Avis sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Commission européenne concernant le système d'échange électronique d'informations sur la sécurité sociale («EESSI»)

Bruxelles, le 28 juillet 2011 (dossier 2011-0016)

1. Procédure

Le 5 janvier 2011, le contrôleur européen de la protection des données («CEPD») a reçu du délégué à la protection des données («DPD») de la Commission européenne une notification de contrôle préalable concernant le système d'échange électronique d'informations sur la sécurité sociale («EESSI»). Il s'agit d'un véritable contrôle préalable; selon le calendrier de mise en œuvre, il est prévu que l'EESSI devienne opérationnel vers la fin de la période de transition, d'ici le 1er mai 2012.

1.1. Conditions requises pour la mise en place de l'EESSI

L'EESSI est un système d'information créé par l'UE; il peut être considéré comme un système informatique à grande échelle étant donné qu'il concerne des échanges transfrontières, entre l'ensemble des États membres, d'un certain nombre de données à caractère personnel sur la sécurité sociale. L'EESSI a donc un impact considérable sur la protection de la vie privée et des données des personnes concernées.

L'impact de ce système informatique à grande échelle sur la protection de la vie privée et des données des personnes concernées doit être évalué à deux niveaux: 1) au niveau législatif, conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001, le CEPD devrait être consulté sur la proposition de législation européenne introduisant un tel système informatique à grande échelle; 2) au niveau de la mise en œuvre, les autorités nationales chargées de la protection des données dans les États membres, et le CEPD en ce qui concerne le traitement effectué par les institutions et organes de l'UE, doivent être dûment informés du traitement des données.

Le CEPD note avec satisfaction que, conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001, il a été consulté par la Commission sur le projet de règlement d'application portant sur la coordination des systèmes de sécurité sociale qui constitue la base juridique prévoyant les détails techniques de l'EESSI. Dans son avis consultatif[1], le CEPD a formulé des observations sur le cadre juridique prévu pour la mise en œuvre de l'EESSI et a mis en évidence des points précis qui nécessitent de prendre des mesures appropriées du point de vue de la protection des données. Certains de ces points ont été examinés dans le règlement d'application lui-même, la version finale intégrant certaines des suggestions soumises par le CEPD; d'autres nécessitent que les États membres et/ou la Commission prennent des mesures d'application supplémentaires.

[1] Avis du CEPD concernant la proposition de règlement du Parlement européen et du Conseil fixant les modalités d'application du règlement (CE) n° 883/2004 portant sur la coordination des systèmes de sécurité sociale (COM (2006)16 final), adopté le 6 mars 2007.

Le CEPD souligne donc que le présent avis sur la notification d'un contrôle préalable, qui analyse les mesures d'application qui lui ont été notifiées par la Commission, devrait être considéré conjointement avec l'avis consultatif.

1.2. Délai pour rendre l'avis

Conformément à l'article 27, paragraphe 4, du règlement (CE) n° 45/2001, le présent avis doit être rendu dans un délai de deux mois. Ce délai peut être suspendu jusqu'à ce que le CEPD ait obtenu les informations complémentaires demandées. Le CEPD a demandé des informations complémentaires à la Commission le 17 février 2011. Ces dernières ont été communiquées respectivement le 3 mars 2011 et le 6 avril 2011. L'avis devait initialement être rendu le 26 avril 2011 (le 24 avril étant un dimanche et le 25 avril le lundi de Pâques). Cependant, compte tenu de la complexité du dossier, le délai a été prolongé d'un mois, conformément à l'article 27, paragraphe 4, du règlement. Des questions complémentaires ont été posées le 28 avril et ont été examinées lors d'une réunion entre le personnel du CEPD et le personnel de la DG EMPL qui s'est tenue le 22 juin 2011. Des précisions ont été apportées par écrit le 6 juillet 2011 et le 8 juillet 2011. Le CEPD a envoyé son projet d'avis le 18 juillet 2011 afin que le DPD puisse soumettre ses observations; elles ont été reçues le 27 juillet 2011. La procédure a été suspendue pendant 182 jours au total. Par conséquent, le présent avis doit être rendu au plus tard le 14 août 2011.

