Avis sur la notification d'un contrôle préalable reçue du Centre européen de prévention et de contrôle des maladies (ECDC) le 22 juillet 2009 concernant le système européen de surveillance (TESSy)

Bruxelles, le 3 septembre 2010 (dossier 2009-0474)

1. Procédure

Le 22 juillet 2009, l'ECDC a soumis au Contrôleur européen de la protection des données (**CEPD**) une notification de contrôle préalable «ex post» concernant le système européen de surveillance épidémiologique et de contrôle des maladies transmissibles. Le 17 juillet 2009 (après réception d'une copie préalable de la notification via e-mail le 16 juillet 2009), le CEPD a demandé l'organisation d'une conférence téléphonique afin de clarifier certains faits. Celle-ci a eu lieu le 10 septembre 2009. À cette occasion, l'ECDC s'est engagé à fournir des informations supplémentaires, ce qu'il a fait le 14 octobre 2009 et le 31 mars 2010. Le 26 mai 2010, le CEPD a envoyé à l'ECDC une synthèse de sa compréhension des faits, incluant ses dernières demandes de clarification. L'ECDC a confirmé les faits et a répondu aux questions le 17 juin 2010. Le 18 juin 2010, le CEPD a prolongé d'un mois le délai fixé pour rendre son avis, dont il a transmis le projet à l'ECDC le 14 juillet 2010 pour observations, lesquelles ont été fournies le 21 août 2010.

2. Les faits

2.1. Introduction. Ce contrôle préalable couvre les aspects liés à la protection des données de TESSy. TESSy est un outil de communication utilisé par l'ECDC et les États membres pour l'échange d'informations visant la prévention des «maladies transmissibles» «dont la déclaration est obligatoire au niveau de l'Union européenne», par exemple la tuberculose, la rougeole, le SRAS et la grippe H1N1[1]. Ce système est notamment conçu pour permettre un échange rapide et efficace de données en matière de surveillance épidémiologique entre les États membres de l'UE. À cet égard, il constitue un précieux instrument pour la protection de la santé publique.

2.2. Les données à caractère personnel échangées. Les données à caractère personnel sont introduites dans le système par les points de contact (autorités sanitaires compétentes) dans les États membres. Les utilisateurs du système font principalement usage des champs de données prédéfinis. Les champs de texte libre sont moins fréquemment utilisés (uniquement de manière ponctuelle lorsque les champs prédéfinis ne fournissent pas une information importante). Les champs prédéfinis peuvent inclure, le plus souvent, les types de maladies, les âges des patients, leur sexe, le pays de notification et de naissance et la nationalité. Bon nombre d'autres champs sont utilisés, généralement en fonction du type de maladie ou d'autres circonstances. Par

[1] Pour les définitions et d'autres détails, voir les documents mentionnés dans la section 2.3 relative à la base juridique de TESSy.

exemple, l'orientation sexuelle est indiquée en cas de maladie sexuellement transmissible. Des champs sont également prévus pour des informations telles que «premier test VIH positif», «date du diagnostic», «date du décès» ou «principal mode de transmission présumé».

Deux types de données à caractère personnel sont échangés via TESSy: des données agrégées sans «numéro de dossier» et des «données par cas» avec «numéro de dossier».

Les données agrégées décrivent, par exemple, le nombre total de cas dans un pays donné et la proportion de cas présentant certaines caractéristiques (nombre de cas parmi les 0-5 ans, nombre de cas recensés chez les hommes, etc.). Les données par cas sont un ensemble de données relatives à un seul patient et à un seul épisode d'une maladie spécifique, par exemple une personne atteinte de légionellose. S'il est possible d'être atteint d'une affection à plusieurs reprises au cours d'une vie, chaque épisode infectieux est considéré comme un cas à part entière. Exemples de données par cas: âge, sexe, date du diagnostic, date de la notification, issue (décès ou non).

Le «numéro de dossier» est un numéro attribué par l'entité qui effectue le transfert de données sur TESSy à une série de données liées à un seul cas (par exemple un patient atteint de tuberculose à un moment donné, de même que le suivi). Il permet à celle-ci de mettre facilement à jour les données le cas échéant (notamment pour enregistrer des informations concernant le traitement consécutif ou le rétablissement). Seuls les autorités compétentes des États membres et l'ECDC y ont accès. Il n'est donc pas accessible aux autres destinataires, tels que la Commission ou le bureau régional de l'OMS pour l'Europe.

