RECOMMANDATIONS

RECOMMANDATION DE LA COMMISSION

du 6 février 2012

relative à des lignes directrices en matière de protection des données concernant le système d'alerte précoce et de réaction (EWRS)

[notifiée sous le numéro C(2012) 568]

(Texte présentant de l'intérêt pour l'EEE)

(2012/73/UE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 292,

après consultation du Contrôleur européen de la protection des données,

considérant ce qui suit:

(1) 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 [1] a établi un réseau de surveillance épidémiologique et de contrôle des maladies transmissibles dans la Communauté et un système d'alerte précoce et de réaction pour la prévention et le contrôle de ces maladies (ci-après le «système d'alerte précoce et de réaction» ou le «système»).

(2) Par sa décision 2000/57/CE du 22 décembre 1999 concernant le système d'alerte précoce et de réaction pour la prévention et le contrôle des maladies transmissibles prévu par la décision n° 2119/98/CE du Parlement européen et du Conseil [2], la Commission a adopté des modalités d'application relatives au système d'alerte précoce et de réaction, lequel vise à mettre en communication structurée et permanente, par les moyens appropriés, la Commission et les autorités sanitaires compétentes des États membres de l'Espace économique européen responsables de la détermination des mesures qui peuvent être nécessaires pour protéger la santé publique et pour prévenir et enrayer la propagation des maladies transmissibles [3].

(3) Le droit à la protection des données à caractère personnel est consacré par la charte des droits fondamentaux de l'Union européenne, notamment son article 8.

(4) Par ailleurs, l'échange d'informations par voie électronique entre les États membres et entre les États membres et la Commission doit intervenir dans le respect des dispositions en matière de protection des données à caractère personnel prévues par 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 [4], ainsi que par le 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 [5].

(5) La décision 2009/547/CE de la Commission du 10 juillet 2009 modifiant la décision 2000/57/CE concernant le système d'alerte précoce et de réaction pour la prévention et le contrôle des maladies transmissibles prévu par la décision n° 2119/98/CE du Parlement européen et du Conseil [6] a instauré des garanties particulières pour l'échange de données à caractère personnel entre les États membres durant les procédures de recherche des contacts aux fins de l'identification des personnes contaminées ou exposées à un risque, en cas de survenance d'un événement lié aux maladies transmissibles susceptible d'avoir une portée européenne.

(6) Le 26 avril 2010, le Contrôleur européen de la protection des données (ci-après le «CEPD») a émis un avis de contrôle préalable [7] dans lequel il a demandé des

[1] JO L 268 du 3.10.1998, p. 1.
[2] JO L 21 du 26.1.2000, p. 32.
[3] Le système d'alerte précoce et de réaction ne peut servir qu'à la notification, par les autorités sanitaires compétentes des États membres, des menaces précises pour la santé publique (les «événements») telles qu'elles sont définies à l'annexe I de la décision 2000/57/CE.
[4] JO L 281 du 23.11.1995, p. 31.
[5] JO L 8 du 12.1.2001, p. 1.
[6] JO L 181 du 14.7.2009, p. 57.
[7] Avis de contrôle préalable du CEPD du 26 avril 2010 sur le système d'alerte précoce et de réaction notifié par la Commission européenne le 18 février 2009 (dossier C 2009-0137). L'avis est publié sur le site du CEPD à l'adresse suivante (http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2010/10-04-26_EWRS_FR.pdf).

précisions sur les responsabilités des différentes personnes intervenant dans le système d'alerte précoce et de réaction, ainsi que des mesures de lutte contre les risques d'atteinte aux droits fondamentaux que présente le traitement des données de recherche des contacts à grande échelle, en cas de pandémie majeure présentant une menace pour la santé publique.

(7) Tenant compte des recommandations formulées par le CEPD dans son avis, la Commission a rédigé un ensemble de lignes directrices en matière de protection des données concernant le système d'alerte précoce et de réaction, lesquelles devraient contribuer à préciser les rôles, les tâches et les obligations des différentes personnes intervenant dans le système et, ainsi, à garantir le respect effectif des dispositions en matière de protection des données précitées et la fourniture d'informations claires et de dispositifs aisément accessibles aux personnes concernées pour qu'elles puissent faire valoir leurs droits,

A ADOPTÉ LA PRÉSENTE RECOMMANDATION:

1. Il est recommandé aux États membres d'appeler l'attention des utilisateurs du système d'alerte précoce et de réaction sur les lignes directrices figurant dans l'annexe de la présente recommandation.

2. Il est recommandé aux autorités nationales compétentes de s'adresser à l'autorité de leur pays chargée de la protection des données pour obtenir des conseils et une assistance quant au meilleur moyen d'appliquer ces lignes directrices conformément à la législation nationale.

3. Il est recommandé aux États membres de fournir à la Commission européenne un retour d'informations sur l'application des lignes directrices figurant en annexe, au plus tard deux ans après l'adoption de la présente recommandation. Ces informations seront communiquées au CEPD et seront prises en compte par la Commission pour évaluer le degré de protection des données assuré par le système d'alerte précoce et de réaction et pour déterminer le contenu et l'opportunité de toute autre mesure, y compris l'adoption éventuelle d'un instrument juridique.

4. Les États membres sont destinataires de la présente recommandation.

Fait à Bruxelles, le 6 février 2012.

Par la Commission

John DALLI

Membre de la Commission

ANNEXE

LIGNES DIRECTRICES EN MATIÈRE DE PROTECTION DES DONNÉES CONCERNANT LE SYSTÈME D'ALERTE PRÉCOCE ET DE RÉACTION (EWRS)

1. INTRODUCTION

Le système d'alerte précoce et de réaction (EWRS) est une application en ligne conçue par la Commission européenne en coopération avec les États membres et visant à mettre en communication structurée et permanente la Commission et les autorités sanitaires compétentes des États membres de l'EEE responsables de la détermination des mesures requises pour protéger la santé publique. Le Centre européen de prévention et de contrôle des maladies (ci-après l'«ECDC»), agence de l'Union européenne, est aussi connecté au système depuis 2005 ([1]).

La coopération entre les autorités sanitaires nationales est essentielle pour renforcer la capacité des États membres de prévenir le risque de propagation de maladies transmissibles dans l'Union européenne et de réagir à temps et de manière coordonnée à des événements provoqués par des maladies transmissibles qui constituent ou sont susceptibles de constituer des menaces pour la santé publique.

Les précédents foyers du syndrome respiratoire aigu sévère (SRAS), de la pandémie de grippe A(H1N1) et d'autres maladies transmissibles attestent clairement la capacité de maladies jusqu'alors inconnues de se propager rapidement, avec pour conséquences une mortalité et une morbidité élevées. Les moyens de transport rapides et les échanges internationaux sont propices à la transmission des maladies transmissibles, qui ne connaissent pas de frontières. Une détection rapide et une communication et une coordination efficaces à l'échelle européenne et internationale sont capitales pour parer de telles éventualités et prévenir toute évolution gravement préjudiciable de la situation.

Le système d'alerte précoce et de réaction est un système centralisé visant à permettre aux États membres d'envoyer des alertes, de partager des informations et de réagir à temps et de manière coordonnée et ferme en cas d'événements susceptibles de constituer une menace pour la santé dans l'Union.