2. Faits

L'EESSI est un système informatique qui connecte les administrations des États membres responsables de la sécurité sociale pour ce qui est des échanges de données électroniques. Il a été mis au point par la Commission européenne en vertu du règlement (CE) n° 883/2004 tel que modifié par le règlement (CE) n° 988/2009 (le «règlement de base») et le règlement (CE) n° 987/2009 (le «règlement d'application») portant sur la coordination des systèmes de sécurité sociale.

Portée de l'EESSI: d'un point de vue géographique, les règles européennes sur la coordination en matière de sécurité sociale s'appliquent non seulement sur le territoire de l'UE mais également dans un certain nombre de pays participants[2], à savoir l'Islande, le Liechtenstein, la Norvège et la Suisse. Les règles européennes sur la coordination en matière de sécurité sociale s'appliquent aux ressortissants des États membres de l'UE et des pays participants ainsi qu'aux ressortissants de pays tiers qui résident légalement dans l'UE et qui ont travaillé dans plus d'un État membre de l'UE. Les données seront échangées entre les administrations compétentes de tous les pays participants dans les domaines régis par les règlements sur la coordination en matière de sécurité sociale, à savoir:

- prestations de maladie, de maternité et de paternité assimilées
- pensions de vieillesse, de retraite anticipée et d'invalidité
- prestations de survie et allocations de décès
- allocations de chômage
- allocations familiales
- prestations en cas d'accidents du travail et de maladies professionnelles

[2] Pour plus de facilité, le présent avis fera uniquement référence aux «États membres». Cependant, la référence dans le présent avis aux «États membres» doit être comprise comme incluant également les pays de l'EEE (Islande, Liechtenstein, Norvège) et la Suisse.

La **finalité** de l'EESSI est de renforcer la protection des droits des citoyens en permettant l'échange électronique, entre les administrations compétentes des États membres, d'informations personnelles sur la sécurité sociale des travailleurs migrants dans l'UE. L'objectif est de remplacer par l'EESSI les 200 formulaires papier actuellement utilisés par les administrations pour communiquer. Les échanges informatiques dans l'EESSI i) faciliteront et accéléreront le processus décisionnel pour le calcul et le paiement des prestations de sécurité sociale; ii) permettront une vérification plus efficace des données; iii) offriront une interface plus souple et plus conviviale entre les différents systèmes; et iv) permettront une collecte précise de données statistiques sur les échanges européens.

Calendrier: les règlements sur la coordination en matière de sécurité sociale sont entrés en vigueur le 1er mai 2010; cependant, il a été convenu d'instaurer une période de transition de deux ans pour permettre aux États membres de connecter leurs applications nationales au système EESSI. Le 1er mai 2012 au plus tard, toutes les administrations devraient être connectées à l'EESSI et échanger des informations via ce système.

Responsables du traitement: rôles et responsabilités
L'exploitation de l'EESSI implique le partage de certaines responsabilités entre les États membres et la Commission:

- **Au niveau des États membres**, les données à caractère personnel sont collectées par les administrations compétentes des États membres, conformément aux règles nationales en matière de protection des données mettant en œuvre la directive 95/46/CE. Chaque administration compétente est responsable de son propre traitement des données et de l'échange de données à caractère personnel dans l'EESSI, conformément aux règles énoncées aux articles 77[3] et 78[4] du règlement de base. En vertu de la directive 95/46/CE, les administrations compétentes responsables de la sécurité sociale peuvent être identifiées comme étant des responsables du traitement et assument donc les obligations et responsabilités correspondantes.

