Avis de contrôle préalable sur le système d'alerte précoce et de réaction (EWRS) notifié par la Commission européenne le 18 février 2009

Bruxelles, le 26 avril 2010 (dossier 2009-0137)

1. Procédure

Le 18 février 2009, la Commission a notifié au Contrôleur européen de la protection des données (ci-après: le «**CEPD**») son système d'alerte précoce et de réaction (ci-après: l'«**EWRS**») pour la prévention et le contrôle des maladies transmissibles, aux fins d'un contrôle préalable *a posteriori*. Le 16 avril 2009, le CEPD a prolongé d'un mois la période qui lui était impartie pour émettre son avis, conformément à l'article 27, paragraphe 4, du règlement (CE) n° 45/2001 (ci-après: le «**règlement**»). Le 11 mai 2009, le CEPD a sollicité la tenue d'une réunion avec la Commission, afin d'obtenir des précisions sur certains faits, et a demandé à assister à une démonstration de l'EWRS. La réunion a eu lieu le 25 novembre 2009 et la Commission a fourni, à cette occasion, des informations complémentaires. Entre-temps, le CEPD a aussi procédé à une enquête auprès des autorités chargées de la protection des données dans les États membres, sur leur expérience de d'utilisation de l'EWRS au niveau national. En outre, le CEPD a envoyé, le 17 décembre 2009, une synthèse de son analyse des faits, accompagnée de demandes d'éclaircissement complémentaires. La Commission a répondu aux questions du CEPD le 12 mars 2010. Le 18 mars 2010, le CEPD a prolongé d'un mois supplémentaire le délai dont il disposait pour émettre son avis. Enfin, le 16 avril 2010, le CEPD a envoyé son projet d'avis à la Commission, pour commentaires. La Commission a fait part de ses observations le 22 avril 2010.

2. Les faits

2.1. Introduction. Le contrôle préalable couvre les aspects de l'EWRS relatifs à la protection des données. L'EWRS est un outil de communication utilisé par la Commission, le Centre européen pour la prévention et le contrôle des maladies (ci-après: l'«**ECDC**»; agence établie en Suède et indépendante de l'Union européenne) et les États membres de l'Union européenne (ainsi que par la Norvège, l'Islande et le Lichtenstein[1]), pour l'échange d'informations «pertinentes au niveau communautaire»[2] concernant la prévention des maladies transmissibles. Ces informations peuvent porter, par exemple, sur la tuberculose, la rougeole, la fièvre jaune, le syndrome respiratoire aigu sévère (SARS) ou la grippe A(H1N1), de même qu'un grand nombre d'autres maladies transmissibles.

[1] Dans un souci de simplicité, la Norvège, l'Islande et le Lichtenstein ne seront pas systématiquement mentionnés dans le présent avis. Seule l'expression «les États membres de l'UE» sera utilisée. Veuillez noter également que l'Organisation mondiale de la santé (ci-après: l'«**OMS**») dispose d'un accès «en lecture seule» à certaines parties des données enregistrées dans l'EWRS, comme cela sera expliqué ultérieurement dans le présent avis.

[2] Pour tous renseignements complémentaires et toutes définitions, prière de consulter les documents mentionnés au paragraphe 2.5 concernant le fondement juridique de l'EWRS.

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

Tandis que chaque État membre dispose de son propre système national de prévention et de contrôle des maladies infectieuses, ce réseau centralisé permet de mener une action transfrontalière et, notamment, de coordonner les mesures prises par les États membres en matière de contrôle des maladies transmissibles. L'EWRS est conçu pour garantir une réaction rapide et efficace de l'Union européenne (ci-après: l'«**UE**») face à des événements — y compris des situations d'urgence — liés à des maladies transmissibles. C'est pourquoi il est fait fréquemment usage de ce système pour notifier des flambées épidémiques, échanger des informations et discuter de la coordination des mesures entre les parties concernées. L'EWRS a été utilisé avec succès dans un certain nombre de situations, comme lors des cas de SARS, de grippe aviaire sous sa forme humaine et d'autres maladies transmissibles graves. Il constitue un instrument important de protection de la santé publique et permet, dès lors, de sauver des vies.

Outre le personnel de la Commission, de l'ECDC et de l'Organisation mondiale de la santé (OMS), plus d'une centaine d'autorités compétentes dans les États membres ont actuellement accès à l'EWRS. L'ECDC assure la gestion de l'EWRS. Ce dernier comporte deux canaux de communication: un canal de messagerie générale, grâce auquel tous les messages téléchargés peuvent être mis à la disposition de tous les utilisateurs simultanément, et un canal de messagerie sélective qui permet de restreindre l'éventail des destinataires. Ce deuxième canal peut être utilisé, entre autres, pour la fonction de «recherche des contacts» telle que décrite ci-après. En raison de la sensibilité des données à caractère personnel, le présent avis se concentre essentiellement sur la recherche des contacts.

2.2. Canal de messagerie générale. Le canal dit de «messagerie générale» est utilisé pour échanger des informations générales présentant un intérêt pour l'ensemble des États membres. Celles-ci portent, en règle générale, sur de nouvelles menaces ou évolutions ainsi que sur les mesures de prévention adoptées par les États membres pour faire face à certaines menaces, comme celle récente liée au virus H1N1. Il est important de noter que les États membres sont tenus de notifier les cas de maladies transmissibles «d'importance communautaire» au moyen de l'EWRS. Ce système favorise donc l'échange d'informations en vue d'améliorer la coordination entre les États membres, l'ECDC et la Commission. Les messages importants peuvent donner lieu à la tenue de réunions de coordination et devenir le point de départ d'une discussion sur une action coordonnée. La décision relative aux mesures de suivi dépend de la gravité et de la particularité de chaque cas.

Les messages transmis via le canal de messagerie générale sont automatiquement mis à la disposition de tous les points de contact des autorités sanitaires dans tous les États membres, ainsi que de la Commission (DG Santé et consommateurs; ci-après: «DG SANCO») de la Commission et de l'ECDC[3].

Outre ces destinataires, l'OMS a aussi accès à l'EWRS. La décision de permettre à l'OMS d'avoir accès à ce système a été prise après la crise du SRAS et l'entrée en vigueur du nouveau règlement sanitaire international (juin 2007). Néanmoins, les points de contact des États membres peuvent décider, lors du téléchargement d'un message général, de ne pas rendre les informations introduites accessibles à l'OMS; dans ce cas, il leur suffit de décocher une case cochée à l'écran. Dans tous les cas, le message est transmis uniquement au Bureau

[3] La notification énumère les noms des autres destinataires des données au sein de la Commission, en plus de la DG SANCO: la DG Énergie et transports (TREN) [devenue DG Mobilité et transports (MOVE)] et les «autres directions générales et services potentiellement concernés». Ces directions générales (DG) n'ont pas accès à l'EWRS. Toutefois, la Commission a expliqué que la DG SANCO *ad hoc* peut, si elle l'estime utile, faire connaître le contenu des messages aux autres DG.

régional pour l'Europe de l'Organisation mondiale de la santé (OMS/Euro), lequel le traite en tant que message confidentiel, conformément au règlement sanitaire international. En effet, la Commission a expliqué au CEPD qu'aucun message n'est envoyé aux différents pays membres de l'OMS.

Tant la Commission que les points de contact dans les États membres disposent d'un accès en lecture et en écriture, c'est-à-dire qu'ils peuvent à la fois télécharger et réviser des messages postés sur l'EWRS. En revanche, l'ECDC et l'OMS n'ont qu'un accès en lecture seule; ils ne peuvent donc pas placer des messages sur l'EWRS.

Le «canal de messagerie générale» n'est pas conçu pour être utilisé aux fins du partage de données à caractère personnel; seuls les noms et coordonnées des points de contact de l'EWRS — autrement dit, des responsables de la santé qui ont accès à l'EWRS — sont joints aux messages qui sont diffusés. Aucune autre donnée à caractère personnel — et, en particulier, aucune donnée concernant la santé — n'est systématiquement échangée via l'EWRS.

La Commission a toutefois précisé qu'il ne peut être exclu que certaines des données introduites dans ce système concernent des individus susceptibles d'être indirectement identifiés. Une telle éventualité peut se produire, par exemple, en cas d'apparition d'une maladie rare dans une petite communauté, lorsque le nom de la communauté est indiqué dans l'EWRS et que l'identité du patient est divulguée par les médias ou connue, d'une quelconque manière, au sein de cette communauté.