2. PORTÉE ET OBJECTIFS DES LIGNES DIRECTRICES

La gestion et l'utilisation du système peuvent requérir l'échange de données à caractère personnel dans des cas particuliers prévus par les instruments juridiques applicables (voir point 4 sur les fondements juridiques de l'échange d'informations à caractère personnel dans le système).

L'échange d'informations à caractère personnel entre les autorités sanitaires compétentes des États membres doit intervenir dans le respect des dispositions en matière de protection des données à caractère personnel énoncées dans la législation nationale transposant la directive 95/46/CE 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.

Or, les utilisateurs du système n'étant pas des experts en protection des données et ne pouvant pas toujours être suffisamment au fait de la réglementation en la matière, il est recommandé d'élaborer des lignes directrices à leur intention pour leur expliquer en des termes accessibles et aisément compréhensibles le fonctionnement du système sous l'angle de la protection des données. Les lignes directrices visent également à informer les utilisateurs nationaux du système des pratiques exemplaires en matière de protection des données et à les inciter à appliquer de manière cohérente et homogène les principes et la législation applicables en la matière.

En revanche, les présentes lignes directrices ne sont pas destinées à couvrir tous les problèmes liés à la protection des données que le système d'alerte précoce et de réaction est susceptible de poser. Les autorités des États membres chargées de la protection des données (ci-après les «autorités chargées de la protection des données») peuvent fournir des conseils et une assistance supplémentaires. Ainsi, les utilisateurs du système sont vivement encouragés à demander l'avis de l'autorité chargée de la protection des données dont ils relèvent quant au meilleur moyen d'appliquer ces lignes directrices dans le contexte national, de manière à respecter pleinement la réglementation nationale en matière de protection des données. Une liste des autorités chargées de la protection des données (et leurs coordonnées) se trouve à l'adresse suivante:

http://ec.europa.eu/justice/policies/privacy/nationalcomm/index_en.htm

Enfin, il convient de souligner que l'interprétation qui est faite de la législation de l'Union sur la protection des données dans les présentes lignes directrices ne fait pas foi: dans le système institutionnel de l'Union, l'interprétation du droit de l'Union est une compétence exclusive de la Cour de justice.

3. DROIT APPLICABLE ET CONTRÔLE

Le droit applicable est fonction de l'utilisateur du système. Ainsi, le traitement de données à caractère personnel par la Commission et l'ECDC dans le cadre de la gestion et de l'exploitation du système (cadre illustré dans les points ci-après) est régi par le règlement (CE) n° 45/2001.

([1]) L'ECDC aide la Commission à faire fonctionner le système d'alerte précoce et de réaction. Cette tâche lui a été confiée par le règlement (CE) n° 851/2004 du Parlement européen et du Conseil du 21 avril 2004 instituant un Centre européen de prévention et de contrôle des maladies, et notamment son article 8 (JO L 142 du 30.4.2004, p. 1).

Le traitement de données à caractère personnel par les autorités nationales compétentes est, quant à lui, régi par la législation nationale en matière de protection des données transposant la directive 95/46/CE. Il convient d'observer que ladite directive laisse une certaine marge de manœuvre aux États membres pour en transposer les dispositions en droit national. Ainsi, la directive autorise les États membres à prévoir des exceptions ou des dérogations à un certain nombre de ses dispositions dans des cas particuliers. Parallèlement, la législation nationale sur la protection des données à laquelle l'utilisateur du système est assujetti peut énoncer des conditions en matière de protection de données plus strictes ou propres au pays qui ne sont pas prévues par la législation des autres États membres.

Compte tenu de ces particularités, les utilisateurs du système sont invités à examiner les présentes lignes directrices avec l'autorité chargée de la protection des données dont ils relèvent pour s'assurer que toutes les dispositions de la législation nationale applicable sont respectées. Par exemple, le niveau de détail des informations à fournir aux personnes concernées au moment de la collecte des données peut varier grandement d'un État membre à l'autre, tout comme les modalités de traitement de catégories particulières de données à caractère personnel (les données relatives à la santé, par exemple).

L'une des principales caractéristiques du cadre juridique de l'Union applicable à la protection des données, formé par le règlement (CE) n° 45/2001 et la directive 95/46/CE, est qu'il est contrôlé par des organismes publics indépendants de protection des données. Le traitement de données à caractère personnel par les institutions et organes de l'Union est contrôlé par le Contrôleur européen de la protection des données (ci-après le «CEPD») [1], tandis que le traitement de ce type de données par des personnes physiques ou morales, par des organismes publics nationaux ou par des agences ou autres organes des États membres est contrôlé par l'autorité chargée de la protection des données du pays concerné. Les autorités de contrôle sont habilitées, dans tous les États membres, à statuer sur des réclamations déposées par des citoyens en ce qui concerne la protection de leurs droits et libertés à l'égard du traitement de données à caractère personnel. Les utilisateurs du système trouveront davantage d'informations sur le traitement à réserver aux requêtes ou réclamations de personnes concernées au point 9 relatif au droit d'accès aux données à caractère personnel et aux autres droits des personnes concernées.

4. FONDEMENTS JURIDIQUES DE L'ÉCHANGE D'INFORMATIONS À CARACTÈRE PERSONNEL DANS LE SYSTÈME

La décision n° 2119/98/CE a instauré un réseau à l'échelle de l'Union européenne (ci-après le «réseau») pour promouvoir la coopération et la coordination entre les États membres, avec l'aide de la Commission, en vue d'améliorer la prévention et le contrôle, dans l'Union, des maladies transmissibles [2]. Le système d'alerte précoce et de réaction, conçu comme l'un des piliers du réseau, permet l'échange d'informations, la consultation et la coordination à l'échelle européenne en cas d'événements provoqués par des maladies transmissibles susceptibles de menacer la santé publique dans l'Union.

Il convient d'observer que les informations échangées dans le cadre du système ne sont pas toutes à caractère personnel. En fait, en général, aucune donnée relative à la santé ni aucune autre donnée à caractère personnel de personnes physiques identifiées ou identifiables ne sont communiquées dans ce cadre.

Qu'entend-on par «données à caractère personnel»?

Au sens de la directive 95/46/CE et du règlement (CE) n° 45/2001, on entend par données à caractère personnel toute information concernant une personne physique identifiée ou identifiable («personne concernée»); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale [3].

La plupart du temps, les autorités sanitaires compétentes des États membres de l'EEE communiquent au réseau, au moyen du système d'alerte précoce et de réaction, des informations relatives à l'apparition ou à la résurgence de cas de maladies transmissibles – ainsi que des informations sur les mesures de contrôle appliquées – ou des informations relatives aux phénomènes d'épidémie inhabituels ou aux nouvelles maladies transmissibles d'origine inconnue [4], susceptibles de nécessiter une action coordonnée en temps utile des États membres afin de maîtriser le risque de propagation dans l'Union [5]. Sur la base des informations disponibles via le réseau, les États membres se consulteront en liaison avec la Commission en vue de coordonner leur action visant la prévention et le contrôle de ces maladies, y compris en ce qui concerne les mesures nationales qu'ils ont adoptées ou ont l'intention d'adopter [6].

En revanche, dans certains cas, les informations communiquées au moyen du système concernent bien des personnes physiques et peuvent être considérées comme des données à caractère personnel.

