci-dessus pour évaluer les possibilités en termes d'anonymisation, de pseudonymisation et de limitation des données traitées.

***Loyauté et licéité.*** L'article 4, paragraphe 1, point a), du règlement exige que les données soient traitées loyalement et licitement. La question de la licéité a été analysée ci-dessus (point 2.2.2). Celle de la loyauté est étroitement liée à l'objet du point 2.2.8, à savoir les informations fournies aux personnes concernées.

***Exactitude.*** Selon 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*". Il est dans l'intérêt de l'EMEA et de toutes les parties intéressées par EudraVigilance que les informations figurant dans les rapports de sécurité soient exactes. À cette fin, il ressort des lignes directrices sur la pharmacovigilance des médicaments à usage humain qu'il existe diverses règles et dispositions, s'appliquant aux différents stades du traitement, qui ont pour but d'assurer l'exactitude des informations à introduire. Compte tenu de l'existence de ces procédures destinées à obtenir les informations les plus fiables, le CEPD n'a aucune raison de penser que le principe de l'exactitude des données n'est pas respecté.

### 2.2.6 Conservation des données

L'article 4, paragraphe 1, point e), du règlement pose le principe selon lequel les données à caractère personnel doivent être "*conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement".*

Selon la notification, les données à caractère personnel sont conservées pendant une période indéterminée afin de permettre une évaluation scientifique pleine et entière des informations.

Le CEPD croit savoir que cette façon de faire vise à optimaliser la tâche de l'EMEA consistant à protéger la sécurité et l'efficacité des médicaments, ainsi que sa mission générale consistant à promouvoir la santé et le bien-être. Cependant, il se demande si, dans tous les cas, les raisons de conserver des informations personnelles identifiables restent valables pour une période illimitée - même après le décès du patient. Dans ce contexte, il invite l'EMEA à réfléchir à la durée appropriée pendant laquelle les informations restent utiles au regard des finalités du traitement. Ce faisant, l'EMEA devrait se concentrer sur le véritable objectif de la conservation des données et prendre en compte la nature sensible de ces dernières. À ce sujet, le recours à l'anonymisation ou à la pseudonymisation serait particulièrement heureux, puisqu'il serait alors inutile de supprimer les données après un certain temps.

### 2.2.7 Transferts des données

Les articles 7, 8 et 9 du règlement énoncent certaines obligations qui s'appliquent lorsque les responsables du traitement transfèrent des données à caractère personnel à des tiers. Les règles diffèrent selon que les données sont transférées *i)* à des institutions ou organes communautaires (article 7), *ii)* à des destinataires relevant de la directive 95/46 (article 8), ou *iii)* à d'autres types de destinataires (article 9).

D'après la notification, les informations sont communiquées à des destinataires qui rentrent dans les catégories ii) et iii) ci-dessus.

Avant d'évaluer les motifs prévus par la loi pour justifier le transfert de données à caractère personnel, le CEPD souhaite rappeler ce qu'il a dit au point 2.2.5 et qui a une incidence directe sur le présent sujet, à savoir que la nécessité, en termes généraux, d'introduire des données à caractère personnel dans EudraVigilance n'a pas été établie. L'utilisation de telles données peut être nécessaire et inévitable dans certains cas précis, mais elle n'est pas établie si elle se fait plus généralement. Si l'EMEA met en œuvre une approche limitant sérieusement l'utilisation de données à caractère personnel introduites dans EudraVigilance, la portée des obligations décrites ci-dessous s'en trouvera forcément réduite.

***Transferts à des autorités compétentes des États membres (ANC) relevant de la directive 95/46/CE (article 8 du règlement)***

Le CEPD fait observer que, quand les destinataires relèvent de la catégorie ii), les informations sont partagées avec des ANC. Comme il l'explique plus en détail ci-dessous, ce partage d'informations doit se faire conformément à l'article 8 du règlement. En outre, les TAMM disposent d'un accès, mais uniquement aux informations qu'eux-mêmes ont communiquées à l'EMEA; on ne peut donc parler de partage d'informations avec eux. Cependant, l'EMEA envisage de leur donner accès aux autres informations contenues dans EudraVigilance. Si tel devait être le cas, elle devrait respecter l'article 8 du règlement, qui régit les transferts à des destinataires relevant de la directive 95/46.