Dans les deux cas, des «techniques d'anonymisation» sont utilisées pour protéger la vie privée, supprimer les identifiants directs et rendre aussi difficile que possible l'identification indirecte des personnes concernées dans les circonstances qui prévalent. En quelques mots, ces techniques sont conçues pour nettoyer les données à caractère personnel de tout identifiant personnel (et non uniquement les identifiants directs) afin d'éliminer ou de réduire les problèmes de confidentialité tout en conservant les informations utiles.

Dans un premier temps, les identifiants personnels manifestes tels que les numéros d'identification, les noms, les dates de naissance, etc. sont automatiquement supprimés. Toutefois, les techniques employées vont généralement beaucoup plus loin, rendant de plus en plus difficile l'identification même indirecte de personnes.

Cela dit, en dépit de l'utilisation de «techniques d'anonymisation», et bien que l'objectif de TESSy ne soit pas d'échanger des informations personnellement identifiables, l'ECDC a expliqué qu'il était parfois nécessaire de veiller à ce que les données restent relativement «granulaires», plutôt que de se maintenir à un «niveau élevé d'agrégation», afin de s'assurer de leur pertinence pour remplir le rôle de surveillance qui leur est dévolu. C'est la raison pour laquelle, entre autres, des données par cas sont nécessaires. Ce besoin de données granulaires explique également pourquoi, par exemple, l'âge en mois (plutôt qu'en années) est nécessaire pour les maladies vaccinables en-deçà de l'âge de deux ans.

Les États membres ont recours à des «techniques d'anonymisation» avant de transférer les données sur TESSy (à moins que cela ne soit pas nécessaire en raison du faible risque d'identification indirecte des personnes concernées). Cependant, même après utilisation de ces techniques, la base de données contient encore des identifiants personnels susceptibles de donner lieu à l'identification indirecte. Il s'agit habituellement des identifiants suivants:

- le numéro de dossier (voir description supra),
- l'âge,

- le sexe.

Pour certaines maladies, d'autres informations d'identification éventuelles peuvent demeurer, dont, par exemple:

- la date du décès,
- l'âge en mois (uniquement pour les maladies vaccinables et les enfants de moins de deux ans),
- le pays de naissance/d'origine du patient,
- le pays de naissance/d'origine de la mère du patient (concernant les maladies pour lesquelles la transmission mère/enfant est possible),
- le lieu de résidence (dans les régions NUTS).

2.3. Base juridique. TESSy est établi en vertu de 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 («**décision Réseau européen**»). Par la suite, le 21 avril 2004, le règlement (CE) n° 851/2004 du Parlement européen et du Conseil a institué une entité distincte, l'ECDC, un centre européen indépendant de prévention et de contrôle des maladies («**règlement ECDC**»). Son article 5, paragraphe 2, confie à l'ECDC la mission d'assurer le fonctionnement du système TESSy.

2.4. Les rôles de l'ECDC et des points de contact dans les États membres. La notification mentionne l'ECDC en tant que responsable du traitement pour le système. Elle signale également que le fonctionnement du système est assuré par le Centre. Ni la décision Réseau européen ni le règlement ECDC n'attribuent spécifiquement le rôle de «responsables du traitement» ou de «coresponsables du traitement» à l'ECDC et aux autorités des États membres ni ne déterminent le rôle de la Commission à cet égard, pas plus qu'ils ne définissent explicitement les rôles précis des responsables des traitements et l'implication ou le rôle des éventuels sous-traitants.

L'ECDC estime toutefois que chaque autorité nationale doit assumer sa part de responsabilité concernant son propre usage de TESSy ainsi que les données qu'elle transfère dans le système et qu'en ce sens, elle agit en tant que responsable du traitement distinct pour le système. Le Centre lui-même, qui assure le fonctionnement de TESSy et garantit la sécurité des données échangées via le système, est également considéré comme un responsable du traitement dans le cadre des activités dont il est responsable, notamment le fonctionnement et la sécurité du système.

L'ECDC explique par ailleurs qu'il n'est pas membre du «réseau européen». Par conséquent, bien qu'il assure le fonctionnement du système et puisse consulter toutes les données incluses dans le système, il ne peut modifier aucun contenu ni transférer des données dans le système.[2] En ce qui concerne la Commission, l'ECDC est d'avis que cette dernière (DG SANCO) n'agit plus en tant que «responsable du traitement» comme n'importe quel destinataire potentiel ayant accès en lecture seule mentionné dans la section 2.5 ci-dessous (par exemple le bureau régional de l'OMS pour l'Europe ou l'EFSA). La Commission n'a notamment pas la possibilité de modifier du contenu ni de transférer des données dans le système. Contrairement à l'ECDC, il n'incombe pas à la Commission d'assurer le fonctionnement du système.