D'une part, la gestion et l'exploitation du système requièrent le traitement d'un nombre restreint de données à caractère personnel d'utilisateurs autorisés du système, le traitement des coordonnées des utilisateurs (nom, organisation, adresse électronique, numéro de téléphone, etc.) étant indispensable à la mise en place et au fonctionnement du système. Ces données à caractère personnel sont collectées par les États membres pour être traitées ultérieurement sous la responsabilité de la Commission, traitement destiné exclusivement à permettre une coopération effective aux fins de la gestion du système et du réseau sous-jacent.

[1] http://www.edps.europa.eu/EDPSWEB/edps/.
[2] Les catégories de maladies transmissibles visées par le réseau sont limitées à celles qui sont énumérées à l'annexe de la décision n° 2119/98/CE.
[3] Article 2, point a), de la directive 95/46/CE et article 2, point a), du règlement (CE) n° 45/2001.
[4] Article 4 de la décision n° 2119/98/CE.
[5] Annexe I de la décision 2000/57/CE définissant les «événements» à notifier dans le cadre du système.
[6] Article 6 de la décision n° 2119/98/CE.

D'autre part, et c'est le plus important, la survenance d'un événement lié à des maladies transmissibles susceptible d'avoir une portée européenne peut imposer aux États membres concernés qu'ils prennent de manière concertée des mesures de contrôle particulières, dites de «recherche des contacts», en vue d'identifier les personnes contaminées et les personnes exposées à un risque et de prévenir la transmission de maladies transmissibles graves. Cette collaboration peut requérir l'échange, au moyen du système, de données à caractère personnel, dont des données sensibles relatives à la santé, sur des cas humains confirmés ou suspectés entre les États membres directement concernés par les mesures de recherche des contacts ([1]).

Qu'entend-on par «traitement de données à caractère personnel»?

Aux termes de la directive 95/46/CE et du règlement (CE) n° 45/2001, on entend par «traitement de données à caractère personnel» «toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction» ([2]).

Dans les cas susmentionnés, le traitement de données à caractère personnel dans le cadre du système doit être fondé sur des bases juridiques précises. À cet égard, l'article 7 de la directive 95/46/CE et les dispositions correspondantes de l'article 5 du règlement (CE) n° 45/2001 énoncent les critères légitimant le traitement de données.

En ce qui concerne les coordonnées des utilisateurs du système, leur traitement est fondé:

— sur l'article 5, point b), du règlement (CE) n° 45/2001: «le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement ([3]) est soumis». Le traitement est nécessaire à la gestion et à l'exploitation du système par la Commission, avec le concours de l'ECDC,

— sur l'article 5, point d), du règlement (CE) n° 45/2001: «la personne concernée a indubitablement donné son consentement». Les coordonnées des utilisateurs sont collectées directement auprès des personnes concernées, après que ces dernières ont été mises en mesure d'accepter en connaissance de cause que leurs données à caractère personnel fassent l'objet d'un traitement dans le cadre du système (voir point 8 relatif à la fourniture d'informations aux personnes concernées).

Les critères énoncés à l'article 7, points c), d) et e), de la directive 95/46/CE sont les plus pertinents pour l'échange des données de recherche des contacts de personnes dans le cadre du système (les coordonnées de la personne contaminée, des informations sur le moyen de transport et sur l'itinéraire de voyage et les lieux de séjour du voyageur, des informations sur les personnes auxquelles le voyageur a rendu visite et sur les personnes potentiellement exposées à une source de contamination) ([4]):

— article 7, point c), de la directive 95/46/CE: «le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis». La mise en place d'un système d'alerte précoce et de réaction pour la prévention et le contrôle des maladies transmissibles dans l'Union est prévue par la décision n° 2119/98/CE. Ladite décision impose aux États membres de faire rapport, au moyen du système, de certains événements provoqués par des maladies transmissibles qui constituent ou sont susceptibles de constituer des menaces pour la santé publique ([5]). Doivent aussi être rapportées les mesures prises par les autorités compétentes des États membres concernés pour prévenir et enrayer la propagation de ces maladies, y compris les mesures de recherche des contacts prises pour trouver les personnes contaminées ou celles exposées à un risque de contamination ([6]),

— article 7, point d), de la directive 95/46/CE: «le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée». En principe, les États membres concernés doivent échanger des données à caractère personnel de personnes contaminées et de personnes exposées à un risque imminent de contamination pour administrer à celles-ci les soins ou le traitement appropriés et pour permettre de les rechercher et de les identifier à des fins d'isolement et de quarantaine, l'objectif étant de protéger la santé des personnes concernées et, en bout de chaîne, de l'ensemble des citoyens de l'Union,

— article 7, point e), de la directive 95/46/CE: «le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées». Le système d'alerte précoce et de réaction est un outil destiné à aider les États membres à coordonner leur action visant à la prévention et au contrôle de maladies transmissibles graves dans l'Union. Il est donc conçu pour concourir à l'exécution d'une mission d'intérêt public dont sont investis les États membres afin de protéger la santé publique.

([1]) Les finalités légitimes du traitement de données à caractère personnel dans le cadre du système ont été précisées et étendues aux données de «recherche des contacts» par la décision 2009/547/CE, modifiant la décision 2000/57/CE de la Commission.
([2]) Article 2, point b), de la directive 95/46/CE et article 2, point b), du règlement (CE) n° 45/2001.
([3]) En ce qui concerne la définition du «responsable du traitement», voir point 5 ci-après.
([4]) Une liste indicative des données à caractère personnel qui peuvent être échangées aux fins de la recherche des contacts figure à l'annexe de la décision 2009/547/CE.
([5]) Article 1er et annexe I de la décision 2000/57/CE définissant les «événements» à rapporter dans le cadre du système.
([6]) Article 2 *bis* de la décision 2000/57/CE, introduit par la décision 2009/547/CE.

Les mêmes raisons d'intérêt public peuvent justifier le traitement, par les États membres, de données sensibles relatives à la santé dans le système (comme des informations sur l'événement présentant une menace pour la santé ou des données sur l'état de santé des personnes contaminées et des personnes exposées à un risque de contamination). Bien que le traitement de données relatives à la santé soit interdit en principe par l'article 8, paragraphe 1, de la directive 95/46/CE, le traitement des données de cette catégorie particulière dans le cadre du système fait l'objet de la dérogation prévue à l'article 8, paragraphe 3, de ladite directive, aux termes duquel ledit traitement n'est pas interdit dès lors qu'il est «nécessaire 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 que le traitement de ces données est effectué par un praticien de la santé soumis par le droit national ou par des réglementations arrêtées par les autorités nationales compétentes au secret professionnel, ou par une autre personne également soumise à une obligation de secret équivalente».

Des dérogations supplémentaires à l'interdiction de traitement de données à caractère personnel relatives à la santé peuvent être prévues, pour un motif d'intérêt public important et sous réserve de garanties appropriées, soit par la législation nationale des États membres, soit sur décision des autorités nationales chargées de la protection des données ([1]).