Le canal de messagerie générale comporte les champs prédéfinis suivants:

- nom de l'individu et de l'organisation ayant fait part du message;
- type de message (ex.: coordination de mesures);
- syndrome/maladie (avec champ de texte libre pour ajouter, au besoin, une caractéristique supplémentaire);
- agent pathogène (ex.: adénovirus);
- motif de la notification (ex.: A1);
- pays d'occurrence;
- date de survenue/détection;
- corps du message (texte libre);
- pièces jointes (maximum trois pièces jointes, dans des formats de fichier courants, tels que doc (Word), pdf, etc.; des photographies peuvent parfois être annexées);
- visibilité pour l'OMS (l'OMS peut-elle ou non voir le message?);
- RSI OMS (informations complémentaires si le message doit être communiqué à l'OMS en vertu du règlement sanitaire international).

2.3. Messagerie sélective et recherche des contacts Le second canal de communication du système est communément appelé «canal de messagerie sélective». Comme son nom l'indique, il peut être utilisé de façon sélective, c'est-à-dire que les expéditeurs peuvent sélectionner au préalable dans une liste (constituée, au total, de 32 cases à cocher, y compris les points de contact des États membres, la Commission et l'ECDC) les noms des seuls destinataires auxquels ils désirent envoyer leur message. Lorsque des messages sont envoyés au moyen de ce canal, les personnes qui n'ont pas été sélectionnées comme destinataires ne peuvent pas visualiser le contenu des messages; cependant, elles peuvent voir qu'un message a été transmis à un moment précis ainsi que les noms de l'expéditeur et des destinataires.

En ce qui concerne la recherche des contacts, qui constitue la raison première de l'utilisation du canal de messagerie sélective, la Commission et l'ECDC ne sont pas destinataires des messages que les États membres échangent et n'ont donc pas accès au contenu des messages. Cette situation correspond aux prescriptions de la législation en vigueur, laquelle exclut l'accès, par la Commission et l'ECDC, aux messages de recherche des contacts circulant via le canal de messagerie sélective (cf. article 2 bis, paragraphe 2, de la décision concernant l'EWRS, telle que modifiée par la décision 2009/547/CE qui introduit une modification concernant la recherche des contacts).

L'OMS n'a accès ni au «canal de messagerie sélective», ni aux données échangées par le biais du «canal d'échange sélectif». Toutefois, en cas d'urgences sanitaires concernant le monde entier et nécessitant de rechercher des contacts hors de l'Union européenne, des données peuvent être transférées à l'OMS indépendamment de l'EWRS, en vertu de l'article 23, paragraphe 1, du nouveau règlement sanitaire international.

Par rapport au canal de messagerie générale, le canal de messagerie sélective présente une structure plus simple: il ne comporte aucun champ de données prédéfini, mais seulement une ligne de texte libre pour l'objet du message et un corps de message avec texte libre. À cela s'ajoute la liste des destinataires. La fonction permettant de joindre des pièces au message est identique à celle du canal de messagerie générale.

Tout comme le canal de messagerie générale, celui consacré à la messagerie sélective peut aussi être utilisé pour des messages ne contenant — en principe — aucune donnée à caractère personnel: par exemple, lorsqu'un message porte sur des propositions de mesures devant être adoptées à la frontière de deux États membres seulement, ces États peuvent décider de communiquer à l'aide du mécanisme de messagerie sélective, plutôt que d'informer tous les autres États membres.

Outre ces types de messages contenant peu ou pas de données à caractère personnel liées à la santé, il est aussi possible d'avoir recours au canal de messagerie sélective pour la «recherche des contacts», comme précisé ci-après.

2.4. Recherche des contacts. La recherche des contacts est une procédure utilisée pour déterminer et rechercher les personnes (ci-après: «**contacts**») susceptibles d'avoir été en contact avec une personne infectée. Lorsque les contacts ont été retrouvés, ils peuvent être soumis à un examen médical et recevoir des soins. La recherche des contacts contribue, en outre, à servir les intérêts sanitaires du grand public, dans la mesure où elle permet de réduire et de prévenir la propagation de la maladie (les personnes infectées ou susceptibles de l'être peuvent être mises en quarantaine, par exemple). La phase de recherche des contacts nécessite de partager des informations médicales souvent très sensibles, ce qui peut avoir des incidences non seulement sur la vie privée des personnes concernées, mais peut aussi conduire à restreindre considérablement leur liberté individuelle (par des mesures de mise en quarantaine ou de non-admission dans un pays, par exemple).

Le recours à la recherche des contacts ne se justifie pas pour toutes les maladies transmissibles. Pour certaines maladies (telles que la tuberculose, la rougeole ou la fièvre hémorragique, par exemple), cette recherche est largement acceptée dans les milieux scientifiques, où elle est perçue comme une mesure utile et nécessaire pour aider à prévenir ou réduire toute nouvelle dissémination. Pour d'autres maladies au contraire, il est généralement admis que la recherche des contacts se révèle inefficace et ne devrait, dès lors, pas être utilisée comme mesure de santé publique. C'est le cas, par exemple, de la grippe A(H1N1). Eu égard

à une troisième catégorie de maladies — qui inclue celles faisant l'objet d'une stigmatisation, telles que les maladies sexuellement transmissibles —, les avis divergent selon les experts: tandis que certains préconisent de procéder à la recherche des contacts, d'autres laissent entendre que celle-ci pourrait se révéler contre-productive, en ce sens que certaines personnes pourraient être amenées à renoncer à un traitement médical de crainte que celui-ci ne porte atteinte à leur droit à la vie privée.

Dans l'Union européenne, l'ECDC émet des avis non contraignants sur l'opportunité ou non de procéder à la recherche des contacts, lors de la survenance d'une maladie spécifique et/ou d'une flambée épidémique. Avant d'émettre son avis, le Centre prend en considération la nature de la maladie, son pouvoir infectieux (ex.: rougeole), sa gravité (ex.: fièvre hémorragique) et le contexte dans lequel l'exposition à la maladie a eu lieu (ex.: dans un avion ou dans un autre environnement confiné). Les orientations définies par l'ECDC sont généralement respectées dans les États membres. Toutefois, il appartient aux États membres, et non à l'ECDC, de décider en finalité — chacun en fonction de ses propres politiques et procédures — de l'opportunité de recourir à la recherche des contacts sur son territoire, eu égard à une maladie spécifique ou un événement particulier. Cela étant, il arrive parfois que cette mesure soit lancée et coordonnée par l'ECDC au niveau transfrontalier, en coopération avec les autorités des États membres concernés.

Pour les maladies sexuellement transmissibles, la recherche des contacts se limite généralement aux partenaires sexuels, alors que pour des maladies présentant un haut degré de virulence, telles que la fièvre hémorragique à virus Ébola et la tuberculose, il y a lieu de procéder à une recherche approfondie couvrant aussi les simples contacts de la personne affectée. Par «simples contacts», il faut entendre, par exemple, les autres membres du groupe de voyageurs dans le cas d'un voyage organisé ou les voyageurs assis à côté de la personne infectée ou dans une rangée située immédiatement devant ou derrière elle, lors d'un vol commercial.

En 2008 et 2009, 44 événements notifiés par l'intermédiaire de l'EWRS ont nécessité une recherche des contacts et ont donné lieu à 66 messages ayant fait l'objet d'un échange sélectif. Au total, 419 contacts ont été retrouvées (dont 169 en 2009). À la suite d'une flambée d'hépatite à bord d'un navire de croisière, il a fallu retrouver la trace de 201 contacts. Le nombre moyen de contacts localisés par événement est de 9,5. Cependant, la plupart des événements (83 %) n'impliquent que 3 contacts, voire moins. La grande majorité des événements sont liés à la tuberculose. Un cas typique est celui d'un ressortissant d'un État membre voyageant vers un autre État membre et chez qui un diagnostic de maladie transmissible est établi durant ou peu de temps après son séjour dans cet autre État membre.