2.5. Destinataires. Actuellement, plus d'un millier d'utilisateurs répartis au sein des diverses autorités compétentes dans les États membres ont un accès direct à TESSy.

[2] Ceci à l'exception des modifications apportées par les opérateurs de la base de données en réponse aux instructions indirectes des États membres (qui sont inscrits). Il s'agit particulièrement de corrections de données qui ont été erronément enregistrées dans TESSy par un État membre et qui ne peuvent pas être facilement corrigées par celui-ci.

Outre les autorités compétentes des États membres, l'ECDC, la Commission (DG SANCO) et l'OMS disposent également d'un accès direct à TESSy. Dans le cas de l'OMS, les données sont accessibles au bureau régional de l'OMS pour l'Europe, qui les traite de manière confidentielle, conformément au règlement sanitaire international. Par conséquent, l'ECDC a expliqué au CEPD qu'aucune donnée n'était transmise aux États membres de l'OMS à titre individuel[3]. D'autres agences de l'UE (telles que l'EFSA) ainsi que la DG JRC(CCR) peuvent aussi bénéficier d'un accès direct aux données, à condition de traiter les données de manière confidentielle. L'accès à TESSy peut être direct dans pareil cas et accordé dans la même mesure qu'aux autorités compétentes des États membres. Un contrat sera conclu et les destinataires devront signer des accords de confidentialité. La publication des données requiert toujours l'approbation de l'État membre qui a fourni les données.

Les points de contact nationaux ont tous un accès de lecture et d'écriture, c'est-à-dire qu'ils peuvent à la fois introduire des données sur TESSy et visionner celles qui y sont déjà présentes. En revanche, l'ECDC, la Commission (dont la DG JRC), les agences européennes et l'OMS ne disposent que d'un accès en lecture seule. Ils ne peuvent ni introduire ni modifier des données dans le système.

2.6. Transferts de données à des tiers. Les demandes de données transmises par des établissements d'enseignement, des universités, des agences de santé publique de pays tiers, des organisations non gouvernementales et des sociétés commerciales seront traitées par l'ECDC et seront soumises à une «évaluation par les pairs» réalisée par un groupe composé de trois coordinateurs nationaux des activités de surveillance et de deux experts de l'ECDC sur la base de critères que l'ECDC envisage de publier sur son site web. Les données pourront être extraites de TESSy, après signature d'un contrat qui définit les droits et obligations des utilisateurs des données.

2.7. Information des personnes concernées. La notification suggère que – du fait que les données à caractère personnel sont collectées au niveau national et introduites dans le système sans identifiant (hormis le numéro de dossier) – il est impossible pour l'ECDC de fournir aux personnes concernées les informations contenues à l'article 12 du règlement sur la protection des données.

2.8. Droits d'accès (dont rectification, effacement et verrouillage). Pour la même raison, l'ECDC a expliqué qu'il lui était impossible de garantir aux personnes concernées le droit d'accéder à leurs données à caractère personnel, de les rectifier, de les verrouiller, de les effacer ou de s'opposer à leur utilisation.

2.9. Période de conservation. La notification explique qu'étant donné le caractère «anonyme» des données, celles-ci sont conservées indéfiniment. L'ECDC a par ailleurs signalé que l'analyse des données est toujours réalisée rétrospectivement dans les cas où une analyse statistique appropriée (en particulier concernant les corrélations) ne peut être effectuée qu'en utilisant les données les plus granulaires disponibles.

2.10. Mesures de sécurité. L'ECDC a expliqué qu'une politique sur la soumission de données à introduire dans TESSy, l'accès aux données présentes dans le système et leur utilisation a été approuvée par le conseil d'administration du Centre. Cette politique décrit les différents droits

[3] Hormis les données relatives au VIH/SIDA qui sont collectées dans le cadre d'une activité de «surveillance conjointe» de l'ECDC et du bureau régional de l'OMS pour l'Europe, qui sont mises à la disposition de tous les participants du réseau VIH/SIDA de la région Europe de l'OMS.

d'accès et responsabilités de l'utilisateur. Selon le document fourni par le CEDP, elle sera confirmée et signée par tous les États membres et la Commission «après l'évaluation de 2010».

Lorsqu'il lui a été demandé de fournir une copie de la politique de sécurité applicable au TESSy, l'ECDC a souligné que le responsable de la sécurité des TIC récemment recruté par l'ECDC élaborera une politique de sécurité spécifique au système ainsi qu'une politique générale de sécurité de l'information.