5. QUI FAIT QUOI DANS LE SYSTÈME D'ALERTE PRÉCOCE ET DE RÉACTION? LA QUESTION DE LA CORESPONSABILITÉ

Le système d'alerte précoce et de réaction a été conçu comme un système à utilisateurs multiples reliant, par des moyens techniques appropriés, dont différents outils de communication structurée, les personnes de contact désignées des autorités sanitaires compétentes des États membres de l'EEE (ci-après les «points de contact nationaux»), la Commission et l'ECDC ainsi que, dans une moindre mesure, l'OMS.

Chacun de ces intervenants est un utilisateur distinct du système, mais l'accès aux informations échangées au moyen du système est modulé grâce à l'utilisation de profils d'utilisateur et d'outils de communication «sélectifs», qui offrent les garanties appropriées quant au respect de la réglementation applicable en matière de protection des données.

Ainsi, le système se compose de deux outils de communication principaux. Le premier, la messagerie dite «générale», permet à l'autorité sanitaire compétente d'un État membre donné de communiquer à tous les points de contact nationaux du système, à la Commission, à l'ECDC et à l'OMS des informations sur des événements provoqués par des maladies transmissibles susceptibles d'avoir une portée européenne qui doivent être rapportés en application de la décision n° 2119/98/CE ([2]).

En général, aucune donnée relative à la santé ni aucune autre donnée à caractère personnel de personnes physiques identifiées ou identifiables ne sont communiquées par la messagerie générale. Des garanties particulières ont été introduites dans le système pour prévenir tout traitement illicite des données au moyen de cette messagerie (voir point 7).

Toutefois, en cas d'événements provoqués par des maladies transmissibles susceptibles d'avoir une portée européenne, il se peut que les États membres concernés doivent prendre de manière concertée des mesures particulières de recherche des contacts en vue de trouver les personnes contaminées et les personnes exposées à un risque de contamination, de manière à prévenir la propagation de ces maladies graves.

Les garanties appropriées ont été mises en place pour garantir le respect de la réglementation en matière de protection des données et limiter l'échange de données de recherche des contacts et de données relatives à la santé aux seuls États membres directement concernés par la procédure de recherche des contacts entamée et, ainsi, empêcher les autres États membres du réseau, la Commission et l'ECDC d'avoir accès à ces données ([3]).

C'est la finalité de la messagerie dite «sélective», intégrée dans le système en tant qu'outil de communication exclusif entre les États membres concernés par une mesure de recherche des contacts donnée.

En échangeant des informations à caractère personnel par la messagerie sélective, les autorités compétentes sont «responsables du traitement» de ces données à caractère personnel et sont donc garantes de la licéité de leurs opérations de traitement et du respect des obligations en matière de protection des données qui leur incombent en vertu de la législation nationale transposant la directive 95/46/CE.

([1]) Comme le prévoit l'article 8, paragraphe 4, de la directive 95/46/CE.
([2]) Voir notamment ses articles 4, 5 et 6.
([3]) Article 2 *bis* de la décision 2000/57/CE, introduit par la décision 2009/547/CE.

Qui est le «responsable du traitement»?

Aux termes de la directive 95/46/CE, le «responsable du traitement» est «la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel» ([1]).

En principe, les utilisateurs de la Commission et de l'ECDC n'ont pas accès aux données à caractère personnel échangées au moyen de la messagerie sélective ([2]). Toutefois, pour des raisons d'ordre technique, la Commission est responsable en dernier ressort de la conservation centralisée des données dans le système, en sa qualité d'administratrice et de coordonnatrice du système. À ce titre, elle est également responsable de l'enregistrement, de la conservation et du traitement ultérieur des données à caractère personnel des utilisateurs autorisés du système qui sont nécessaires pour faire fonctionner ce dernier.

Le système d'alerte précoce et de réaction est donc un exemple typique de coresponsabilité, la responsabilité de garantir la protection des données étant répartie, à différents niveaux, entre la Commission et les États membres. En outre, en 2005, la Commission et les États membres, en leur qualité de coresponsables du traitement, ont délégué l'exploitation quotidienne de l'application informatique du système à l'ECDC, une tâche dont ce dernier s'acquitte depuis au nom de la Commission. L'ECDC est par ailleurs chargé de garantir, en sa qualité de «sous-traitant», la confidentialité et la sécurité des opérations de traitement effectuées dans le cadre du système, conformément aux obligations énoncées aux articles 21 et 22 du règlement (CE) n° 45/2001.

Qui est le «sous-traitant» et quelles sont ses obligations?

Aux termes du règlement (CE) n° 45/2001, le «sous-traitant» est «la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement» ([3]).

Le règlement prévoit que, lorsqu'une opération de traitement est effectuée pour son compte, le responsable du traitement choisit un sous-traitant qui apporte des garanties suffisantes au regard des mesures techniques et d'organisation nécessaires pour garantir la sécurité des données. Le responsable du traitement est responsable en dernier ressort de la conformité avec ces mesures. Néanmoins, les obligations énoncées aux articles 21 et 22 du règlement en matière de confidentialité et de sécurité du traitement incombent également au sous-traitant ([4]).

6. PRINCIPES APPLICABLES EN MATIÈRE DE PROTECTION DES DONNÉES

Le traitement de données à caractère personnel dans le cadre du système doit être conforme à un ensemble de principes en matière de protection des données énoncés dans le règlement (CE) n° 45/2001 et dans la directive 95/46/CE.

En leur qualité de responsables du traitement, la Commission et les autorités compétentes des États membres ont la responsabilité de veiller au respect de ces principes à chaque fois qu'elles traitent des données à caractère personnel au moyen du système. Certains grands principes en matière de protection des données sont exposés ci-après. Ils s'appliquent sans préjudice des autres prescriptions en matière de protection des données énoncées dans les instruments juridiques applicables, lesquelles font l'objet de lignes directrices sous différents points du présent document. Ainsi, les utilisateurs du système sont invités à lire attentivement le point 8 relatif à la fourniture d'informations aux personnes concernées, et le point 9, qui traite du droit d'accès et autres droits des personnes concernées.

6.1. *Principes de la licéité du traitement et de la limitation des finalités*

Les responsables du traitement doivent s'assurer que les données à caractère personnel sont traitées loyalement et licitement. Le premier principe veut que la collecte et tout traitement ultérieur de données à caractère personnel soient fondés sur des motifs légitimes prévus par la loi ([5]). Le second principe veut que les données à caractère personnel ne soient collectées que pour des finalités déterminées, explicites et légitimes et ne soient pas traitées ultérieurement de manière incompatible avec ces finalités ([6]).

([1]) Définition figurant à l'article 2, point d), de la directive 95/46/CE.

([2]) Dans des circonstances exceptionnelles, la Commission peut être associée à l'échange de données à caractère personnel au moyen de la messagerie sélective du système lorsque son association est absolument nécessaire pour coordonner les mesures de santé publique prévues par la décision n° 2119/98/CE et ses modalités d'application ou pour permettre que ces mesures soient bien prises à temps. Dans ce cas, la Commission veillera à ce que le traitement soit licite et conforme aux dispositions du règlement (CE) n° 45/2001.

([3]) Définition figurant à l'article 2, point e), du règlement (CE) n° 45/2001.

([4]) Ces principes sont consacrés à l'article 23, paragraphe 1, du règlement (CE) n° 45/2001 sur le traitement de données à caractère personnel pour le compte du responsable du traitement.