L'article 8 contient différentes justifications du transfert de données à caractère personnel. Vu les conditions particulières du traitement qu'elle effectue, l'EMEA peut se prévaloir du point a), selon lequel des données à caractère personnel peuvent être transférées si elles vont être utilisées pour exécuter une mission d'intérêt public - ou du point b), si le transfert est fait dans l'intérêt légitime de la personne concernée. Alors que l'article 8 prévoit que c'est au destinataire à établir l'existence

d'un intérêt, le CEPD interprète pour sa part cette disposition comme signifiant que, si le transfert n'est pas effectué à la demande du destinataire, c'est à l'expéditeur qu'incombe la charge de la preuve. Dans ce cas, l'EMEA pourrait devoir soumettre le traitement à un nouvel examen.

Conformément à ce qui précède, lorsque les informations ne sont pas envoyées à la demande du destinataire, l'EMEA doit établir la nécessité du transfert. Le CEPD est conscient qu'il existe un besoin permanent que le destinataire reçoive les informations lorsqu'elles sont disponibles. Ce besoin a été pris en compte dans le cadre réglementaire mentionné au point 2.2.2. En particulier, l'article 57, paragraphe 1, point d), du règlement 726/2004 précise que toutes les ANC devraient avoir accès en permanence à EudraVigilance. De l'avis du CEPD, cela suffit pour établir l'existence d'un intérêt à disposer de ces informations.

Bien entendu, ce qui précède doit être appliqué en tenant compte des observations émises aux points 2.2.4 et 2.2.5 à propos de la nécessité de ne traiter des données sensibles que lorsque c'est absolument nécessaire. On peut donc légitimement invoquer l'article 8 dans la mesure où le volume de données relatives à la santé qui sont transférées est limité à ce qui est absolument nécessaire.

***Transferts de données à caractère personnel à des destinataires autres que des institutions et organes communautaires et qui ne relèvent pas de la directive 95/46/CE (article 9)***

Les destinataires de la catégorie iii) avec lesquels l'EMEA partage des informations sont les autorités suivantes: le ministère de la santé du Canada, le ministère de la santé, de l'emploi et du bien-être du Japon et la Federal Drugs Administration (FDA) des États-Unis. Les données transférées portent sur des effets indésirables et peuvent inclure des données à caractère personnel. L'EMEA a procédé à un échange de lettre avec les représentants des ministères de ces trois pays.

*Interdiction des transferts de données et rôle de la Commission:* l'article 9, paragraphe 1, du règlement stipule 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*".

C'est la Commission européenne qui est compétente pour déterminer, sur la base de l'article 25, paragraphe 6, de la directive, si un pays tiers assure un niveau de protection adéquat au moyen de sa législation nationale ou du fait de ses engagements internationaux.

La Commission n'a pas encore fait savoir si elle estimait que la législation ou les engagements applicables aux destinataires des données transmises par l'EMEA (Canada, Japon et États-Unis) assuraient un niveau de protection adéquat.

***Détermination par le responsable du traitement du niveau de protection du transfert assuré par chacun des trois ministères.*** Selon l'article 9, paragraphe 2, du règlement, l'EMEA est, en tant que responsable du traitement, en mesure d'évaluer si le transfert spécifique de données vers les ministères de la santé des trois pays offre un niveau de protection adéquat. Ce faisant, l'Agence doit évaluer tous les éléments caractérisant le transfert: la nature des données, la finalité et la durée du traitement envisagé, le type de destinataire, la législation, tant générale que sectorielle, ainsi que les règles professionnelles et les mesures de sécurité appliquées dans ce pays. Le CEPD suggère d'établir un registre décrivant l'évaluation et son résultat.