- **Rôle de la Commission dans la détermination des finalités et des moyens du traitement dans l'EESSI**: selon la notification soumise au CEPD, la Commission est un responsable du traitement compte tenu de son rôle dans l'EESSI. La Commission est responsable de la coordination de l'EESSI, elle assure le secrétariat du comité directeur du projet EESSI et participe, ayant voix consultative, à la commission administrative pour la coordination des systèmes de

[3] L'article 77 dispose que «*[l]orsque, en vertu du présent règlement ou du règlement d'application, les autorités ou institutions d'un État membre communiquent des données à caractère personnel aux autorités ou institutions d'un autre État membre, cette communication est soumise à la législation en matière de protection des données de l'État membre qui les transmet. Toute communication par l'autorité ou institution de l'État membre qui les a reçues, ainsi que le stockage, la modification et la destruction des données par cet État membre sont soumises à la législation en matière de protection des données de l'État membre qui les reçoit. Les données requises pour l'application du présent règlement et de son règlement d'application sont transmises par un État membre à un autre État membre dans le respect des dispositions communautaires en matière de protection des personnes physiques à l'égard du traitement et de la libre circulation des données à caractère personnel*».

[4] L'article 78, paragraphe 2, prévoit notamment que «*[c]haque État membre a la responsabilité de gérer sa propre partie des services de traitement électronique de l'information dans le respect des dispositions communautaires en matière de protection des personnes physiques à l'égard du traitement et de la libre circulation des données à caractère personnel*».

sécurité sociale (la «commission administrative»)[5]. La Commission est également responsable de l'infrastructure centrale et de la garantie de la sécurité des données échangées. De ce fait, la Commission européenne partage certaines responsabilités et obligations en tant que responsable du traitement en ce qui concerne l'EESSI, en application du règlement (CE) n° 45/2001. En outre, la Commission est également le responsable du traitement de la base de données publique qui sera créée en vertu de l'article 88, paragraphe 4, du règlement d'application, dans laquelle figurera la liste des administrations compétentes pour chaque État membre, ainsi que leurs points de contact.[6]

- **Futur rôle de la Commission en tant qu'utilisateur du système:** alors qu'un tel rôle n'est pas envisagé lors du lancement de l'EESSI, il est prévu à plus long terme que la Commission (PMO) devienne un utilisateur de l'EESSI en tant qu'administration compétente. Le service compétent au sein de la Commission ayant la responsabilité d'un tel traitement sera le responsable dudit traitement et il assumera les obligations et responsabilités prévues dans le règlement (CE) n° 45/2001. Ce rôle nécessitera de soumettre au CEPD une notification distincte de contrôle préalable; il n'est donc pas décrit ni analysé dans le présent avis.

La **responsabilité principale** du traitement entrepris par la Commission aux fins de l'exploitation de l'infrastructure EESSI incombe à l'unité «Coordination des systèmes de sécurité sociale, libre circulation des travailleurs», à la DG Emploi, Affaires sociales et Inclusion (DG EMPL, B.4). Dans le cadre des pratiques de travail standard à la DG EMPL, l'unité B.4 est soutenue par l'unité G.4 en ce qui concerne les connaissances, l'expertise et le support techniques et informatiques. L'unité G.4 est chargée du développement, de la maintenance et du support du système qui prendra en charge l'échange électronique de messages.

Sous-traitant: la Commission a désigné le centre de données DIGIT de la Commission comme **sous-traitant**. Le centre de données DIGIT de la Commission héberge et exploite des composantes centrales de l'EESSI (en particulier l'infrastructure sTESTA qui sert de réseau de communication connectant les réseaux nationaux des États membres entre eux et avec le centre de données DIGIT). Il envoie des informations et collecte des statistiques. La DG EMPL et DIGIT se sont accordés sur une proposition d'hébergement pour l'exploitation de l'infrastructure EESSI centrale hébergée dans le centre de données DIGIT de la Commission. Un accord de niveau de service entre la DG EMPL et DIGIT est en voie de finalisation. Un projet de l'ANS standard a été fourni au CEPD; la page 9 de l'ANS standard contient des clauses en matière de protection des données appliquant l'article 23 du règlement.