([5]) Le principe de la licéité du traitement résulte des dispositions conjointes de l'article 6, paragraphe 1, point a), de l'article 7 et de l'article 8 de la directive 95/46/CE. Voir également dispositions correspondantes du règlement (CE) n° 45/2001.

([6]) Le principe de la limitation des finalités est énoncé à l'article 6, paragraphe 1, point b), de la directive 95/46/CE et dans la disposition correspondante de l'article 4, paragraphe 1, point b), du règlement (CE) n° 45/2001.

6.2. *Principes relatifs à la qualité des données*

Les responsables du traitement doivent veiller à ce que les données à caractère personnel soient adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées. Les données doivent également être exactes et être mises à jour ([1]).

6.3. *Principes relatifs à la conservation des données*

Les responsables du traitement doivent s'assurer que les données à caractère personnel sont 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 ([2]).

6.4. *Principes de la confidentialité et de la sécurité des données*

Les responsables du traitement doivent veiller à ce que toute personne ayant accès à des données à caractère personnel et agissant sous leur autorité ou sous l'autorité du sous-traitant, ainsi que le sous-traitant lui-même, ne traite ces données que sur instruction du responsable du traitement ([3]). En outre, les responsables du traitement sont tenus de prendre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, ainsi que contre toute autre forme de traitement illicite ([4]).

Pour la bonne application des principes susmentionnés dans le cadre de l'utilisation du système, les utilisateurs sont invités à suivre notamment les recommandations ci-après:

pour s'assurer que l'opération de traitement est juridiquement fondée, que les données sont collectées à des fins légitimes et explicites et qu'elles ne sont pas traitées ultérieurement de manière incompatible avec ces finalités, les utilisateurs doivent, à chaque fois qu'ils collectent ou traitent des données à caractère personnel dans le cadre du système:

— vérifier cas par cas si l'application de mesures coordonnées de recherche des contacts – et l'utilisation de la messagerie sélective du système aux fins de l'échange de données de recherche des contacts et d'autres données à caractère personnel – est justifiée compte tenu de la nature de la maladie et des avantages scientifiquement avérés de la recherche des contacts en vue de prévenir ou de freiner la propagation de la maladie, au vu de l'évaluation des risques fournie par les autorités sanitaires des États membres et par les agences scientifiques existantes, à savoir l'ECDC et l'OMS,

— s'abstenir d'utiliser la messagerie générale aux fins de l'échange de données de recherche des contacts et d'autres données à caractère personnel. Il convient notamment qu'ils veillent à ce que ce type de données ne figure ni dans le corps du texte des messages d'ordre général qu'ils envoient, ni dans les pièces jointes de ceux-ci, ni dans tout autre formulaire. L'utilisation de la messagerie générale aux fins de la recherche des contacts serait illégitime et disproportionnée en ce sens qu'elle entraînerait la communication de données à caractère personnel à des destinataires (dont la Commission et l'ECDC) qui ne sont pas concernés par la procédure de recherche des contacts et qui n'ont pas besoin de ces données,

— en cas d'utilisation de la messagerie sélective, ne sélectionner comme destinataires des messages sélectifs contenant des données à caractère personnel que les autorités compétentes des États membres dont la coopération à la procédure de recherche des contacts en question est nécessaire,

les utilisateurs du système devraient être particulièrement vigilants lorsqu'ils échangent, par la messagerie sélective, des données sensibles sur l'état de santé de personnes identifiées ou identifiables, par exemple de personnes contaminées ou exposées à un risque dont les coordonnées ou d'autres informations à caractère personnel sont communiquées de manière concomitante au moyen du système, de sorte que les personnes en question peuvent être identifiées directement ou indirectement. Dans ce cas, toutes les recommandations précitées continuent de s'appliquer. En outre, les utilisateurs du système doivent garder à l'esprit que l'échange de données sensibles n'est autorisé par la directive 95/46/CE que dans un nombre très limité de cas, à savoir ([5]):

— lorsque la personne dont les données sont collectées a donné son consentement explicite à leur traitement [article 8, paragraphe 2, point a), de la directive 95/46/CE]. Toutefois, du fait de la nécessité d'intervenir à temps en cas d'urgence sanitaire, il peut se révéler impossible de fournir aux personnes concernées tous les renseignements nécessaires pour leur permettre de donner leur consentement en connaissance de cause (voir point 8 relatif à la fourniture d'informations aux personnes concernées). En outre, l'éventualité que des données soient communiquées ultérieurement au moyen du système n'est pas connue au moment de la collecte de celles-ci,

([1]) Article 6, paragraphe 1, points c) et d), de la directive 95/46/CE et article 4, paragraphe 1, points c) et d), du règlement (CE) n° 45/2001.
([2]) Article 6, paragraphe 1, point e), de la directive 95/46/CE et article 4, paragraphe 1, point e), du règlement (CE) n° 45/2001.
([3]) Le principe de la confidentialité est énoncé à l'article 16 de la directive 95/46/CE et dans la disposition correspondante de l'article 21 du règlement (CE) n° 45/2001.
([4]) Le principe de la sécurité des données est énoncé à l'article 17 de la directive 95/46/CE et dans la disposition correspondante de l'article 22 du règlement (CE) n° 45/2001.
([5]) La liste complète des dérogations à l'interdiction de traiter certaines catégories particulières de données, notamment les données relatives à la santé, figure à l'article 8, paragraphes 2, 3, 4 et 5, de la directive 95/46/CE.

— à défaut de consentement des personnes concernées, le traitement de données relatives à la santé peut être jugé légitime s'il est nécessaire 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», à condition que ces données soient traitées par un praticien de la santé soumis à l'obligation du secret professionnel, ou par une autre personne également soumise à une obligation équivalente (article 8, paragraphe 3, de la directive 95/46/CE). En d'autres termes, à chaque envoi d'un message sélectif contenant des données sensibles relatives à la santé à des destinataires d'autres États membres, les utilisateurs du système devraient se demander si ces données sont absolument nécessaires aux autorités compétentes des États membres concernés pour pouvoir prendre les mesures particulières requises pour l'une des finalités susmentionnées. Il est également rappelé aux utilisateurs du système que des motifs supplémentaires de traitement de données relatives à la santé peuvent être prévus par la législation de leur pays transposant la directive 95/46/CE ou sur décision de l'autorité chargée de la protection des données dont ils relèvent [1],

pour garantir la qualité des données à caractère personnel qu'ils échangent au moyen du système, les utilisateurs doivent, notamment avant l'envoi d'un message sélectif, se demander:

— si les données à caractère personnel qu'ils souhaitent communiquer sont absolument nécessaires pour permettre une procédure de recherche des contacts efficace. En d'autres termes, l'autorité compétente émettrice du message ne doit fournir à l'autorité de l'autre État membre concerné ou aux autorités des autres États membres concernés que les données à caractère personnel qui sont nécessaires pour identifier sans risque d'erreur des personnes contaminées ou exposées. La liste indicative des données à caractère personnel qui peuvent être échangées aux fins de la recherche des contacts – qui figure à l'annexe de la décision 2009/547/CE – ne vaut pas autorisation générale et inconditionnelle du traitement de ces catégories de données. Par ailleurs, il convient d'être très prudent en ce qui concerne le traitement de données à caractère personnel autres que celles figurant dans ladite annexe, leur communication étant susceptible d'être excessive et déraisonnable. Il vaut mieux déterminer cas par cas si l'inscription de telle ou telle donnée à caractère personnel est absolument nécessaire aux fins de la procédure de recherche des contacts en question.