L'EMEA n'a pas fait savoir au CEPD si elle avait procédé à une évaluation de ce type ni fait connaître les conclusions qu'elle a pu en tirer. Lorsqu'elle procède à cette évaluation, l'EMEA voudra peut-être tenir compte de ce qui suit.

Premièrement, vu que la Commission n'a pas établi que la législation ou les engagements internationaux de ces pays offrent une protection adéquate, il peut être utile de tenir compte qu'une telle législation existe et s'appliquerait comme suit aux données transférées dans ces pays:

*Japon:* depuis 2005, le Japon dispose d'une législation sur la protection des données (Personal Information Protection Law), mais celle-ci ne s'applique pas aux institutions publiques, aux organismes publics locaux ni aux agences administratives indépendantes, qui sont soumises à une autre loi (Act on the Protection of Personal Information Held by Administrative Organs - Loi nº 58 de 2003, dans sa dernière version). Par exemple, la loi nº 58 de 2003 reconnaît le droit d'accès mais ne contient pas les autres garanties prévues par l'UE.

*Canada.* La Loi sur la protection des renseignements personnels et les documents électroniques ("PIPEDA") a été considérée comme adéquate, mais elle ne s'applique qu'au secteur privé, et non au secteur public. Au niveau fédéral, la loi sur la protection des renseignements personnels réglemente la collecte, l'utilisation et la divulgation de données à caractère personnel par les institutions étatiques. Elle donne aux particuliers un droit d'accès aux informations personnelles détenues par ces agences, mais ne comprend pas les autres protections prévues par l'UE. Elle décrit aussi la mission et les tâches du Commissariat fédéral à la protection de la vie privée, qui est responsable, entre autres, de l'application de la loi. Ce dernier a suggéré de réformer la loi sur la protection des renseignements personnels.

*États-Unis.* Les principes dits de "Safe Harbour" ont aussi été considérés comme offrant un niveau adéquat de protection, mais ils ne s'appliquent pas à la FDA du ministère de la santé. La protection des informations personnelles traitées par le gouvernement fédéral fait principalement l'objet de la Privacy Act de 1974 et de la Computer Matching and Privacy Act. La première a été adoptée à la fois pour protéger les informations personnelles figurant dans les bases de données fédérales et pour donner aux particuliers certains droits sur lesdites informations (droit d'accès). L'Office of Management and Budget a été chargé d'une supervision centrale.

Deuxièmement, dans les trois cas, l'EMEA devrait évaluer si les normes en vigueur en matière de protection des données sont appliquées dans la pratique et s'il existe une véritable procédure permettant aux particuliers de faire valoir leurs droits ou d'obtenir réparation si les choses vont mal.

Troisièmement, dans les trois cas, l'EMEA devrait, lorsqu'elle évalue les circonstances du transfert, tenir compte, par exemple lorsque des informations directement identifiables sont transférées, des mesures de sécurité prises pour protéger les données.

Quatrièmement, il faudrait aussi tenir compte des engagements pris par les parties (expéditeur et destinataire) pour préserver la confidentialité des informations, ainsi que de l'engagement de ne pas transférer les données sans avoir consulté au préalable l'EMEA.

***Possibilité d'invoquer des dérogations ou des clauses contractuelles.*** Si l'EMEA n'effectue pas l'évaluation décrite ci-dessus ou si elle conclut que les transferts de données n'offrent pas un niveau de protection adéquat, elle peut toujours se prévaloir des dérogations à l'interdiction énoncées à l'article 9, paragraphe 6, du règlement ou faire état de garanties suffisantes prévues dans des clauses contractuelles à conclure avec chacun des destinataires (article 9, paragraphe 7).