[5] La commission administrative, qui est rattachée à la Commission européenne, est le principal organe de direction dans le domaine de la coordination des systèmes européens de sécurité sociale. Elle est composée de représentants de tous les pays participants ainsi que d'un représentant de la Commission européenne. Les décisions prises au sein de cette commission administrative s'agissant de la mise en œuvre de l'EESSI concernent tous les aspects politiques, organisationnels et techniques ayant trait au déploiement, à la mise en œuvre et à l'exploitation du système. Par exemple, la commission administrative a décidé du contenu et du format des documents électroniques structurés (DES). En ce qui concerne le traitement des données, elle demande conseil à la commission technique pour le traitement des données.

[6] Les activités de traitement entreprises par la Commission concernant la fourniture de services de répertoire EESSI ne sont pas soumises en tant que telles au contrôle préalable du CEPD. Cependant, compte tenu du fait qu'elles sont un élément essentiel de l'EESSI, ces activités de traitement sont décrites dans le présent avis.

Description du traitement: les données à caractère personnel sont collectées par des administrations locales, régionales et nationales et sont ensuite transmises via l'EESSI aux administrations compétentes d'autres États membres au moyen d'un réseau sécurisé commun. Une architecture européenne commune pour l'échange électronique des données a été définie par la commission administrative, ses principales caractéristiques étant les suivantes:

Architecture de haut niveau de l'EESSI: le système est conçu comme une topologie «en étoile» avec un nœud central de coordination (NC) et des points d'extrémité appelés points d'accès (PA), qui sont déployés dans les États membres. L'EESSI est essentiellement composé i) d'une unité centrale (le nœud de coordination) qui sera hébergée dans le centre de données DIGIT de la Commission et comprenant les services d'annuaire EESSI, et ii) des parties internationales des PA des États membres qui sont connectés via un réseau sécurisé (sTesta) avec le nœud de coordination à travers lequel toutes les données électroniques doivent être échangées entre les États membres.

L'infrastructure européenne commune est développée au niveau de l'UE tandis que les États membres sont chargés de prendre les mesures nécessaires afin de se connecter à l'ensemble du système. À cette fin, les États membres ont désigné un point d'accès au minimum et cinq au maximum, par l'intermédiaire desquels les données sont transmises entre les États membres. L'EESSI concerne uniquement l'échange d'informations entre les États membres via leurs points d'accès. La transmission de données des parties nationales du ou des points d'accès aux institutions nationales de sécurité sociale relève exclusivement de la compétence des États membres.

EESSI AP_RI et WEBIC (interface web pour les agents): la Commission a mis au point un logiciel d'application de référence que les États membres peuvent utiliser sur une base volontaire. L'application de référence comprend un point d'accès international et national prédéfini (AP_RI) et une interface web par défaut pour les agents (l'outil WEBIC).

Messages et flux DES: les informations sur la sécurité sociale sont échangées au moyen de documents électroniques structurés (DES) qui seront échangés selon un protocole d'affaires. La structure des messages et le protocole sont approuvés par les comités directeurs et les groupes de travail concernés. Les DES peuvent uniquement être échangés selon des flux de travail prédéfinis. À cette fin, une centaine de flux dans lesquels les DES peuvent être échangés ont été définis. Ces flux sont la traduction des processus d'échange d'informations entre les administrations qui sont définis par le règlement d'application. Les flux peuvent uniquement être échangés entre deux administrations compétentes; si les données doivent être envoyées à plusieurs destinataires, l'administration qui les expédie doit réitérer l'opération autant de fois qu'il y a de destinataires. Les données ne peuvent en aucun cas être envoyées simultanément à tous les destinataires.

Fonctions de recherche dans l'EESSI: les agents des administrations compétentes ont la possibilité de rechercher des flux d'information dans l'EESSI. Ils auront accès aux en-têtes des flux, mais seront en mesure d'accéder au contenu d'un message DES donné uniquement s'ils y sont autorisés, c'est-à-dire s'ils sont l'expéditeur/ le destinataire désigné de ce flux.