3. Aspects juridiques et recommandations

3.1. Applicabilité du règlement. Le traitement notifié, dans la mesure où il concerne les activités de la Commission et de l'ECDC, relève du champ d'application du règlement (CE) n° 45/2001 (**«le règlement»**) en vertu de ses articles 2 et 3. Le traitement des données à caractère personnel effectué par la Commission et l'ECDC est supervisé par le CEPD (voir le règlement, article premier).[4]

Il importe de noter que dans certaines situations, les données statistiques peuvent constituer des données à caractère personnel même si diverses «techniques d'anonymisation» sont utilisées, conformément à des normes communément appliquées dans le domaine des statistiques. Comme l'a indiqué précédemment le CEPD dans plusieurs avis consultatifs[5], *«si, du point de vue de la protection des données, les "données rendues anonymes" sont des données conservées sous une forme qui ne permet plus l'identification de la personne concernée (…), il s'agit par contre, du point de vue statistique, de données qui ne permettent pas l'identification directe. Il découle de cette définition qu'une identification indirecte n'empêche pas que les données concernées puissent être considérées, d'un point de vue statistique, comme des données anonymes*».

La première étape consiste généralement à supprimer les identifiants personnels directs et évidents tels que les numéros d'identification, les noms, les dates de naissance, etc. Diverses autres «techniques d'anonymisation» sont également fréquemment utilisées pour rendre de plus en plus difficile l'identification de personnes.

En dépit de ces efforts, il est à noter que les données continueront d'être considérées comme des «données à caractère personnel» et seront par conséquent couvertes par le règlement aussi longtemps que des personnes pourront être indirectement identifiées. Le simple fait que «des techniques d'anonymisation ont été utilisées» ne signifie pas que les données sont considérées comme étant «rendues anonymes» au sens du considérant 8 du règlement.[6]

Il importe également de noter le statut des données «codées». Dans pareil cas, les données à caractère personnel *«correspondent à un code, la clé permettant d'établir une correspondance entre ce code et des identifiants courants de ces personnes physiques (comme le nom, la date de naissance, l'adresse) étant conservée séparément»*[7]. Cela peut signifier que dans certaines

[4] Dans le cas d'un point de contact national dans un État membre, le droit applicable est la législation nationale en matière de protection des données, qui doit être en conformité avec la directive 95/46/CE. Le traitement des données à caractère personnel effectué par ces points de contact est supervisé par leurs autorités nationales chargées de la protection des données.

[5] Voir l'avis du Contrôleur européen de la protection des données sur une proposition de règlement du Parlement européen et du Conseil relatif aux statistiques communautaires de la santé publique et de la santé et de la sécurité au travail, JO 2007/C - 295/01, et l'avis du 20 mai 2008 sur la proposition de règlement relatif aux statistiques européennes (COM(2007) 625 final), JO 2008/C - 308/01.

[6] Considérant 8, voir notamment: *«Afin de déterminer si une personne est identifiable, il convient de prendre en considération l'ensemble des moyens susceptibles d'être raisonnablement utilisés par le responsable du traitement ou par toute autre personne pour identifier ladite personne»*.

[7] Voir, par exemple, les pages 18 et suivantes de l'avis 4/2007 sur le concept des données à caractère personnel rendu par le groupe de travail «Article 29» sur la protection des données.

situations faisant appel aux «codes», le lien entre une donnée statistique ou une série de données statistiques et une personne concernée spécifique peut être rétabli. C'est parfois voulu de manière spécifique, notamment dans une situation d'essais cliniques afin de permettre le traitement des patients en cas de répercussions nocives sur la santé ou dans des études longitudinales. À d'autres moments, la capacité d'identifier des personnes n'est pas nécessaire au-delà de la période initiale qui peut s'avérer nécessaire pour vérifier l'exactitude des statistiques. Dans tous les cas, des mesures techniques, organisationnelles et juridiques adéquates devraient être prises pour s'assurer que les codes ne seront utilisés que lorsqu'ils sont destinés spécifiquement à des fins claires et bien définies. Aussi longtemps que les clés ne seront pas détruites et que la possibilité de rétablir un lien direct avec la personne demeure, les données à caractère personnel codées ne peuvent pas être considérées comme totalement «anonymes».

Les données codées sont pertinentes à deux égards concernant TESSy. Premièrement, s'agissant des données par cas, grâce au numéro de dossier, l'autorité sanitaire compétente qui a initialement introduit les données dans le système sera capable d'identifier les personnes concernées. Deuxièmement, même dans les cas où les données introduites dans le système sont des données agrégées plutôt que des données par cas, il pourrait toutefois être possible, au moins dans certains cas, que les autorités compétentes des États membres ou d'autres entités (par exemple les entités ayant collecté les données) détiennent toujours les clés qui leur permettraient d'identifier les personnes concernées.