Parmi les diverses dérogations prévues au paragraphe 6, l'EMEA peut invoquer le point d), à savoir "*le transfert est nécessaire (…) pour des motifs d'intérêt public importants*". L'on peut soutenir que les transferts d'informations ont pour objectif global de contribuer à la protection et au renforcement de la santé publique et satisfont dès lors au critère de l'intérêt public. Cette dérogation, qui est également prévue par la directive, est censée s'appliquer aux transferts entre les administrations publiques, par exemple dans le cas de transferts de données entre les administrations douanières, fiscales ou de sécurité sociale. En l'espèce, il s'agit bien de transferts entre administrations, qui peuvent être considérés comme nécessaires pour un motif d'intérêt public, à savoir la protection de la santé des citoyens. Il ne s'agit pas d'un intérêt ordinaire, mais très important, ce qui plaide encore davantage en faveur de l'application de ce motif.

Toutefois, comme l'a constaté le groupe de travail de l'article 29, les exceptions aux obligations ne devraient s'appliquer qu'à des transferts de données occasionnels: "*le groupe recommande que les transferts de données à caractère personnel qui présentent la caractéristique d'être importants parce qu'ils sont répétés, volumineux ou habituels devraient, si possible, avoir lieu dans un cadre juridique spécifique (à savoir, des contrats ou des règles d'entreprise contraignantes*)".

Si les transferts de données de l'EMEA sont sporadiques (par exemple, s'ils ont lieu dans des cas très précis où ils sont absolument nécessaires), l'Agence serait à même d'invoquer cette dérogation. Par contre, si les transferts sont réguliers, elle devrait conclure des clauses contractuelles (voir ci-dessous) afin de prévoir des garanties.

Possibilité de recourir à des clauses contractuelles pour prévoir des garanties: le CEPD note que l'EMEA a procédé à un échange de lettres avec les trois ministères (Japon, Canada et Etats-Unis). Il faut se demander si ces lettres offrent les garanties nécessaires au sens de l'article 9, paragraphe 7, du règlement. Le CEPD constate que ces lettres ne contiennent aucune disposition spécifique sur la protection des données, mais des dispositions exigeant que la confidentialité des informations soit préservée, ainsi qu'un engagement de ne pas transférer les données sans consultation préalable de leur premier expéditeur. Les lettres ne prévoient pas l'application des principes essentiels en matière de protection des données, comme la qualité des données, la transparence, le droit d'accès, de rectification et d'opposition ou la sécurité, nécessaires pour assurer un niveau de protection adéquat.

En résumé, l'EMEA peut invoquer la dérogation prévue à l'article 9, paragraphe 6, point d), du règlement si les transferts sont occasionnels et peu nombreux. Sans cela, elle doit apprécier, en tenant compte des circonstances du transfert, si le destinataire offre des garanties adéquates pour ledit transfert. Si sa conclusion est négative, elle doit conclure avec les trois destinataires des accords prévoyant des garanties efficaces. Le CEPD invite l'EMEA à analyser les options susmentionnées et, en tenant compte des circonstances de l'espèce, à se mettre en conformité avec le règlement. Il souhaite être informé de l'issue de cette analyse. Si l'option retenue est le recours à des clauses contractuelles, par exemple, sur la base des échanges de lettres actuels ou de versions modifiées, il prie instamment l'EMEA de veiller à y inclure les principes essentiels en matière de protection des données et de l'en avertir en conséquence.

### 2.2.8 Information de la personne concernée

Selon l'article 11 du règlement, ceux qui collectent des données à caractère personnel sont tenus d'informer les personnes concernées de cette collecte et du traitement qui s'ensuit. L'article 12 vise les cas où les données n'ont pas été fournies par la personne concernée. Conformément aux deux dispositions, les personnes doivent en outre être informées, entre autres, des finalités du traitement et de l'identité des destinataires des données.

L'article 12, paragraphe 2, précise que cette information n'est pas requise, entre autres, i) si la personne est déjà informée ou ii) si l'information se révèle impossible ou implique des efforts disproportionnés.