Traitement ultérieur et conservation des données à caractère personnel en dehors du système d'alerte précoce et de réaction:

Il importe tout particulièrement de faire observer que la législation nationale sur la protection des données transposant la directive 95/46/CE s'applique aussi à la conservation des données à caractère personnel collectées au moyen du système et à leur traitement ultérieur en dehors du système. Par traitement ultérieur, on entend, par exemple, le fait que des données à caractère personnel préalablement centralisées par le système soient conservées par des utilisateurs sur leur propre PC ou dans des bases de données nationales, ou le fait que ces données soient transmises par l'autorité compétente responsable de leur traitement dans le cadre du système à d'autres autorités ou à des tiers. Il est rappelé aux utilisateurs du système ce qui suit:

— la conservation de données et leur traitement ultérieur en dehors du système ne peuvent pas être incompatibles avec les finalités pour lesquelles elles ont été collectées et échangées à l'origine dans le cadre du système,

— ce traitement ultérieur doit avoir une base juridique dans la législation nationale en matière de protection des données et doit être nécessaire, adéquat, pertinent et non excessif par rapport aux finalités pour lesquelles les données ont été collectées dans le cadre du système à l'origine,

— les données doivent être tenues à jour et être supprimées dès lors qu'elles ne sont plus nécessaires aux finalités pour lesquelles elles ont fait l'objet d'un traitement ultérieur,

— lorsque des données sont extraites du système pour être communiquées à des tiers, le responsable du traitement doit en informer les personnes concernées de manière à assurer un traitement loyal des données, sauf si cette information se révèle impossible ou implique des efforts disproportionnés ou si la législation prévoit expressément la communication des données (voir article 11, paragraphe 2, de la directive 95/46/CE). La communication de données peut être une obligation légale dans un seul des États membres concernés; cette obligation n'étant pas censée être bien connue en dehors de ce pays, il convient de veiller à ce que la personne concernée soit informée de la communication des données qui la concernent même lorsque celle-ci est expressément prévue par la législation.

7. UN ENVIRONNEMENT PROPICE À LA PROTECTION DES DONNÉES

Plusieurs fonctions ont déjà été intégrées dans le système pour améliorer le respect des principes relatifs à la protection des données définis au point 6 et inciter les utilisateurs à se poser la question du respect de la protection des données chaque fois qu'ils ont recours au système. Exemples:

— un avertissement s'affiche de manière visible dans l'aperçu des messages du système informant les utilisateurs que la messagerie générale n'est pas destinée à accueillir des données de recherche des contacts ni d'autres données à caractère personnel, son utilisation pouvant entraîner la communication de ces données à des destinataires autres que ceux qui en ont besoin,

— l'accès aux informations échangées au moyen du système est modulé grâce à l'utilisation de profils d'utilisateur et d'outils de communication sélectifs, qui offrent les garanties appropriées quant au respect de la réglementation applicable en matière de protection des données,

[1] Article 8, paragraphe 4, de la directive 95/46/CE.

— la messagerie sélective du système constitue un outil de communication exclusif pour l'échange d'informations à caractère personnel entre les seuls États membres concernés. Le système prévoit par défaut l'exclusion automatique de la Commission et de l'ECDC de la liste des destinataires possibles de messages sélectifs contenant des données à caractère personnel ([1]),

— le système efface automatiquement tous les messages sélectifs contenant des informations à caractère personnel douze mois après la date d'envoi desdits messages (pour en savoir plus, voir point 11 sur la conservation des données),

— une fonction a été intégrée dans le système pour permettre aux utilisateurs de rectifier ou de supprimer directement et à tout moment les messages sélectifs contenant des informations à caractère personnel qui sont erronées, ne sont plus à jour, sont devenues caduques ou ne sont pas conformes à la réglementation en matière de protection des données. Le système informera automatiquement l'autre utilisateur ou les autres utilisateurs du système participant à l'échange d'informations sélectif en question que le message a été supprimé ou que son contenu a été rectifié, pour garantir le respect de la réglementation en matière de protection des données,

— la messagerie sélective contient à présent une fonction permettant aux autorités nationales concernées par un échange d'informations donné de communiquer et de coopérer en cas de demandes d'accès, de rectification, de verrouillage ou de suppression de la part de personnes concernées.

Par ailleurs, il est prévu d'intégrer, à moyenne échéance, le module de formation accessible à partir de l'application du système en vue de fournir aux utilisateurs des explications détaillées sur le fonctionnement du système sous l'angle de la protection des données. L'utilisation des différentes fonctions destinées à améliorer le respect de la réglementation en matière de protection des données sera illustrée par des exemples concrets.

La Commission entend veiller avec les États membres à ce que le principe du respect de la vie privée dès la conception (*privacy by design*) soit appliqué dès la conception de ces fonctions et de tout autre aménagement ultérieur du système d'alerte précoce et de réaction ([2]) et à ce que les principes de nécessité, de proportionnalité, de limitation des finalités et de limitation maximale des données seront pris en compte lorsqu'il s'agira de décider des informations pouvant être échangées au moyen du système, des personnes admises à les échanger et des modalités d'échange.

8. FOURNITURE D'INFORMATIONS AUX PERSONNES CONCERNÉES

L'une des principales prescriptions du cadre juridique de l'Union en matière de protection des données est l'obligation imposée au responsable du traitement des données de fournir aux personnes concernées des informations claires sur les traitements qu'il compte réserver à leurs données à caractère personnel.

Conformément à son rôle de coordonnatrice du système et pour remplir l'obligation précitée ([3]), la Commission a publié une déclaration de confidentialité claire et précise sur sa page web consacrée au système en ce qui concerne les opérations de traitement effectuées sous la responsabilité de la Commission et celles effectuées par les autorités compétentes, notamment dans le cadre des activités de recherche des contacts.

Toutefois, la responsabilité de la fourniture d'informations aux personnes concernées incombe également aux autorités compétentes des États membres en leur qualité de responsables du traitement pour les opérations de traitement qu'elles effectuent dans le cadre du système.

Quelles «informations» les autorités nationales compétentes doivent-elles fournir aux personnes concernées?

En cas de collecte de données directement auprès de la personne concernée, l'article 10 de la directive 95/46/CE dispose que le responsable du traitement ou son représentant doit fournir à la personne auprès de laquelle il collecte des données la concernant, au moment de la collecte, au moins les informations énumérées ci-après, sauf si la personne concernée en est déjà informée:

a) l'identité du responsable du traitement et, le cas échéant, de son représentant;

([1]) Néanmoins, il demeure possible pour les utilisateurs d'utiliser cette messagerie pour communiquer de manière sélective des informations liées à des aspects techniques ne contenant pas de données à caractère personnel. En cas d'utilisation de cette option en lieu et place de l'option par défaut, l'autorité émettrice du message peut sélectionner la Commission et l'ECDC en tant que destinataires. Cette fonction a été ajoutée au système pour tenir compte du rôle institutionnel de la Commission dans la coordination de la gestion des risques et des événements, ainsi que du rôle de l'ECDC dans l'évaluation des risques.