Les données collectées lors de la procédure de recherche des contacts diffèrent selon les États membres. Il n'existe pas de procédure spécifique pour la collecte de ces données et la nature de celles-ci varie en fonction des différentes maladies et situations pathologiques survenues lors de l'événement nécessitant une recherche des contacts. À titre d'exemple, il peut arriver qu'une personne doive être recherchée car elle est suspectée d'avoir été infectée par le virus de la rage (infection mortelle dans 100 % des cas), à la suite d'un contact étroit avec un chien infecté. Dans ce cas, les informations à obtenir portent sur sa présence à un endroit spécifique et durant une période de temps précise. Dans d'autres cas, il s'agit de retrouver des individus suspectés d'avoir contracté la tuberculose ou une méningite durant un vol long courrier: en pareilles circonstances, les données requises concernent les numéros des sièges dans l'avion. La responsabilité de collecter ces données en fonction de la situation spécifique incombe exclusivement aux autorités sanitaires publiques des différents États membres. La

Commission a expliqué que les compagnies aériennes, les voyagistes et les autres autorités ne collectent pas des données aux fins de la recherche des contacts au niveau national.

Les activités relatives à la recherche des contacts n'ont pas été harmonisées dans le cadre de la législation de l'UE. De ce fait, les États membres doivent échanger les données de recherche des contacts via l'EWRS lorsque ces données sont déjà «disponibles» et lorsqu'il apparaît «nécessaire» de les partager. La législation européenne applicable détermine les catégories de données de recherche des contacts qui peuvent être échangées via l'EWRS. La liste établie inclut, notamment, les données suivantes:

- informations personnelles: nom et prénoms; nationalité; date de naissance; sexe; type et numéro de document d'identité, et autorité de délivrance; domicile actuel; numéros de téléphone; adresse électronique;
- informations relatives au voyage: numéro et date du vol, nom du bateau, plaque d'immatriculation, etc.; numéro de siège, numéro de cabine;
- informations relatives aux contacts: noms des personnes visitées/lieux de séjour; dates du séjour, adresses des lieux de séjour; numéros de téléphone; adresse électronique;
- informations relatives aux personnes accompagnant le voyageur: nom et prénoms; nationalité; type et numéro de document d'identité, et autorité de délivrance; domicile actuel; numéros de téléphone; adresse électronique;
- coordonnées en cas d'urgence: nom de la personne à contacter; domicile; numéros de téléphone; adresse électronique.

Après notification des données au moyen de l'EWRS, chaque État membre met en œuvre, conformément à sa législation nationale et dans le respect de la législation de l'UE, toutes les actions requises pour prendre contact avec les personnes identifiées.

2.5. Base juridique. L'EWRS a été établi conformément à la décision 2000/57/CE de la Commission du 22 décembre 1999 concernant le système d'alerte précoce et de réaction pour la prévention et le contrôle des maladies transmissibles (ci-après: «**décision concernant l'EWRS**»). En tant que mesure d'exécution prise par la Commission, la décision concernant l'EWRS fait suite à la décision n° 2119/98/CE du Parlement européen et du Conseil du 24 septembre 1998 instaurant un réseau de surveillance épidémiologique et de contrôle des maladies transmissibles dans la Communauté (ci-après: «**décision relative à un réseau communautaire**»).

Par la suite, le règlement (CE) n° 851/2004 du Parlement européen et du Conseil du 21 avril 2004 a institué le Centre européen de prévention et de contrôle des maladies (ECDC) en tant qu'entité distincte et indépendante (ci-après: «**règlement instituant l'ECDC**»). Aux termes de l'article 8 dudit règlement, l'ECDC assure la gestion de l'EWRS.

Enfin, la procédure de recherche des contacts a été introduite dans le cadre d'une modification apportée à la décision concernant l'EWRS par la décision 2009/547/CE de la Commission du 10 juillet 2009 (ci-après: «**modification relative à la recherche des contacts**»).

2.6. Les rôles de la Commission, de l'ECDC, de Steria et des points de contact dans les États membres. La notification indique, d'une part, que la Commission assure la fonction de «responsable du traitement» dans le cadre de l'EWRS et, d'autre part, que ce système est «géré par» l'ECDC. Elle fait également mention d'un fournisseur de services, Steria, établi en Suède et soumis à la législation suédoise; Steria est désigné comme étant un «fournisseur d'hébergement externe» ou un «fournisseur de services d'application». La notification ne fournit, en revanche, aucune précision quant au rôle des autorités compétentes dans les États

membres. Au cours de la procédure de contrôle préalable, le CEPD a reçu les explications complémentaires exposées ci-après.

La décision concernant l'EWRS ne précise pas spécifiquement que les fonctions de «responsable du traitement» et de «coresponsable du traitement» sont attribuées à la Commission et aux États membres, pas plus qu'elle ne définit de façon explicite les rôles exacts des responsables du traitement et la participation ou le rôle des sous-traitants éventuels. La Commission estime cependant que l'autorité compétente dans chaque État membre assume une certaine responsabilité quant à l'usage qu'elle fait de l'EWRS et quant aux données qu'elle télécharge au sein de ce système; en ce sens, l'autorité agit en tant que «coresponsable du traitement» pour l'EWRS. Dans le même temps, la Commission, qui gère l'EWRS et garantit la sécurité des données échangées dans ce cadre, devrait aussi être considérée comme un «responsable du traitement» pour ce qui est des activités dont elle assume la responsabilité, y compris le fonctionnement et la sécurité du système.

La Commission a expliqué, en outre, que le rôle de la DG SANCO consiste généralement à gérer la coordination, tandis que celui de l'ECDC porte sur l'évaluation des risques. L'ECDC ne faisant pas partie du «réseau communautaire», il ne dispose d'aucun accès en écriture et ne peut poster aucun message, même s'il gère le système et jouit d'un accès en lecture. La Commission et l'ECDC considèrent le rôle de ce dernier comme celui d'un sous-traitant plutôt que d'un responsable du traitement.

Il n'existe, à l'heure actuelle, aucun contrat entre la Commission et l'ECDC concernant le rôle et les responsabilités de l'ECDC, ni aucun autre document — juridiquement contraignant ou autre — qui fournisse une description de leurs rôles respectifs. Selon la Commission, une révision de la législation actuelle de l'UE concernant les maladies transmissibles sera proposée à moyen terme. Celle-ci offrira peut-être l'occasion de se pencher plus en profondeur sur les questions relatives à la protection des données et, en particulier, sur les rôles et responsabilités des responsables et coresponsables du traitement ainsi que des sous-traitants.

La Commission a expliqué, par ailleurs, que l'ECDC a signé un contrat avec Steria, qui comporte des dispositions relatives à la protection et à la sécurité des données.

2.7. Informations fournies aux personnes concernées. La notification laisse à penser que les personnes concernées sont informées de manière ponctuelle par l'autorité sanitaire nationale qui est impliquée. En particulier, des informations pourraient être communiquées à un «contact» (oralement ou par écrit) lorsque les personnes chargées de la recherche des contacts se mettent en rapport avec celui-ci pour la première fois.

Au cours de la procédure de contrôle préalable, la Commission a précisé que les États membres ont été invités, dans le passé, à expliquer comment ils se conforment à la législation de l'UE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (directive 95/46/CE) et qu'elle entend mettre à nouveau cette question à l'ordre du jour de la prochaine réunion du comité chargé de l'EWRS, aux termes de la décision relative à un réseau communautaire.

Faisant suite à la demande du CEPD, la Commission a confirmé, par ailleurs, qu'elle envisage de fournir des informations concernant les aspects relatifs à la protection des données de l'EWRS sur le site web de la DG SANCO. Ces informations porteront sur le fonctionnement de l'EWRS et sur les garanties en matière de protection des données (ex.: comment les droits d'accès peuvent-ils être exercés et auprès de qui les personnes concernées peuvent-elles introduire une plainte?). Le site proposera aussi des exemples de meilleures pratiques aux utilisateurs du système.

2.8. Droits d'accès (y compris droits de rectification, d'effacement et de verrouillage). À la demande du CEPD concernant les droits d'accès, la Commission a répondu que des informations sur l'exercice de ces droits seront fournies sur le site web de la DG SANCO, comme indiqué ci-dessus (point 2.7). L'institution n'a donné aucun détail supplémentaire.