Le CEPD a appris que l'EMEA ne donne aucune information aux personnes parce qu'elle n'a pas de contact direct avec elles et qu'identifier chacune d'elles, retrouver leur adresse et leur donner les informations requises serait une très lourde tâche. L'EMEA fait observer que les ANC, les TAMM et les promoteurs doivent respecter les dispositions nationales mettant en œuvre la directive, qui exigent d'informer les personnes du traitement et du transfert envisagé.

Le CEPD est d'accord avec l'EMEA et reconnaît que, dans la plupart des cas, il serait très peu commode, voire impossible, d'identifier les personnes visées dans les rapports de sécurité afin de leur donner les informations requises. À cet égard, il estime que l'EMEA peut invoquer l'article 12, paragraphe 2, et faire valoir que l'information impliquerait des efforts disproportionnés pour trouver les coordonnées des personnes.

Cependant, les entités au niveau local (ANC et TAMM) peuvent et doivent informer les personnes. Dans ce contexte, le CEPD estime que l'EMEA, dans la mesure où elle est co-responsable du traitement, doit assumer une certaine responsabilité pour veiller à ce que les ANC et les TAMM s'acquittent de leur obligation au niveau local, parce que ce respect au niveau local peut garantir celui au niveau de l'EMEA. Par exemple, si une note diffusée au niveau local avertit du transfert des données à l'EMEA et de leur utilisation ultérieure dans EudraVigilance, les personnes seront informées dans le respect de la législation tant nationale que communautaire sur la protection des données.

Même si l'EMEA n'a pas de pouvoir coercitif sur ces entités pour les obliger à remplir leurs obligations, elle peut contribuer à faciliter le respect des règles au niveau local. Le CEPD estime que certaines mesures pourraient être mises en œuvre dans ce but: l'EMEA devrait entrer en dialogue au moins avec les ANC, pour examiner comment assurer le respect de cette obligation. À ce sujet, le CEPD suggère de rédiger un modèle de note d'avertissement à utiliser lorsque les données sont collectées au niveau local, qui devrait faire référence au transfert vers l'EMEA et à la diffusion des informations via EudraVigilance.

Dans le cadre des efforts déployés pour veiller à ce que la note d'avertissement a bien été communiquée aux patients, l'EMEA devrait envisager d'insérer un avis sur son site Web, dans la partie consacrée à EudraVigilance, et à l'intégrer également dans le système utilisé par les ANC et les TAMM pour lui envoyer leurs rapports de sécurité.

Le CEPD invite l'EMEA à entreprendre ces travaux avec les ANC et, si possible, avec les TAMM, afin de garantir la remise d'une note d'avertissement aux personnes.

### 2.2.9 Droit d'accès et de rectification

Selon l'article 13 du règlement, la personne concernée a le droit d'obtenir du responsable du traitement, sans contrainte, à tout moment dans un délai de trois mois à partir de la réception de la demande d'information et gratuitement, 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 confère à la personne concernée le droit de rectifier les données inexactes ou incomplètes.

La notification ne mentionne pas les droits d'accès et de rectification des personnes concernées ni les procédures permettant de les exercer parce que, précise l'EMEA, l'Agence n'a pas de contact

direct avec les personnes concernées. L'EMEA a fait savoir au CEPD qu'elle n'avait jamais reçu de demande d'accès émanant de particuliers.

Le CEPD fait observer que, si les particuliers ne sont pas informés de ce que leurs données seront utilisées dans EudraVigilance, ils ne vont évidemment pas contacter l'EMEA pour présenter une demande d'accès, puisqu'ils ne savent toute simplement pas que leurs données sont traitées. Il est également possible qu'ils présentent une demande d'accès au niveau local.

Le CEPD estime que l'EMEA devrait mettre en place une procédure donnant accès aux données à caractère personnel et permettant de rectifier des données inexactes ou incomplètes lorsque les personnes concernées en font la demande. Si un patient ou d'autres personnes dont des données sont détenues par l'EMEA présentent une demande d'accès, l'Agence doit examiner ces demandes et y répondre en conséquence.