([2]) En vertu de ce principe, les technologies de l'information et des communications (TIC) doivent être conçues et mises au point dans le respect de la réglementation en matière de vie privée et de protection des données dès les premiers stades de leur conception et à tous les stades de leur mise au point.

([3]) L'obligation d'information qui incombe à la Commission est fondée sur les articles 11 et 12 du règlement (CE) n° 45/2001.

b) les finalités du traitement auquel les données sont destinées;

c) toute information supplémentaire telle que:

— les destinataires ou les catégories de destinataires des données,

— le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse,

— l'existence d'un droit d'accès aux données la concernant et de rectification de ces données,

dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

L'article 11 de la directive 95/46/CE énumère les informations que le responsable du traitement doit au moins fournir lorsque les données n'ont pas été collectées auprès de la personne concernée. Ces informations doivent être données au moment de l'enregistrement des données à caractère personnel ou, si une communication de données à des tiers est envisagée, au plus tard lors de la première communication de données ([1]).

Selon les dispositions qui précèdent, au moment de la collecte de données à caractère personnel auprès de personnes physiques (ou, au plus tard, au moment de la première communication des données au moyen du système) aux fins de l'adoption des mesures nécessaires à la protection de la santé publique en ce qui concerne des événements devant être communiqués en application de la décision n° 2119/98/CE et de ses modalités d'exécution, les autorités nationales compétentes devraient faire parvenir directement aux personnes concernées un avis juridique contenant les informations énumérées aux articles 10 et 11 de la directive 95/46/CE. L'avis devrait présenter brièvement le système d'alerte précoce et de réaction et proposer un lien vers les documents utiles et les déclarations de confidentialité figurant sur les sites web nationaux des autorités compétentes, ainsi que vers la page web de la Commission consacrée au système.

Le niveau de détail des informations à indiquer dans l'avis juridique peut varier grandement d'un État membre à l'autre. Dans certains États membres, la législation impose des obligations plus strictes aux responsables du traitement, dont la communication d'informations supplémentaires, notamment sur le droit des personnes concernées d'obtenir réparation, sur la conservation et les périodes de conservation des données, sur les mesures de sécurité des données, etc.

Il est vrai que du fait de la nécessité d'intervenir à temps en cas d'urgence sanitaire, il peut se révéler impossible, lorsque les données n'ont pas été collectées auprès des personnes concernées, de faire parvenir à celles-ci un avis les informant des finalités du traitement de leurs données à caractère personnel. À cet égard, l'article 11, paragraphe 2, de la directive 95/46/CE prévoit que le droit d'information des personnes concernées peut être restreint lorsque «l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ou si la législation prévoit expressément l'enregistrement ou la communication des données. Dans ces cas, les États membres prévoient des garanties appropriées».

Plus généralement, il convient d'observer que la législation nationale en matière de protection des données transposant la directive 95/46/CE peut prévoir des restrictions ou limitations particulières au droit à l'information des personnes concernées ([2]). De telles restrictions ou limitations particulières nationales devraient être clairement précisées dans les avis de confidentialité transmis aux personnes concernées et dans les déclarations de confidentialité publiées sur les sites web nationaux des autorités compétentes.

Il appartient aux autorités nationales compétentes des États membres de décider de la forme de ces informations et du mode de transmission de celles-ci aux personnes concernées. Comme la plupart des autorités compétentes effectueront des opérations de traitement autres que des échanges d'informations dans le cadre du système, le mode de transmission d'informations aux personnes physiques peut être, le cas échéant, le même que celui qu'elles utilisent pour transmettre des informations de même nature relatives à d'autres opérations de traitement dans le cadre de la législation nationale. En outre, il est recommandé que les autorités compétentes mettent à jour ou complètent les avis ou déclarations de confidentialité – pour celles dont le site web en contient déjà – avec une mention particulière sur l'échange de données à caractère personnel dans le cadre du système d'alerte précoce et de réaction.

([1]) Les informations à fournir sont celles énumérées à l'article 10 cité, mais aussi les catégories de données concernées. Cette information n'est évidemment pas nécessaire en cas de collecte auprès de la personne concernée, qui est informée des catégories de données concernées au moment où elles sont collectées.

([2]) L'article 13, paragraphe 1, de la directive 95/46/CE sur les exceptions et limitations est libellé comme suit: «Les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6, paragraphe 1, à l'article 10, à l'article 11, paragraphe 1, et aux articles 12 et 21, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder: a) la sûreté de l'État; b) la défense; c) la sécurité publique; d) la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées; e) un intérêt économique ou financier important d'un État membre ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal; f) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points c), d) et e); g) la protection de la personne concernée ou des droits et libertés d'autrui.»

Pour toutes les raisons susmentionnées, il est de la plus haute importance que les autorités compétentes des États membres consultent l'autorité nationale chargée de la protection des données aux fins de l'élaboration des avis juridiques standard et des déclarations de confidentialité standard conformément aux articles 10 et 11 de la directive 95/46/CE.

9. DROIT D'ACCÈS À DES DONNÉES À CARACTÈRE PERSONNEL ET AUTRES DROITS DES PERSONNES CONCERNÉES

Les prescriptions relatives à la fourniture d'informations aux personnes concernées dans le cadre de la protection des données examinées au point 8 visent à garantir, à terme, la transparence des opérations de traitement des données à caractère personnel. La transparence est également l'objectif sous-jacent des dispositions relatives aux droits d'accès des personnes concernées énoncées dans les instruments juridiques de l'Union en matière de protection des données [1].

Qu'entend-on par «droit d'accès aux données» de la personne concernée?

Les responsables du traitement des données sont tenus de garantir à toute personne concernée le droit d'obtenir, sans délais ni frais excessifs, la confirmation que des données à caractère personnel la concernant sont ou ne sont pas en cours de traitement, ainsi que des informations sur les finalités de ce traitement et sur les destinataires auxquels les données peuvent être communiquées.

Les responsables du traitement doivent également garantir aux personnes concernées le droit d'obtenir la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la législation applicable en matière de protection des données, en raison du caractère incomplet ou inexact des données par exemple.

Enfin, les responsables du traitement doivent notifier aux tiers auxquels les données ont été communiquées toute rectification, tout effacement ou tout verrouillage effectué sur demande légitime de la personne concernée, à moins que cette notification se révèle impossible ou suppose un effort disproportionné.

En leur qualité de responsables du traitement, la Commission et les États membres sont coresponsables de l'octroi de droits d'accès, de rectification, de verrouillage et de suppression des données à caractère personnel traitées dans le cadre du système dans les conditions énoncées ci-après.

Il incombe à la Commission d'octroyer l'accès à des données à caractère personnel des points de contacts nationaux et de traiter les demandes de rectification, de verrouillage et de suppression y afférentes. Pour en savoir plus sur leurs droits en tant que personnes concernées, les points de contact nationaux sont invités à consulter la clause applicable de la déclaration de confidentialité figurant sur la page web de la Commission consacrée au système [2].