3.2. Motifs de réalisation d'un contrôle préalable. Le traitement relève de l'article 27, paragraphe 2, point a), du règlement, qui requiert un contrôle préalable, entre autres, du «traitement des données liées à la santé» par le CEPD.

3.3. Délais de notification et d'émission de l'avis du CEPD. TESSy était déjà en service avant qu'une notification ne soit transmise au CEPD; par conséquent, cette procédure de contrôle préalable est à présent mise en œuvre et les recommandations du CEPD doivent être appliquées ex post. Pour le futur, le CEPD attire l'attention de l'ECDC sur le fait que l'avis du CEPD devrait généralement être sollicité et reçu avant le début de tout traitement de données à caractère personnel.

En vertu de l'article 27, paragraphe 4, du règlement, le présent avis doit être rendu dans un délai de deux mois, déduction faite de toute période de suspension accordée pour la réception d'informations supplémentaires requises par le CEPD. La procédure a été suspendue pendant 261 jours (plus le mois d'août en 2009 et 2010). En outre, le CEPD a prolongé d'un mois le délai qui lui était imparti pour rendre un avis, qu'il doit par conséquent rendre au plus tard le 6 septembre 2010.

3.4. Licéité du traitement (article 5, point a), du règlement). Le traitement repose sur la base juridique décrite dans la section 2.3 susmentionnée. Ainsi, des instruments juridiques spécifiques «adoptés sur la base des traités» définissent les conditions fondamentales applicables aux traitements notifiés. Le CEPD apprécie également le fait que le traitement de données à caractère personnel, après utilisation de «techniques d'anonymisation» adéquates (proportionnées au risque d'atteinte à la vie privée) et moyennant d'autres garanties prévues dans l'avis, soit nécessaire et proportionné aux fins de la protection de la santé publique dans l'Union européenne. Par conséquent, le traitement est licite. Il est toutefois recommandé de renforcer et de clarifier la base juridique du traitement en établissant une distribution plus claire des tâches et en répartissant plus précisément les responsabilités, en particulier entre l'ECDC, la Commission et les points de contact nationaux, comme indiqué au point 3.5 ci-dessous.

3.5. Répartition des responsabilités pour le traitement et utilisation de TESSy. À titre préliminaire, le CEPD fait remarquer que dans toute situation impliquant le traitement de données à caractère personnel, il est vital d'identifier correctement le responsable du traitement. Le groupe de travail «Article 29» sur la protection des données a récemment souligné cette nécessité dans son avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant», adopté le 16 février 2010. L'identification claire et non équivoque du responsable du traitement est cruciale essentiellement parce qu'elle détermine qui sera chargé de veiller au respect des règles en matière de protection des données.

Comme mentionné dans l'avis du groupe de travail[8], «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.» La clarté est particulièrement nécessaire dans les situations impliquant plusieurs acteurs dans une relation coopérative. C'est souvent le cas avec les systèmes d'information européens utilisés à des fins publiques lorsque l'objet du traitement est défini dans le droit de l'UE.

Pour ces raisons, le CEPD invite instamment la Commission et l'ECDC à définir, de manière claire et non équivoque, les tâches et responsabilités de chaque partie associée au traitement de données, y compris l'ECDC, la Commission et les points de contact nationaux. Idéalement, et à moyen terme, ce processus devrait devenir juridiquement contraignant, via la législation européenne. En guise de solution provisoire (mais aussi pour fournir de plus amples détails à long terme même si de nouvelles législations sont adoptées), des éclaircissements peuvent être apportés sous une autre forme, plus concrète. Cela peut prendre plusieurs formes. Une possibilité serait d'adopter une série de lignes directrices sur la protection des données introduites dans TESSy. En théorie, cela peut prendre, par exemple, la forme d'une recommandation de la Commission.[9]

Lors de la répartition des responsabilités dans les lignes directrices en matière de protection des données introduites dans TESSy, il convient notamment de répondre aux questions suivantes:

- Qui est responsable de la qualité (proportionnalité, exactitude, etc.) des données?
- Qui peut fixer les périodes de conservation des données?
- Qui détermine les personnes qui ont accès à la base de données?
- Qui est autorisé à transférer des données à des tiers?
- Qui informe les personnes concernées?
- Qui est chargé de prendre les mesures nécessaires lorsque des personnes concernées souhaitent exercer leur droit d'accès, de rectification, de verrouillage ou d'effacement?
- Qui est responsable en dernier ressort de la sécurité de TESSy?
- Qui prend les décisions relatives à la conception de TESSy?