Le CEPD est conscient que, dans certains cas, il peut être difficile pour l'EMEA d'accorder l'accès. Cependant, ces difficultés n'éteignent pas l'obligation générale de l'EMEA consistant à examiner les demandes et à donner l'accès lorsqu'il est demandé. Toutefois, si dans un cas donné l'EMEA n'est pas capable d'identifier les informations relatives à un particulier qui demande à y accéder, elle peut légalement refuser l'accès en expliquant les raisons de son refus.

### 2.2.10 Mesures de sécurité

Selon les articles 22 et 23 du règlement, le responsable du traitement et le sous-traitant doivent 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 diffusion ou tout accès non autorisés, toute destruction accidentelle ou illicite, toute perte accidentelle ou toute altération, ainsi que toute autre forme de traitement illicite.

Le CEPD prend note des mesures techniques et organisationnelles actuellement adoptées par l'EMEA concernant EudraVigilance. Il prend également acte de l'adoption par l'EMEA de normes sur la gestion de la sécurité des informations. Il recommande néanmoins à l'EMEA d'adopter les mesures supplémentaires suivantes:

.....

## 3. Conclusion

À l'exception des questions soulevées au point 2.2.5 à propos de la "qualité des données", rien ne permet de conclure à un manquement aux dispositions du règlement, sous réserve que les considérations figurant dans le présent avis soient pleinement prises en compte. En ce qui concerne la qualité des données, il est impossible de ne pas procéder à un examen minutieux et à une réévaluation des pratiques actuelles. L'EMEA devrait en particulier:

- *entreprendre* un examen de la possibilité de réduire à son minimum le volume de données à caractère personnel figurant dans les rapports de sécurité. Examiner, avec les ANC et les TAMM, quelles sont les données véritablement nécessaires dans les rapports de sécurité, aux différents niveaux (local et EMEA), de sorte que les mêmes normes soient applicables dans l'ensemble de l'UE, en tenant compte du principe de la minimisation des données;
- *entreprendre* une étude des possibilités de recourir à l'anonymisation ou à la pseudonymisation des données à caractère personnel. L'EMEA devrait, avec les ANC et les TAMM, évaluer la mesure dans laquelle et les moyens par lesquels l'anonymisation et la

pseudonymisation pourraient s'appliquer aux données figurant dans les rapports de sécurité;

- *vérifier* qu'elle peut invoquer un des *motifs prévus par la loi* pour traiter les données relatives à la santé. À cette fin, l'EMEA veillera à ce que seules les données strictement *"nécessaires aux fins de la médecine préventive"* soient introduites dans EudraVigilance; à défaut, elle devra obtenir le consentement explicite visé à l'article 10, paragraphe 2, point a); si ledit consentement sert de motif, il convient de *coopérer* avec les ANC et les TAMM pour s'assurer que ceux-ci ne lui envoient que des données de patients qui ont donné leur consentement préalable;
- *examiner* si une période de conservation limitée des données permettrait d'atteindre les finalités recherchées par le traitement;
- *évaluer* les motifs justifiant de transférer des données en dehors de l'UE: les autorités destinataires assurent-elles un niveau de protection adéquat (article 9, paragraphe 2)? Ou bien une dérogation prévue à l'article 9, paragraphe 6, point d), s'applique-t-elle parce que les transferts ne sont pas réguliers? À titre subsidiaire, envisager de conclure des accords qui reprennent les principes essentiels de la protection des données. *Informer* le CEPD de la décision finale adoptée à cet égard;
- *ouvrir un dialogue* avec les ANC, les TAMM et les promoteurs afin d'élaborer un projet de note type qui donnerait aux particuliers les informations requises, et qui devrait mentionner EudraVigilance. Insérer également une note de ce type dans le site web de l'EMEA;
- mettre en place une procédure permettant d'exercer le droit d'accès et de rectification des données à caractère personnel;
- adopter les mesures de sécurité décrites dans le présent avis.

Fait à Bruxelles, le 7 septembre 2009.

***[Signé]***

Peter HUSTINX
Contrôleur européen de la protection des données