Répertoire central EESSI[7]: un répertoire central hébergé dans le centre de données de la Commission contient des informations relatives aux administrations de sécurité sociale.

[7] Voir la note de bas de page 6.

Le répertoire central traite les coordonnées des administrations ainsi que les données à caractère personnel des personnes de contact des administrations compétentes. Ce répertoire sera utilisé:

- par les PA pour rechercher l'adresse du PA destinataire. À cette fin, une réplication du répertoire central est périodiquement transmise aux PA;
- par le NC pour valider l'adresse du PA tout en relayant les messages DES;
- par les fonctionnaires des administrations des États membres pour identifier les administrations d'autres États membres (en utilisant la réplication locale du PA du répertoire central);
- par les citoyens européens pour obtenir des informations sur les administrations via le site web public de l'EESSI (en utilisant une réplication du répertoire central dénommée «répertoire public»).

Référentiel d'informations: il existera un référentiel d'informations qui permettra de diffuser des informations générales sur l'EESSI aux acteurs concernés (p. ex. documentation type de l'EESSI, documents de conception, mises à jour logicielles, etc.).

Les personnes concernées sont les travailleurs et les membres de leur famille ayant travaillé dans plusieurs États membres et demandant à bénéficier de prestations de la sécurité sociale[8]. Les règlements relatifs à la sécurité sociale coordonnent également les droits de sécurité sociale des personnes inactives qui ont des liens avec plusieurs États membres. Les règlements s'appliquent également aux ressortissants de pays tiers qui résident légalement dans l'UE, conformément au règlement (CE) n° 1231/2010 du Conseil[9].

Données à caractère personnel échangées dans l'EESSI: des dispositions spécifiques du règlement de base définissent la portée des données à caractère personnel qui doivent être échangées entre les administrations compétentes. Un modèle EESSI qui définit le contenu des données qui seront échangées dans les DES et les types de flux a été convenu dans les groupes de travail mis en place par la commission administrative. Au total, 350 DES ont été définis. Les DES seront réexaminés une fois qu'une certaine expérience de l'utilisation des DES et des flux aura été acquise. En fonction des prestations sociales demandées et d'autres éléments, les types suivants de données à caractère personnel peuvent être échangés via l'EESSI:

- nom, sexe, adresse, date et lieu de naissance, renseignements sur le lieu de résidence, situation familiale, composition de la famille et identité (y compris p. ex. adoption d'enfants) des membres de la famille, en vie et décédés, informations concernant les droits de sécurité sociale (numéro de sécurité sociale, NIP (numéro d'identification personnel) dans l'administration de sécurité sociale compétente, début, fin, raisons d'un éventuel refus etc.), informations sur la santé du patient (y compris p. ex. examens/traitements médicaux) et accidents, informations sur les prestations perçues, informations financières (y compris numéros de compte bancaire, d'identification fiscale et de registre du commerce, revenus), situation et

[8] Il est prévu, à terme, que les fonctionnaires européens et d'autres catégories de personnel travaillant pour les institutions et les organes de l'UE deviennent également des personnes concernées dans l'EESSI. Le présent avis ne traitera pas de ces aspects qui seront analysés séparément lorsqu'une notification de contrôle préalable sera soumise au CEPD par le responsable du traitement européen concerné s'agissant de son activité de traitement en tant qu'administration compétente dans l'EESSI.

[9] Règlement (UE) n° 1231/2010 visant à étendre le règlement (CE) n° 883/2004 et le règlement (CE) n° 987/2009 aux ressortissants de pays tiers qui ne sont pas déjà couverts par ces règlements uniquement en raison de leur nationalité.

expérience professionnelles (y compris motif de licenciement). Des données révélant l'orientation sexuelle peuvent, dans certains cas, être déduites de l'état civil.