Pour chacun de ces points, il convient de déterminer qui est autorisé à prendre la décision finale, mais également qui prend les décisions sur le plan pratique et de quelle manière. Si plusieurs parties sont impliquées à l'un ou l'autre niveau, les règles régissant leur coopération et leurs responsabilités doivent être définies précisément.

[8] Voir la page 7, section II.3, de l'avis.
[9] Voir, par exemple, sur les lignes directrices en matière de protection des données pour le Système d'information sur le marché intérieur (IMI) élaborées par la Commission, le site http://ec.europa.eu/internal_market/imi-net/docs/recommendation_2009_C2041_fr.pdf.

Les responsables du traitement et les sous-traitants doivent être clairement indiqués d'une façon qui corresponde au rôle effectif et au statut légal des institutions et organes concernés.

Enfin, au vu du nombre de parties impliquées, et tout en reconnaissant pleinement le rôle que les autorités nationales chargées de la protection des données peuvent jouer lorsqu'il s'agit de garantir le respect par les points de contact nationaux, les lignes directrices peuvent également être utilisées pour promouvoir les bonnes pratiques et une approche cohérente et transparente.

3.6. Qualité des données (caractère adéquat, pertinence, proportionnalité, loyauté, licéité, limitation de l'objet, exactitude: articles 4, paragraphe 1, points a), b), c) et d))

Globalement, le CEPD est satisfait de la conception de TESSy du point de vue de la qualité des données et n'a détecté aucune faille systémique donnant lieu à des inquiétudes majeures au sujet de la qualité.

Cependant, garantir la conformité à long terme requiert des efforts et une attention constants. Chaque utilisateur du système habilité à modifier ou introduire du contenu est individuellement responsable de la qualité des données qu'il transfère sur le système. Afin de faciliter le respect des règles par les différents utilisateurs, le CEPD recommande d'intégrer les aspects liés à la protection des données dans toute formation dispensée aux utilisateurs du système. Des informations sur les points suivants peuvent notamment être incluses:

- comment s'assurer que seules des données pertinentes et non excessives sont incluses dans la base de données (p. ex. utilisation de «techniques d'anonymisation» appropriées),
- comment s'assurer que les données erronées sont rectifiées et que les données incluses sont actualisées,
- comment informer les personnes concernées, et
- comment leur garantir l'accès à leurs données à caractère personnel lorsqu'elles en font la demande.

Il convient d'attirer l'attention des points de contact nationaux sur l'existence des lignes directrices relatives à TESSy et l'importance d'intégrer les questions liées à la protection des données dans le programme des formations dispensées aux utilisateurs du système. Les lignes directrices devraient également être affichées clairement sur l'interface utilisateur du système et contenir, à titre de bonne pratique, des exemples concrets.

De manière spécifique, le CEPD rappelle en outre à l'ECDC que les champs de texte libre devraient être édités avec circonspection afin de s'assurer que le niveau de risque pour la protection des données soit similairement faible dans le reste de la base de données – par exemple, tous les identifiants personnels directs devraient être supprimés et aucune donnée extrême ne devrait figurer parmi les données.

3.7. Conservation des données (article 4, paragraphe 1, point e)). Concernant la conservation des données, le CEPD recommande de supprimer les numéros de dossier dès qu'ils ne sont plus nécessaires pour mettre à jour la base de données. La suppression devrait être automatisée et ses critères correctement définis. Elle devrait être garantie par son intégration à part entière dans l'architecture du système.

Hormis en ce qui concerne le numéro de dossier, le CEPD n'est, à ce stade, et dans l'attente de nouvelles évolutions techniques et autres, en rien opposé à la conservation des données pour une durée indéterminée, à condition que des «techniques d'anonymisation» adéquates soient utilisées et que l'accès à ces données demeure limité et sécurisé, tel qu'indiqué dans le présent avis.

3.8. Destinataires et transferts de données. Le CEPD approuve le fait que les destinataires et destinataires potentiels des données soient limités à ceux identifiés dans la section 2 et que des garanties soient proposées pour s'assurer que les données dévoilées demeurent confidentielles et ne seront utilisées qu'à de véritables fins de recherches. Il salue en particulier la mise en place d'une procédure spécifique (**«évaluation par les pairs»**) visant à traiter les demandes d'accès selon des critères transparents (à déterminer et publier ultérieurement), ainsi que le fait que les données ne seront disponibles qu'après signature d'un contrat définissant les droits et obligations des utilisateurs des données TESSy.