2.9. Période de conservation. En ce qui concerne les messages transmis au moyen du canal de messagerie sélective, la Commission envisage d'intégrer à l'EWRS une fonction automatisée d'effacement automatique de toutes les données de recherche des contacts permettant d'identifier personnellement les personnes concernées, dans un délai d'un an à compter de l'introduction des informations dans l'EWRS. De l'avis de la Commission, cette période d'un an pour la conservation des informations relatives à la recherche des contacts se justifie par le fait que les périodes d'incubation de certaines maladies transmissibles peuvent être longues (comme pour la tuberculose, par exemple) et qu'il peut se révéler nécessaire, dès lors, de prendre contact avec des personnes jusqu'à douze mois après que celles-ci ont été exposées.

La Commission prévoit de conserver certaines données, rendues anonymes, au-delà de ce délai d'un an, à des fins statistiques, scientifiques ou de recherche. L'effacement de données à caractère personnel après un an de conservation serait automatique et consisterait à supprimer le corps des messages relatifs à la recherche de contacts ainsi que leurs pièces jointes (susceptibles de contenir des données à caractère personnel), tout en conservant l'en-tête du message composée uniquement de champs structurés, tels que le nom de la maladie et le pays d'origine.

Les messages généraux qui ne contiennent pas de données à caractère personnel sont gardés indéfiniment car ils sont utilisés comme ligne de base pour détecter des schémas d'événements inhabituels lors de l'analyse des tendances. En pareils cas, tant le corps du message décrivant l'événement que les champs structurés indiquant le nom de la maladie, le lieu de survenance et d'autres caractéristiques prédéfinies des événements sont conservés.

2.10. Mesures de sécurité. La Commission a fourni les documents suivants au CEPD, pour examen:

- mesures relatives à la sécurité technique de l'infrastructure de l'EWRS en matière de technologie de l'information;
- sécurité de l'application informatique de l'EWRS;
- extraits du contrat de service conclu entre l'ECDC et Steria (eu égard à la protection des données et à la sécurité).

2.11. Précision et proportionnalité des données échangées. La Commission a expliqué qu'il y a lieu de considérer que la précision et la proportionnalité des informations téléchargées dans l'EWRS sont contrôlées par l'ECDC, dans le cadre de ses activités journalières de surveillance des événements susceptibles d'avoir des incidences sur la santé publique dans le monde entier et, plus spécifiquement, dans l'Union européenne.

Pour ce qui est de la formation des utilisateurs, la Commission a souligné le caractère convivial du système. Grâce à l'expérience pluriannuelle des utilisateurs dans les États membres, les nouveaux utilisateurs établis dans les États membres sont assurés d'être formés par leurs autorités nationales sur place. Néanmoins, un module de formation a été intégré au système, afin de permettre à l'utilisateur de se former lui-même ou de trouver des réponses à des questions spécifiques qu'il se pose sur certaines fonctionnalités de l'application. Au sein

de la DG SANCO, une formation est régulièrement assurée aux nouveaux utilisateurs et un module spécifique baptisé «TEST EWRS» a été mis au point et produit à cette fin, afin d'éviter tout risque d'utilisation abusive de l'application informatique «réelle» de l'EWRS durant cette formation. Dans ce modèle, tous les messages utilisés pour former les utilisateurs sont fictifs, de sorte qu'il n'est fait usage d'aucun nom ou événement réel (lesquels sont, par définition, «confidentiels»). Un guide d'utilisation de l'EWRS est disponible dans le module de formation.

3. Aspects juridiques et recommandations

3.1. Applicabilité du règlement. Dans la mesure où il concerne les activités de la Commission et de l'ECDC, le traitement notifié relève du champ d'application du règlement (CE) n° 45/2001 (ci-après: le «**règlement**»), conformément à ses articles 2 et 3. Le traitement des données à caractère personnel par la Commission et l'ECDC est contrôlé par le CEPD (voir article 1er du règlement)[4].

3.2. Raisons d'effectuer un contrôle préalable. Le traitement est soumis à l'article 27, paragraphe 2, point a), du règlement, qui requiert un contrôle préalable du CEPD en ce qui concerne, entre autres, les «traitements de données relatives à la santé».

3.3. Délais de notification et de publication de l'avis du CEPD. L'EWRS était déjà en fonctionnement lorsque le CEPD en a été notifié. L'avis du CEPD devrait, en principe, être demandé et donné avant le début de tout traitement de données à caractère personnel. Néanmoins, étant donné qu'un grand nombre d'opérations de traitement était déjà en place avant que le CEPD ne soit opérationnel en 2004 et que des institutions et organes n'ont pas encore totalement résorbé leur retard de notifications, ces procédures de contrôle préalables sont maintenant menées *a posteriori*.

Conformément à l'article 27, paragraphe 4, du règlement, le présent avis doit être rendu dans un délai de deux mois, sans tenir compte des périodes de suspension autorisées pour la réception des informations complémentaires demandées par le CEPD. La procédure a été suspendue pendant 311 jours. De plus, le CEPD a prolongé de deux mois le délai pour rendre son avis. Le présent avis doit donc être rendu au plus tard le 26 avril 2010.

3.4. Licéité du traitement (article 5, point a), du règlement). Le fondement juridique du traitement est décrit *supra*, au point 2.5. Ainsi, des instruments juridiques spécifiques «adoptés sur la base des traités» autorisent et prévoient les conditions de base pour les traitements notifiés. Le CEPD est également convaincu que le traitement est nécessaire et proportionné eu égard aux intérêts publics de protection de la santé publique dans l'Union européenne, et qu'il est dès lors licite. Cela dit, il conviendra, à court ou moyen terme, de renforcer et de préciser le fondement juridique du traitement, en établissant une répartition plus nette des tâches et en attribuant plus clairement les responsabilités, notamment entre la Commission et l'ECDC, mais aussi entre les points de contact de l'EWRS dans les États membres, comme décrit ci-dessous (point 3.5).

[4] Pour les points de contact nationaux établis dans les différents États membres, la législation applicable est la législation nationale en matière de protection des données, laquelle doit se conformer à la directive 95/46/CE. Le traitement des données à caractère personnel par ces points de contact est contrôlé par les autorités nationales chargées de la protection des données.

3.5. Responsabilité en matière de gestion et d'utilisation de l'EWRS: responsables du traitement et sous-traitants

3.5.1. Nécessité d'indiquer avec précision qui sont les responsables du traitement et les sous-traitants, et de répartir clairement les responsabilités. À titre liminaire, le CEPD souligne que, dans toute situation où des données à caractère personnel sont traitées, il est essentiel de déterminer avec exactitude le responsable du traitement. Cette nécessité a été récemment mise en exergue par le groupe de travail «Article 29» sur la protection des données, dans son avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant» qui a été adopté le 16 février 2010. La raison première pour laquelle l'identification claire et univoque du responsable du traitement se révèle aussi cruciale est qu'elle permet de déterminer la personne chargée de faire respecter les règles en matière de protection des données.

Comme indiqué dans l'avis du groupe de travail susmentionné[5], «lorsqu'on ne sait pas exactement qui doit faire quoi (par exemple, en l'absence de responsable ou en présence d'une multitude de responsables potentiels du traitement), le risque évident est que la directive ait peu, voire pas d'effets et que ses dispositions restent lettre morte». Faire preuve de précision se révèle particulièrement nécessaire dans les situations impliquant de multiples acteurs dans une relation de coopération, ce qui est souvent le cas avec les systèmes d'information de l'UE utilisés à des fins publiques, où la finalité du traitement est définie par la législation de l'UE.

Pour ces motifs, le CEPD exhorte les législateurs, la Commission et l'ECDC à définir, de manière claire et non ambiguë, les tâches et responsabilités de chaque partie impliquée dans le traitement des données, y compris la Commission, l'ECDC et les points de contact dans les États membres. Idéalement, il conviendrait à moyen terme que la législation de l'UE confère à cette définition un caractère contraignant. Toutefois, une solution provisoire (qui permettrait aussi de fournir de plus amples renseignements à long terme, même si de nouvelles dispositions législatives sont adoptées par la suite) pourrait consister à donner des éclaircissements d'une autre manière, plus concrète, par exemple dans le cadre d'un ensemble de lignes directrices en matière de protection des données pour l'EWRS. Techniquement, ces lignes directrices peuvent être formulées, par exemple, sous la forme d'une recommandation de la Commission[6].