Les utilisateurs du système sont également informés que le système contient déjà une fonction leur permettant de modifier directement leurs données à caractère personnel. Toutefois, les champs identifiant le compte d'utilisateur (adresse électronique accréditée de l'utilisateur, type de compte, etc.) ne peuvent être modifiés par les utilisateurs eux-mêmes, et ce pour prévenir le risque que des utilisateurs non autorisés aient accès au système. Par conséquent, toute demande de modification de ces champs doit être adressée au responsable du traitement de la Commission, ainsi qu'il est indiqué dans la déclaration de confidentialité sur la page web de la Commission consacrée au système.

Le traitement des demandes de personnes concernées liées à des données relatives à la recherche des contacts et à la santé et à d'autres données à caractère personnel échangées entre les États membres au moyen du système relève de la responsabilité des autorités compétentes participant à l'échange sélectif d'informations en question. Cette responsabilité est régie par les dispositions applicables de la législation nationale en matière de protection des données transposant la directive 95/46/CE.

Toutefois, il convient d'observer que la législation nationale en matière de protection des données transposant la directive 95/46/CE peut prévoir des restrictions ou limitations particulières aux droits d'accès, de rectification, d'effacement et de verrouillage de données dont jouissent les personnes concernées [3]. De telles restrictions ou limitations devraient être clairement précisées dans les avis de confidentialité transmis aux personnes concernées et dans les déclarations de confidentialité publiées sur les sites web nationaux des autorités compétentes. Les points de contact du système qui souhaitent en savoir plus sur le sujet sont donc invités à s'adresser à l'autorité chargée de la protection des données dont ils relèvent.

La complexité du système, qui permet à de multiples utilisateurs d'intervenir dans des opérations de traitement communes, nécessite une politique claire et simple en matière de droit d'accès des personnes concernées, dans la mesure où ces dernières ne connaissent pas le fonctionnement du système et doivent être mises en mesure d'exercer effectivement leurs droits.

[1] Article 12 de la directive 95/46/CE et articles 13 à 18 du règlement (CE) n° 45/2001.
[2] La déclaration de confidentialité est également accessible à tous les utilisateurs du système depuis la section sécurisée de l'application du système.
[3] Article 13, paragraphe 1, de la directive 95/46/CE.

Il est recommandé que lorsqu'une personne concernée croit savoir que des données à caractère personnel la concernant sont en cours de traitement dans le cadre du système et qu'elle souhaite y avoir accès ou les faire supprimer ou rectifier, elle doit être en mesure de s'adresser aux autorités nationales compétentes avec lesquelles elle est entrée en contact et/ou qui ont collecté ses données en rapport avec un événement particulier présentant un risque pour la santé publique (l'autorité du pays dont ressort la personne concernée et celle du pays de résidence de celle-ci à la date de l'événement, par exemple), ainsi qu'à toute autre autorité participant à l'échange d'informations en question en rapport avec la recherche des contacts.

Aucune autorité compétente participant à l'échange d'informations en question ne devrait refuser l'accès, la rectification ou la suppression des données au motif qu'elle ne les a pas introduites dans le système ou qu'elle estime qu'une autre autorité compétente doit s'en charger. Ainsi, si la personne concernée introduit la demande auprès d'une autorité compétente autre que celle qui a introduit les informations à l'origine au moyen de la messagerie sélective, cette autre autorité doit transférer la demande, à l'aide de la fonction particulière visée au point 7, à l'autorité compétente émettrice du message d'origine, laquelle se prononcera sur la demande.

Le cas échéant, avant de rendre sa décision, l'autorité compétente qui a introduit les informations dans le système peut consulter d'autres autorités compétentes participant à l'échange d'informations ou concernées par la requête de la personne concernée à l'aide de la fonction particulière visée au point 7.

Il convient également d'informer les personnes concernées que si elles ne sont pas satisfaites de la suite réservée à leur demande, elles peuvent s'adresser à une autre autorité compétente participant à l'échange d'informations. En toute hypothèse, les personnes concernées ont le droit de déposer une réclamation auprès de l'autorité chargée de la protection des données du pays de l'une de ces autorités compétentes, à leur convenance. Le cas échéant et si nécessaire, les autorités nationales chargées de la protection des données doivent coopérer entre elles afin de traiter la réclamation (article 28 de la directive 95/46/CE).

Enfin, à la suite d'une recommandation formulée par le CEPD dans son avis, la Commission a introduit une nouvelle fonction dans le système permettant la rectification et la suppression en ligne, aux fins du respect de la protection des données, de messages sélectifs contenant des informations à caractère personnel qui sont erronées, ne sont pas à jour, sont devenues caduques ou ne sont pas conformes à la réglementation en matière de protection des données.

10. SÉCURITÉ DES DONNÉES

L'accès au système est limité aux utilisateurs autorisés de la Commission et de l'ECDC et aux points de contact nationaux du système officiellement désignés. L'accès est réservé aux détenteurs d'un compte d'utilisateur sécurisé et personnalisé protégé par un mot de passe.

Les procédures de traitement des informations à caractère personnel dans le cadre du système sont conformes aux prescriptions des articles 21 et 22 du règlement (CE) n° 45/2001.

11. CONSERVATION DES DONNÉES

Conformément aux dispositions en matière de protection des données énoncées à l'article 4, paragraphe 1, point e), du règlement (CE) n° 45/2001 et à l'article 6, paragraphe 1, point e), de la directive 95/46/CE, le système effacera automatiquement tous les messages sélectifs contenant des informations à caractère personnel douze mois après la date d'envoi desdits messages.

Cette fonction, une garantie qui fait partie intégrante du système, ne dispense toutefois pas les utilisateurs du système – en tant que seuls responsables de leurs propres opérations de traitement à l'aide de la messagerie sélective – de prendre des mesures pour éliminer du système les données à caractère personnel qui deviennent caduques avant l'expiration du délai par défaut, qui est d'un an.

À cette fin, la Commission a introduit une nouvelle fonction dans le système permettant aux utilisateurs de supprimer directement et à tout moment les messages sélectifs contenant des informations à caractère personnel qui ne sont plus nécessaires.

Enfin, il convient de rappeler que les autorités nationales compétentes sont responsables du respect des dispositions en matière de protection des données de la législation nationale transposant la directive 95/46/CE relatives à la conservation des données à caractère personnel. L'effacement automatique des informations à caractère personnel conservées dans le système à l'expiration du délai d'un an n'empêche pas les utilisateurs du système de conserver lesdites informations en dehors du système pour des délais différents (plus longs, par exemple), à condition que cette conservation se fasse conformément aux obligations que leur impose la législation de leur pays applicable en matière de protection des données et que les délais prévus par ladite législation soient compatibles avec les prescriptions de l'article 6, paragraphe 1, point e), de la directive 95/46/CE.

12. COOPÉRATION AVEC LES AUTORITÉS NATIONALES CHARGÉES DE LA PROTECTION DES DONNÉES

Les autorités compétentes sont invitées à consulter l'autorité chargée de la protection des données dans leur pays pour de plus amples informations, a fortiori en cas de problèmes liés à la protection des données qui ne sont pas abordés dans les présentes lignes directrices.

Les autorités compétentes doivent également être conscientes du fait que la législation nationale transposant la directive 95/46/CE peut leur imposer d'informer l'autorité nationale chargée de la protection des données des opérations de traitement de données qu'elles effectuent dans le cadre du système. Dans certains États membres, il se peut même que ladite autorité doive l'autoriser préalablement.