Ces garanties sont en effet nécessaires pour éviter toute atteinte à la vie privée des personnes concernées tant que les données divulguées à des tiers ne sont pas totalement «anonymes».

Le CEPD souligne que la justification de la nécessité du transfert en vertu de l'article 8, point b), du règlement doit être appropriée. Il importe avant tout (i) que les transferts soient réalisés à de véritables fins de recherches, (ii) que les chercheurs garantissent la confidentialité des données, et (iii) qu'ils ne les utilisent qu'à des fins de recherches spécifiques. Dans le cadre de la procédure d'évaluation par les pairs, il convient entre autres que le tiers demandeur indique un objet de recherche, que les pairs évaluateurs vérifient l'identité et les références du chercheur (p. ex. s'il est ou non membre d'un institut de recherche), qu'ils lui fassent signer un contrat de confidentialité et que la sécurité des données soit garantie (p. ex. en fournissant une connexion internet sécurisée ou en cryptant les données fournies sur un support média). Il est également à noter que les chercheurs seront soumis à la législation nationale de leur pays pour tout traitement réalisé à la suite du transfert, et notamment aux dispositions relatives à la supervision, à la responsabilité et au respect des règles applicables. Par ailleurs, le CEPD recommande que le contrat même inclue des sanctions appropriées pour les cas de violation des engagements pris par les chercheurs ou les organisations.

En outre, le CEPD rappelle à la Commission et à l'ECDC que tout transfert de données international, en particulier à l'OMS, ne peut avoir lieu qu'aux conditions visées à l'article 9 du règlement. Il recommande au Centre d'examiner, avec l'assistance de ses délégués à la protection des données (**«DPD»**), les possibilités de se conformer à cet article dans le cadre du suivi du présent avis sur la notification d'un contrôle préalable.

3.9. Droit d'accès et de rectification (article 13). En dépit de la nature statistique des données (et même si la possibilité d'identification n'est qu'indirecte), l'ECDC devrait réévaluer s'il peut exister des situations dans lesquelles une personne concernée pourrait souhaiter accéder à ses données personnelles, les rectifier ou s'opposer à leur utilisation. Des mesures adéquates devraient être mises en place pour remédier à de telles situations, même si les demandes d'accès devraient être rares. Ce point devrait être établi dans les lignes directrices relatives à la protection des données introduites dans TESSy – sur le site de la DG SANCO (ou de l'ECDC) consacré au système – lesquelles devraient être mises à la disposition des utilisateurs de l'application, sur l'application même. Il conviendrait à tout le moins d'indiquer à chaque organisation utilisatrice de TESSy une personne de contact chargée de traiter les demandes d'accès. Lors de la répartition des responsabilités entre les différentes parties, tel qu'il a été suggéré dans la section 3.5, il importe de déterminer qui est le mieux placé pour accorder l'accès aux personnes concernées (p. ex. l'organisation qui a introduit les données pourrait être la seule capable de lier les données statistiques à la personne concernée grâce à une clé dont elle serait la détentrice).

3.10. Information de la personne concernée (articles 11 et 12). Les articles 11 et 12 du règlement requièrent que certaines informations soient fournies aux personnes concernées afin de garantir la transparence du traitement des données à caractère personnel. Étant donné que TESSy

est utilisé dans trente pays ainsi qu'à l'ECDC, à la Commission et au point de contact de l'OMS pour l'Europe, il est essentiel que des informations cohérentes soient mises à la disposition des personnes concernées au sujet du fonctionnement du système, du traitement de leurs données et des modalités d'exercice de leurs droits.

En tant qu'opérateur du système, l'ECDC est le mieux placé pour jouer un rôle de coordinateur et fournir des informations en ligne centralisées et facilement accessibles sur son site web[10]. À cela devrait s'ajouter, si possible, la diffusion d'une déclaration de protection des données par les autorités compétentes des États membres conformément à leur législation applicable.

3.11. Mesures de sécurité (article 22). Le CEPD recommande à l'ECDC d'élaborer une politique de sécurité spécifique pour le système TESSy. Cette politique devrait reposer sur une évaluation précise des risques permettant de détecter les menaces potentielles pour le système et son volet communication. Cette initiative devrait permettre d'identifier des mesures de sécurité strictes à appliquer ou de valider celles déjà en place. Cette politique de sécurité devrait compléter la politique des droits d'accès déjà définie et, entre autres, clarifier l'utilisation des fichiers d'enregistrement de l'application, la sécurité de la communication entre les utilisateurs et le système, ainsi que la gestion des droits d'accès de l'administrateur du système.