Afin que l'importance de ces précisions et de l'adoption de lignes directrices en matière de protection des données pour l'EWRS soit replacée dans son contexte, le CEPD met l'accent sur les risques de violation des droits fondamentaux que toute recherche des contacts menée à grande échelle pourrait comporter à l'avenir. Bien qu'il ait été établi, durant la procédure de contrôle préalable (et l'enquête internationale), que l'étendue des données à caractère personnel échangées au moyen de l'EWRS à des fins de recherche des contacts est relativement limitée, le recours à la procédure de recherche des contacts de l'EWRS ne peut être exclue dans le futur, en cas de pandémie majeure présentant une menace pour la santé publique. Quoique ce recours puisse se révéler nécessaire et proportionné eu égard aux objectifs légitimes de santé publique, il importe de ne pas oublier qu'il risque de porter atteinte aux droits fondamentaux d'un grand nombre de personnes, tant en ce qui concerne la protection des données les concernant et leur vie privée, que leur liberté de mouvement et leur liberté individuelle (par leur mise en quarantaine ou des restrictions de déplacement, par

[5] Voir page 7, paragraphe II.3.

[6] Voir, par exemple, la recommandation de la Commission sur des lignes directrices en matière de protection des données pour le Système d'information sur le marché intérieur (IMI), à l'adresse suivante: http://ec.europa.eu/internal_market/imi-net/docs/recommendation_2009_C2041_fr.pdf

exemple). Au même titre qu'il y a lieu de se préparer sérieusement à faire face à toute menace potentielle pour la santé publique, il convient, pour les raisons susmentionnées, de se préparer en temps opportun à pareilles éventualités, de manière à garantir la protection des droits fondamentaux.

Il conviendra, lors de l'attribution des responsabilités, de veiller à ce que les lignes directrices en matière de protection des données pour l'EWRS prennent en considération les questions suivantes:

- Qui est chargé de garantir la qualité (proportionnalité, précision, etc.) des données?
- Qui peut déterminer les périodes de conservation?
- Qui est habilité à désigner les personnes pouvant avoir accès à la base de données?
- Qui est autorisé à transférer des données à des tiers?
- Qui assure l'information des personnes concernées?
- Qui a la responsabilité d'agir lorsque les personnes concernées demandent l'accès à des données, leur rectification, leur verrouillage ou leur effacement?
- Qui peut décider de prendre une mesure d'exception ou de limitation aux termes de l'article 20 du règlement (et des dispositions correspondantes de la directive 95/46/CE)?
- Qui porte la responsabilité ultime de la sécurité de l'EWRS?
- Qui prend les décisions concernant la conception de l'EWRS (autrement dit, qui peut décider de l'intégration d'une fonction automatique limitant les périodes de conservation à un an?)?

Pour chacun des points énumérés ci-dessus, il y a lieu de déterminer la personne habilitée à prendre la décision ultime, mais aussi celle ayant compétence pour prendre des décisions sur le plan pratique ainsi que les modalités de ces prises de décision. Si diverses parties sont impliquées dans l'un quelconque de ces aspects, il convient d'indiquer avec précision quelles sont les règles de coopération.

Enfin, le CEPD attire l'attention sur le fait qu'il est non seulement dans l'intérêt patent des personnes concernées, mais aussi dans celui des responsables du traitement et des sous-traitants, de répartir les responsabilités de façon transparente et prévisible. En l'absence de précisions suffisantes, la Commission et l'ECDC pourraient, en effet, en cas d'infraction aux règles de protection des données, être considérées comme conjointement et solidairement responsables, quelle que soit la partie fautive.

3.5.2. Réévaluation du rôle de l'ECDC. Au cours de la procédure de contrôle préalable, la Commission et l'ECDC ont laissé entendre que la meilleure définition qui puisse être donnée de leurs rôles respectifs est celle d'une relation «responsable du traitement/sous-traitant»: la Commission détermine les finalités de la collecte des données et les modalités de traitement, tandis que l'ECDC suit simplement les instructions, en tant que sous-traitant.

Le CEPD recommande à la Commission et à l'ECDC de reconsidérer attentivement les deux points suivants:

- leur approche correspond-elle à la situation factuelle d'aujourd'hui?
- ne serait-il pas plus pratique et plus efficace de répartir différemment les rôles à l'avenir?

Durant la procédure de contrôle préalable, la Commission et l'ECDC n'ont pas fourni de preuves suffisantes attestant du fait que le rôle de l'ECDC se limite à celui d'un sous-traitant

qui se contente de suivre les instructions de la Commission. Dans le même temps, plusieurs aspects historiques, factuels et juridiques laissent à penser que l'ECDC agit non pas comme un sous-traitant, mais comme un coresponsable du traitement, en ce sens qu'il partage, dans une mesure non négligeable, la responsabilité des prises de décision avec la Commission, pour ce qui est de la détermination des finalités et des moyens du traitement des données. Tout en se réservant le droit d'adopter, à l'avenir, une autre position si une présentation plus complète des faits devait lui être présentée ultérieurement ou si le cadre juridique ou les circonstances devaient être modifiés d'une quelconque manière, le CEPD estime, en l'état actuel des choses, que le rôle de l'ECDC peut être mieux défini comme un «coresponsable du traitement» conjointement et solidairement responsable de la gestion de l'EWRS.

Pour expliquer son point de vue, le CEPD juge opportun d'établir une distinction entre le rôle de la Commission et celui de l'EWRS dans la gestion du système, d'une part, et en tant qu'utilisateurs du système, d'autre part.

3.5.2.1. L'ECDC et la Commission en tant que gestionnaire(s) de l'EWRS. Il ressort clairement du contexte historique[7] que, si l'EWRS a été initialement mis au point et géré par la Commission, sa gestion a été confiée par la suite à l'ECDC. La base juridique de ce transfert réside dans l'article 8 du règlement de l'ECDC, lequel dispose que «[l]e Centre soutient et aide la Commission, en gérant le système d'alerte précoce et de réaction et en garantissant avec les États membres la capacité de réagir de manière coordonnée». Ainsi, sur le plan pratique et journalier, la gestion de l'application informatique de l'EWRS est clairement de la responsabilité de l'ECDC plutôt que de celle de la Commission[8]. C'est aussi l'ECDC qui héberge l'EWRS en qualité de sous-traitant et non la Commission qui a conclu et négocié le contrat avec Steria. Il résulte des faits présentés au CEPD que la Commission ne joue plus aucun rôle dans la gestion de l'EWRS.

En outre, l'accent mis par le règlement instituant l'ECDC sur l'indépendance de ce Centre laisse planer des doutes quant à la latitude dont la Commission dispose pour donner des instructions à l'ECDC concernant la protection des données. Il ne peut être exclu que l'ECDC — qui dispose de son propre conseil d'administration composé, en majorité, de représentants des États membres[9] — adopte une position différente de la Commission eu égard à certaines garanties importantes en matière de protection des données. Cependant, le règlement instituant l'ECDC utilise les termes «soutien» et «coopération» pour décrire la relation entre la Commission et l'ECDC. Il se peut, en effet, que la Commission et l'ECDC soient amenés actuellement à prendre des décisions conjointes sur des questions plus stratégiques, sans qu'aucune disposition ne précise clairement qui a compétence pour trancher en cas de désaccord et, partant, qui assume la responsabilité des prises de décision, en fin de compte. Cet élément appuie la conclusion du CEPD selon laquelle l'ECDC et la Commission agissent, à l'heure actuelle, en tant que coresponsables du traitement et sont conjointement et solidairement responsables de la gestion de l'EWRS.

[7] Voir, par exemple, le point 8 («Transfert de l'EWRS au CEPCM») du rapport de la Commission au Conseil et au Parlement européen sur le fonctionnement du système d'alerte précoce et de réaction (EWRS) du réseau communautaire de surveillance épidémiologique et de contrôle des maladies transmissibles au cours des années 2006 et 2007 (décision 2000/57/CE).

[8] Il y a lieu de noter, cependant, que les points de contact de l'EWRS sont formellement nommés par les autorités sanitaires compétentes des États membres. Ces nominations officielles sont transmises à la Commission qui demande à l'ECDC d'activer leur accès à l'application informatique. C'est donc l'ECDC qui fournit le code d'accès et le mot de passe aux points de contact de l'EWRS ainsi qu'aux utilisateurs de l'EWRS à la Commission et à l'OMS.

[9] Voir article 14 du règlement instituant l'ECDC.

3.5.2.2. L'ECDC et la Commission en tant qu'utilisateurs de l'EWRS. La Commission jouit d'un accès à la fois «en lecture» et «en écriture» à l'EWRS, tandis que l'ECDC ne dispose que d'un accès «en lecture» et ne peut pas envoyer de messages au moyen de l'EWRS. Lors de la procédure de contrôle préalable, il a été également expliqué au CEPD que, de manière plus vaste et générale, le rôle de l'ECDC se concentre sur l'évaluation des risques, alors que celui de la Commission est axé sur la coopération.

Il appert, dès lors, que la Commission ne se contente pas de porter la casquette de «coresponsable du traitement dans le cadre de la gestion du système», mais elle porte aussi celle de «responsable du traitement dans le cadre de sa propre utilisation du système» — fonction qu'elle assume à titre individuel et séparément de la première —, au même titre, somme toute, que les différents points de contact nationaux sont tous responsables de leur propre utilisation de l'EWRS et constituent donc, chacun séparément, des responsables du traitement. À titre d'exemple, la Commission est responsable de la précision et de la proportionnalité de toutes les données à caractère personnel qu'elle introduit dans le système.

Quoique de manière plus limitée, l'ECDC assume aussi la fonction distincte de «responsable du traitement» lors de l'utilisation de données à caractère personnel qui lui sont accessibles en «lecture seule». En tant que responsable du traitement, le Centre est tenu, par exemple, d'apprécier au cas par cas s'il est autorisé à transférer ces données à des tiers.

3.5.3. Les points de contact des États membres, en tant que responsables du traitement à titre individuel. Eu égard au rôle des points de contact des États membres, le CEPD partage l'analyse de la Commission et de l'ECDC, selon laquelle chaque point de contact assume, à titre individuel, la fonction de «responsable du traitement», en ce sens que chacun est responsable de ses propres opérations de traitement des données lors de l'utilisation de l'EWRS. Compte tenu du nombre de parties différentes concernées et tout en reconnaissant pleinement le rôle que les autorités nationales chargées de la protection des données peuvent jouer pour garantir le respect des règles en la matière par les points de contact nationaux, le CEPD recommande l'adoption de lignes directrices en matière de protection des données pour l'EWRS (voir point 3.5.1), de manière à encourager les meilleures pratiques ainsi qu'une approche cohérente et transparente.

3.5.4. Conclusion. Pour ce qui est des responsabilités de la Commission et de l'ECDC concernant la gestion de l'EWRS, le CEPD estime, en résumé, ne pas avoir reçu d'éléments probants de nature à réfuter la thèse selon laquelle la relation existant actuellement entre la Commission et l'ECDC consiste, dans les faits, à exercer un contrôle conjoint. Il considère, en outre, que le rôle, les tâches et les obligations incombant respectivement à ces deux institutions n'ont pas été clairement répartis entre celles-ci. Par conséquent, le CEPD est d'avis que, jusqu'à ce que leurs rôles respectifs soient précisés, la Commission et l'ECDC sont conjointement et solidairement responsables de la gestion du système[10].

Il convient d'indiquer clairement qui sont les responsables du traitement et qui sont les sous-traitants, en veillant à ce que ces indications correspondent au rôle réel de chacun ainsi qu'au statut juridique des institutions et organes concernés. Il importe ainsi de préciser qui est responsable de quoi et comment les personnes concernées peuvent exercer leurs droits. À court terme, il est recommandé d'adopter un ensemble de lignes directrices en matière de protection des données pour l'EWRS. Le CEPD invite aussi la Commission à œuvrer en

[10] Dans le même temps, chaque point de contact dans les États membres — comme tout autre utilisateur (que ce soit la Commission, l'ECDC ou l'OMS) — est responsable, séparément et individuellement, de l'utilisation qu'il fait du système.

faveur d'une révision du cadre juridique, de manière à garantir une base juridique plus solide et une répartition précise des responsabilités.

3.6. Qualité des données (adéquation, pertinence, proportionnalité, loyauté, licéité, limitation des finalités, exactitude: article 4, paragraphe 1, points a), b), c) et d))

Dans l'ensemble, le CEPD estime que la conception de l'EWRS est satisfaisante eu égard aux finalités de qualité des données et il n'a détecté aucune défaillance systémique nuisant de façon notable à la qualité. Le CEPD approuve, notamment, l'utilisation du canal de messagerie sélective qui permet d'envoyer un message aux seuls destinataires devant être atteints dans le cadre d'une recherche des contacts, de même que la structure claire et simple d'envoi de messages généraux.

Néanmoins, le maintien du respect des règles de qualité requiert une attention et des efforts continus. Chaque utilisateur du système qui dispose d'un accès en écriture (en particulier, les points de contact nationaux, mais aussi la Commission) est individuellement responsable de la qualité des données qu'il introduit dans le système. Afin que les divers utilisateurs puissent se conformer plus aisément aux règles applicables, le CEPD recommande au gestionnaire du système (Commission/ECDC) d'intensifier ses efforts dans les domaines suivants:

3.6.1. Intégration des aspects relatifs à la protection des données dans les formations. Le CEPD estime que certains éléments de la protection des données devraient être intégrés dans toutes les formations dispensées aux utilisateurs du système. Le module de formation à l'EWRS, notamment, devrait inclure des documents sur les aspects relatifs à la protection des données à prendre en compte pour l'utilisation du système. Ces documents pourraient fournir, entre autres, des réponses aux questions suivantes:

- comment veiller à n'introduire dans la base de données que des données pertinentes et non excessives (ex.: en cas de maladie, ne pas introduire des informations obtenues à la suite d'une recherche des contacts, si les résultats positifs de cette recherche ne sont pas suffisamment établis; n'introduire aucune donnée à caractère personnel dans des messages généraux)?
- comment s'assurer que toutes les données incorrectes sont rectifiées (ex.: rectification de noms erronément orthographiés) et que les données introduites sont constamment actualisées?
- comment informer les personnes concernées?
- comment leur donner accès à leurs données à caractère personnel, si elles en font la demande?

Il convient d'attirer l'attention des points de contact nationaux sur l'existence du module de formation et du guide d'utilisation de l'EWRS, de même que sur l'importance de l'intégration de la protection des données dans la formation dispensée aux utilisateurs du système. En outre, le module de formation et le guide lui-même devraient être clairement mis en évidence dans l'interface utilisateur de l'EWRS et devraient, à titre de meilleure pratique, contenir des exemples concrets.

3.6.2. Rectification/effacement de données en ligne. Si l'EWRS n'est pas encore doté de cette fonction, il y a lieu de s'assurer que l'autorité qui télécharge des données dans le système est en mesure d'effacer ou de modifier (rectifier ou mettre à jour) directement en ligne toute donnée incorrecte, non pertinente ou non actualisée. Dans le cadre des bonnes pratiques, il serait aussi utile de prévoir un dispositif permettant, à n'importe quel destinataire,

d'envoyer un message à l'autorité qui a téléchargé des données, en cas de doute quant à l'exactitude ou la mise en jour de certaines données.

3.6.3. Possibilité, à l'avenir, d'un format structuré pour la recherche des contacts. Bien que la modification relative à la recherche des contacts précise quelles sont les données de contact qui peuvent être échangées, il n'existe, à l'heure actuelle, aucun champ de données structurées dans le canal de messagerie sélective de l'EWRS qui convienne pour un échange d'informations plus structurées (et, partant, plus limitées et plus cohérentes). Les données relatives à la recherche des contacts sont transmises comme de simples pièces jointes ou dans des champs de texte libre. Toutefois, le CEPD est d'avis que ce problème ne revêt pas, pour l'heure, une importance notable, étant donné que les procédures de recherche des contacts et les données collectées varient considérablement d'un État membre à un autre, et que le volume de données de contact échangées demeure relativement faible. Cet aspect devra, néanmoins, être réexaminé à l'avenir, si la recherche des contacts se généralise.