La procédure de modification/correction de données par l'ECDC à la demande d'un utilisateur dans un État membre (opération considérée comme étant une exception pour les actions que les utilisateurs dans les États membres peuvent difficilement ou ne peuvent pas du tout exécuter avec les outils actuellement disponibles) doit également être documentée en détail. Le CEPD estime judicieux que cette procédure soit prévue, même si l'ECDC devrait s'évertuer à ne pas du tout y recourir dans le futur et fournir aux États membres les instruments nécessaires pour qu'ils puissent effectuer eux-mêmes les corrections dans tous les cas.

Au vu du nombre important d'utilisateurs (près d'un millier) et des interactions entre l'ECDC et les États membres pour la gestion de ces utilisateurs, le CEPD recommande à l'ECDC d'envisager la possibilité d'assortir les comptes d'utilisateur d'une durée de vie limitée. L'entité chargée de désigner l'utilisateur devrait avoir la possibilité de demander la création d'un compte utilisateur et de fixer un délai au terme duquel le compte serait automatiquement clos. En cas de maintien de comptes à durée de vie illimitée, l'ECDC devrait demander régulièrement à cette entité de réexaminer et de confirmer la liste des utilisateurs (dans ses observations sur le projet d'avis du CEPD, l'ECDC a confirmé qu'il suivait actuellement cette dernière approche, à savoir que les comptes sont ouverts pour une période indéfinie, mais que des réexamens réguliers sont prévus).

Conclusion

Le CEPD estime qu'il n'y a pas lieu de conclure à une quelconque violation des dispositions du règlement dans la mesure où les recommandations formulées dans la section 3 sont appliquées, à savoir:

- **Répartition des responsabilités**

  Les responsables du traitement et les sous-traitants doivent être clairement indiqués d'une façon qui corresponde au rôle effectif et au statut légal des organisations concernées. Il convient de mentionner qui est responsable de quoi ainsi que la façon dont les personnes

[10] Voir, par exemple, le site http://ec.europa.eu/internal_market/imi-net/data_protection_fr.html, qui fournit des informations sur les aspects du système d'information sur le marché intérieur relatifs à la protection des données.

concernées peuvent exercer leurs droits. Il est recommandé d'adopter une série de lignes directrices en matière de protection des données introduites dans TESSy.

- **Qualité des données et formation**

La qualité des données devrait être évaluée par chaque utilisateur introduisant des données à caractère personnel dans le système. Pour faciliter cette évaluation, les aspects liés à la protection des données devraient être intégrés dans la formation dispensée aux utilisateurs.

- **Conservation des données**

Les numéros de dossier devraient être automatiquement supprimés lorsque leur utilisation n'est plus nécessaire.

- **Transferts à des tiers**

Des garanties supplémentaires devraient être appliquées, comme indiqué dans la section 3.8, à propos des transferts à des tiers et à l'OMS.

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

En dépit de la nature statistique des données, l'ECDC devrait réévaluer s'il peut exister des situations dans lesquelles une personne concernée pourrait souhaiter accéder à ses données personnelles, les rectifier ou s'opposer à leur utilisation. Des mesures adéquates devraient être mises en place pour remédier à de telles situations, même si les demandes d'accès devraient être rares. Il conviendrait à tout le moins d'indiquer à chaque organisation utilisatrice de TESSy une personne de contact chargée de traiter les demandes d'accès.

- **Information des personnes concernées**

Afin de garantir la cohérence et la transparence, l'opérateur de TESSy devrait fournir des informations complètes et accessibles aux personnes concernées sur son site web. À cela devrait s'ajouter la diffusion d'une déclaration de protection des données par les points de contact des États membres conformément à leur législation nationale applicable en matière de protection des données.

- **Sécurité**

Une politique de sécurité spécifique devrait être adoptée dans les plus brefs délais afin de contribuer à garantir la sécurité de TESSy ainsi que de vérifier et de démontrer que le système est correctement administré. Si les trois mois impartis pour assurer le suivi des recommandations du présent avis s'avèrent insuffisants pour garantir l'adoption et l'application de cette politique, l'ECDC rend compte, dans un délai de trois mois, des mesures prises à ce stade et transmet au CEPD une feuille de route claire (incluant des points d'action et un calendrier d'exécution) pour adoption finale et mise en œuvre.

Fait à Bruxelles, le 3 septembre 2010

(**signé**)

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données