3.7. Conservation des données (article 4, paragraphe 1, point e)). En ce qui concerne la conservation des données, le CEPD se félicite de la décision de la Commission de proposer un mécanisme et un délai raisonnable pour l'effacement «automatique» (c'est-à-dire «techniquement intégré») des messages de recherche des contacts. Cette décision se révèle particulièrement importante, compte tenu du problème récurrent qui se pose avec les grandes bases de données informatiques: si l'effacement est conditionné au «classement des dossiers» par les gestionnaires des dossiers et si le système ne prévoit donc pas l'effacement automatique des dossiers inactifs indépendamment de leur classement, certains dossiers peuvent rester ouverts durant une période de temps excessive, sans qu'aucune raison ne le justifie. Le CEPD se réjouit, dès lors, que la Commission envisage d'intégrer un dispositif d'effacement automatique dans le système, de manière à garantir la clôture des dossiers en temps opportun.

À l'heure actuelle, le CEPD n'émet aucune objection à l'égard de la proposition de conserver les données de recherche des contacts durant une année complète. Cependant, il recommande de réévaluer régulièrement, dans le futur, la nécessité de maintenir une période de conservation d'un an, en particulier si la recherche des contacts devait être utilisée, à l'avenir, à une échelle beaucoup plus vaste et pour des maladies dont la période d'incubation est nettement plus courte. En pareille hypothèse, il serait conseillé d'établir une différenciation selon les maladies: à titre d'exemple, les données de recherche des contacts pourraient être effacées après seulement un an dans le cas de la tuberculose, mais dans un délai plus restreint pour les maladies présentant une période d'incubation beaucoup plus courte.

Par ailleurs, le CEPD recommande que, lors de l'intégration du dispositif d'effacement automatique dans le système, une autre fonction soit également intégrée, qui permette aux points de contact des États membres qui le désirent d'effacer, avant l'expiration du délai par défaut d'un an, certaines données de recherche des contacts qu'ils ont téléchargées.

3.8. Destinataires et transferts de données. Le CEPD se félicite de ce que les destinataires soient limités à ceux indiqués à la section 2 du règlement.

En outre, le CEPD rappelle à la Commission et à l'ECDC que lorsque des données sont transférées à l'OMS (en dehors de l'application de l'EWRS) ou si des transferts de données imprévus sont demandés par un tiers, la Commission et l'ECDC ne doivent autoriser ce transfert que pour autant

- que la personne concernée ait donné son consentement non ambigu ou explicite (eu égard aux données sensibles) et éclairé, ou
- que les conditions expressément admises par le règlement soient respectées.

En cas de doute, le CEPD recommande que l'ECDC ou la Commission consulte son délégué à la protection des données (ci-après: «**DPD**») avant d'effectuer le transfert demandé. Il souligne aussi que, conformément à l'article 7, paragraphe 3, du règlement, le responsable du traitement doit informer les destinataires du fait qu'ils peuvent traiter les données à caractère personnel uniquement aux fins qui ont motivé leur transmission.

3.9. Droit d'accès et de rectification (article 13). La Commission et l'ECDC doivent indiquer, de manière précise et efficace, tant aux utilisateurs du système qu'aux personnes concernées, comment ces dernières peuvent effectivement exercer leurs droits d'accès et, en particulier, avec qui elles doivent prendre contact si elles souhaitent avoir accès à leurs données ou les rectifier. Ces informations devraient être reprises dans les lignes directrices en matière de protection des données pour l'EWRS ainsi que sur le site web de la DG SANCO (ou de l'ECDC) consacré à l'EWRS; elles devraient aussi être intégrées dans l'application informatique de l'EWRS, afin que les utilisateurs de cette application puissent en disposer.

Comme le groupe de travail «Article 29» l'a expliqué dans son avis 1/2010 mentionné *supra*[11], «[l]es parties qui agissent conjointement disposent d'une certaine latitude pour attribuer et se répartir les obligations et les responsabilités, pour autant qu'elles en garantissent le respect absolu». Cela suppose dans le cas présent — mais aussi compte tenu du caractère international et de la complexité du système — que, quel que soit le degré de précision avec lequel les règles relatives aux droits d'accès seront établies, il demeurera essentiel de veiller à ce que les personnes concernées puissent prendre contact avec toutes les parties intervenant dans l'échange d'information (à savoir, les points de contacts de l'EWRS concernés, l'ECDC ou la Commission) pour demander l'accès à leurs données et qu'elles puissent recevoir une réponse précise et opportune dès la première demande (plutôt que de devoir tenter à de multiples reprises d'entrer en contact avec diverses parties, jusqu'à ce que l'une d'entre elles accepte, finalement, de prendre cette demande en charge). De manière générale, toutes les parties concernées par un message sélectif contenant des données de recherche des contacts devraient être disposées à répondre à des demandes d'accès. Toutefois, cette règle générale n'exclut pas la possibilité d'une approche «fondée sur l'origine», laissant la possibilité aux parties de coopérer entre elles ou de renvoyer la responsabilité de la décision à la partie ayant introduit le message en premier lieu dans le système. Toutefois, ces mécanismes provisoires ne doivent pas être sources de retards excessifs, de confusion ou de complexité pour la personne concernée.

C'est la raison pour laquelle le CEPD vous encourage aussi à envisager la possibilité d'«intégrer» dans l'architecture du système des moyens d'aider les points de contact nationaux à coopérer, si une demande d'accès ou de rectification est adressée à l'un d'entre eux et s'ils doivent prendre contact avec leurs homologues dans d'autres États membres pour pouvoir répondre favorablement à la demande ou garantir que la correction ou la mise à jour est effectuée dans tout le système. Lorsque cette coopération entre les autorités compétentes se révèle nécessaire pour garantir que l'accès sera accordé ou que les corrections requises seront effectuées, il y a lieu de tirer parti de l'architecture de l'EWRS: les points de contact doivent être capables de communiquer avec chacun d'entre eux au sujet des demandes d'accès ou de rectification, de manière aussi efficace que lorsqu'ils échangent des informations liées à la recherche des contacts. Pour ce faire, il suffit peut-être d'adjoindre au canal de messagerie

[11] Voir page 25 de l'avis 1/2010 du groupe de travail, première phrase de la conclusion préliminaire.

sélective une fonctionnalité supplémentaire pour les demandes d'accès et d'expliquer les modalités d'utilisation dans le module de formation.

3.10. Informations à fournir aux personnes concernées (articles 11 et 12). Les articles 11 et 12 du règlement exigent que certaines informations soient fournies aux personnes concernées afin de garantir la transparence du traitement des données à caractère personnel. Considérant que l'EWRS est utilisé dans trente pays différents, de même que par l'ECDC, la Commission et le point de contact de l'OMS pour l'Europe, il est fondamental de veiller à ce que les personnes concernées reçoivent des informations cohérentes en ce qui concerne le fonctionnement de l'EWRS, la manière dont leurs données sont traitées et les possibilités qui leur sont offertes pour exercer leurs droits.

En tant que gestionnaires du système, l'ECDC et la Commission sont les mieux placés pour jouer un rôle de coordination et pour fournir, sur leur site web[12], des informations aisément disponibles en ligne et au niveau central. Dans la mesure du possible, celles-ci devraient être complétées par des avis sur la protection des données, insérés par les autorités compétentes dans les États membres en fonction des législations nationales applicables. Dans tous ces avis, une attention particulière devrait être accordée à la recherche des contacts.

3.11. Mesures de sécurité (article 22)

3.11.1. Remarques générales. Les documents fournis au CEPD donnent à penser que l'ECDC a pris attentivement en considération la dimension de la sécurité de l'application de l'EWRS. Cependant, les documents portent principalement sur des mesures de sécurité liées à l'infrastructure et à l'application, tandis que celles concernant l'organisation et le personnel impliqué dans la gestion de l'application semblent ne pas être documentées. Le CEPD recommande à l'ECDC de fournir également des documents détaillés au sujet de ces deux dimensions et de regrouper les mesures de sécurité relatives à l'infrastructure, la technologie, le personnel et l'organisation dans une même rubrique définissant la politique de sécurité adoptée pour l'EWRS.

Par ailleurs, le document intitulé *Technical security measures for the IT infrastructure of the EWRS* [Mesures relatives à la sécurité technique de l'infrastructure de l'EWRS en matière de technologie de l'information] n'indique pas toujours clairement quelles sont les mesures appliquées aux serveurs de l'ECDC, à ceux de Steria ou à ceux des deux entités. Ce manque de clarté à cet égard est flagrant dans la partie 3.3 dudit document, relative à la sécurité des serveurs, de même que dans la partie 3.5 relative aux services de colocation. Le CEPD recommande d'établir une nette distinction entre les mesures de sécurité appliquées à Steria et celles appliquées à l'ECDC, et de préciser clairement quelles sont, parmi ces mesures, celles qui sont appliquées aux deux entités.

3.11.2. Accès mobile à l'EWRS. À la lumière des informations fournies, le CEPD reconnaît que, du point de vue des applications, le niveau de sécurité ne devrait pas diminuer en cas d'accès mobile. Toutefois, l'environnement dans lequel cette connexion mobile s'inscrira sera évidemment différent de la connexion de bureau traditionnelle qui est relativement sûre. Il est dès lors nécessaire de sensibiliser les utilisateurs aux conditions dans lesquelles cette connexion aura lieu. Entre autres, certains systèmes d'exploitation mobiles offrent aussi la possibilité de conserver le nom d'utilisateur et le mot de passe, en les proposant automatiquement à chaque connexion. Cette option devrait être supprimée afin d'éviter toute possibilité d'accès direct à l'EWRS, au cas où le dispositif mobile serait volé.

[12] Voir, par exemple, le site http://ec.europa.eu/internal_market/imi-net/data_protection_fr.html qui fournit des informations en matière de protection des données dans le Système d'information du marché intérieur.

3.11.3. Sauvegarde. Lorsque des bandes de sauvegarde sont stockées dans un autre lieu que celui où elles ont été enregistrées, les règles standard de sécurité imposent de les crypter avant leur transport vers le lieu final de stockage. Or, ce point n'est pas mentionné pas dans le document concernant les mesures relatives à la sécurité technique de l'infrastructure de l'EWRS en matière de technologie de l'information. Si des mesures de cryptage des bandes de sauvegarde sont déjà prises, le CEPD recommande de fournir des documents qui en attestent. Dans le cas contraire, il invite l'ECDC à déterminer la solution la plus appropriée pour mettre en œuvre cette bonne pratique.

3.11.4. Incidents de sécurité. Une procédure rigoureuse de gestion des incidents de sécurité (registre, plan de recours à la hiérarchie, etc.) constitue un outil puissant et efficace pour continuer à améliorer le niveau de sécurité de l'application. Hormis le temps de réaction indiqué dans le document lié aux mesures de sécurité technique et trois contre-mesures énumérées dans le document sur la sécurité de l'application informatique de l'EWRS, aucune procédure de gestion des incidents de sécurité n'est présentée de façon détaillée dans les documents fournis. Le CEPD recommande donc à l'ECDC d'élaborer une procédure solide et cohérente de gestion des incidents de sécurité, en l'étayant par des documents.

3.12. Contacts avec les autorités chargées de la protection des données dans les États membres. Il est possible que, dans certains États membres, l'utilisation de l'EWRS par les points de contact — notamment à des fins de recherche des contacts — soit soumise à une forme ou une autre d'exigence de notification ou d'autorisation préalable, en raison du fait qu'ils échangent des données médicales. Les points de contact nationaux devraient, dès lors, examiner s'ils doivent donner notification aux autorités nationales chargées de la protection des données ou solliciter des conseils quant à l'utilisation de l'EWRS. Afin d'attirer l'attention des points de contact sur ce point, le CEPD recommande à la Commission/l'ECDC de les informer de la nécessité éventuelle de consulter les autorités nationales chargées de la protection des données.

3.13. Vérification et maintien du respect des règles. Le contrôle préalable est un exercice ponctuel, conçu pour assister le responsable du traitement dans l'élaboration (ou réélaboration, dans le cas des contrôles préalables *a posteriori*) de son système et dans l'établissement d'un ensemble approprié de garanties en matière de protection des données. Dans tous les cas, il est crucial qu'au terme du contrôle préalable et du suivi, les responsables du traitement maintiennent leur engagement en faveur des bonnes pratiques de protection des données et continuent à veiller au respect des règles en la matière, en procédant à des contrôles réguliers et, le cas échéant, en adaptant leurs pratiques.

Le CEPD encourage la Commission et l'ECDC à garder la protection des données présente à l'esprit, lors des évolutions futures du système. Dans cette optique, il recommande de mettre en place des garanties supplémentaires sur le plan pratique, en appliquant le principe du respect de la vie privée dès la conception et en coopérant, autant que de besoin, avec les parties prenantes, y compris les autorités chargées de la protection des données dans les États membres, afin de veiller à rencontrer leurs préoccupations. Parmi les meilleures pratiques qu'il encourage, le CEPD serait particulièrement favorable à l'exécution de contrôles et à la délivrance de rapports périodiques, en tant qu'outils de vérification du respect des règles et du principe de bonne administration. Le cas échéant, il peut être utile d'attirer l'attention sur les problèmes majeurs relatifs à la protection des données, dans les rapports périodiques requis aux termes de l'article 3 de la décision concernant l'EWRS.

Enfin, le CEPD tient aussi à souligner que l'engagement des parties prenantes (y compris les autorités locales chargées de la protection des données), la formation, la sensibilisation et la transparence constituent à ses yeux des garanties particulièrement importantes pour assurer aux personnes concernées un traitement loyal des données dans l'EWRS.

Conclusion

Le CEPD n'a aucun motif de croire à une violation des dispositions du règlement pour autant que les recommandations figurant à la section 3 soient mises en œuvre, à savoir:

- **Responsables du traitement et sous-traitants**

  Il convient d'indiquer clairement qui sont les responsables du traitement et qui sont les sous-traitants, en veillant à ce que ces indications correspondent au rôle réel de chacun ainsi qu'au statut juridique des institutions et organes concernés. Il importe ainsi de préciser qui est responsable de quoi et comment les personnes concernées peuvent exercer leurs droits. À court terme, il est recommandé d'adopter un ensemble de lignes directrices en matière de protection des données pour l'EWRS. Le CEPD invite aussi la Commission à œuvrer en faveur d'une révision du cadre juridique, de manière à garantir une base juridique plus solide et une répartition précise des responsabilités.

- **Qualité des données et formation**

  La qualité des données doit être évaluée individuellement par les utilisateurs qui téléchargent des données personnelles sur l'EWRS. Afin de faciliter cette évaluation, il convient d'intégrer les aspects de la protection des données dans la formation dispensée aux utilisateurs et de mettre à leur disposition des outils en ligne qui permettent à ces derniers de rectifier toutes données inexactes introduites dans le système. À l'avenir, il pourrait aussi être opportun de proposer un format plus structuré pour l'échange des informations liées à la recherche des contacts.

- **Conservation des données**

  Le CEPD accueille favorablement la proposition de la Commission concernant l'effacement automatique des données de recherche des contacts. Il conviendrait, en outre, de prévoir une fonctionnalité permettant aux utilisateurs d'effacer des données avant la période par défaut d'un an. Une approche plus différenciée, prenant en compte les différentes maladies qui présentent des périodes d'incubation nettement plus courtes, pourrait également se révéler nécessaire à l'avenir.

- **Droits d'accès des personnes concernées**

  Il y a lieu d'établir un mécanisme clair qui permette aux personnes concernées d'exercer leur droit d'accès. Le fait qu'une personne concernée adresse sa demande à une partie autre que celle qui a introduit les informations dans le système ne devrait pas occasionner de retard excessif dans la réponse donnée à sa demande. Le mécanisme devrait être simple et convivial, et il devrait être communiqué de façon efficace, tant aux utilisateurs du système qu'aux personnes concernées.

- **Informations fournies aux personnes concernées.**

Afin de garantir la cohérence et la transparence du système, l'opérateur de l'EWRS devrait fournir, sur son site web, des informations complètes et aisément compréhensibles à l'intention des personnes concernées. À ces informations devrait s'ajouter un avis inséré par les points de contact des États membres, conformément aux législations nationales en matière de protection des données.

- **Sécurité**

Les mesures organisationnelles relatives à la gestion et au personnel doivent être documentées. Comme expliqué dans le présent avis, des éclaircissements et des améliorations complémentaires sont nécessaires eu égard à quelques points spécifiques.

- **Coopération avec les autorités chargées de la protection des données dans les États membres**

Il pourrait être utile que les points de contact nationaux prennent contact avec les autorités chargées de la protection des données dans les États membres.

Fait à Bruxelles, le 26 avril 2010.

(signé)

Peter HUSTINX
Le contrôleur européen de la protection des données