Transferts de données: les destinataires des données échangées via l'EESSI seront les agents des administrations des États membres compétentes dans le domaine spécifique de la sécurité sociale. La Commission assure l'échange de données à caractère personnel entre les États membres mais n'aura pas accès au contenu des données à caractère personnel qui transiteront de manière cryptée par l'EESSI (la Commission peut uniquement accéder aux en-têtes des messages à des fins statistiques, comme expliqué ci-dessous). Les membres du personnel de DIGIT ont accès à certaines données techniques utilisées par le système de messagerie en leur qualité d'administrateurs CE du nœud de coordination aux fins de la gestion du nœud de coordination et de la collecte de statistiques. Les membres du personnel de la DG EMPL, G.4, ont accès à certaines données dans l'EESSI en leur qualité d'administrateur CE[10] et administrateur SR[11] du répertoire central EESSI.

Les personnes concernées ont **le droit d'accéder** à leurs données et de les rectifier en contactant l'administration locale, régionale ou nationale à laquelle elles ont soumis leur demande de prestations sociales ou toute autre autorité compétente nationale vers laquelle elles sont redirigées. Selon les règlements relatifs à la sécurité sociale, il incombe aux États membres de s'assurer que les personnes concernées sont en mesure d'exercer pleinement leurs droits en ce qui concerne la protection des données à caractère personnel. Étant donné que la Commission ne collecte pas les données à caractère personnel des personnes concernées et qu'elle n'y a pas accès, elle ne peut les autoriser à accéder à leurs données et à les rectifier. La Commission leur facilitera cependant l'exercice de leurs droits en publiant une déclaration de confidentialité sur le site web de l'EESSI indiquant quels sont les moyens mis à leur disposition pour faire valoir leurs droits. Si les personnes concernées contactent la Commission concernant l'accès à leurs données, cette dernière les invitera à contacter l'administration nationale. En ce qui concerne les traitements entrepris par la Commission, les personnes concernées ont la possibilité d'envoyer une demande de renseignements au responsable du traitement par courrier ou courrier électronique (les coordonnées sont indiquées sur le site web de l'EESSI).

L'information des personnes concernées sera assurée par l'administration locale, régionale ou nationale auprès de laquelle les personnes concernées déposent une demande de prestations sociales. En outre, la Commission a adopté une notification relative à la protection des données qui sera publiée sur le site web de l'EESSI, contenant des informations sur le traitement des données à caractère personnel dans l'EESSI et sur les responsabilités respectives des États membres et de la Commission.

Les données à caractère personnel **ne sont pas stockées dans le système EESSI**, mais elles sont conservées dans des référentiels par les points d'accès des administrations nationales, sous leur responsabilité. Elles pourraient également être stockées par les autorités des États membres dans des bases de données locales lorsque des systèmes informatiques nationaux existent. Les données à caractère personnel sont conservées aux fins se rapportant à la demande d'une personne concernée sous la responsabilité des

[10] Un administrateur CE est tenu de maintenir des éléments de configuration centralisée dans la base de données.

[11] Un administrateur SR est une sorte de super utilisateur à qui l'on demande de commencer à configurer une base de données de services de répertoire vide.

administrations nationales qui les échangent. Les personnes concernées sont invitées à se renseigner sur les durées de conservation applicables en contactant l'autorité auprès de laquelle elles ont déposé leur demande.

La Commission ne conserve aucune donnée à caractère personnel dans l'infrastructure relevant de sa responsabilité. S'il s'avérait nécessaire de stocker temporairement des données pendant une courte durée à des fins techniques, les données à caractère personnel resteront dans tous les cas cryptées. Les messages en transit sont stockés temporairement pendant 2 jours maximum pour des raisons techniques dans le centre de données DIGIT de manière cryptée. Ils sont envoyés dès que cela est techniquement possible au PA destinataire.

Statistiques sur les échanges européens: les États membres sont responsables de la collecte de données statistiques relatives aux personnes concernées. L'article 91 du règlement de base dispose que les statistiques sont collectées et organisées suivant le plan et la méthode définis par la commission administrative; ce plan et cette méthode n'ont pas encore été convenus et sont en cours d'examen. La Commission collectera les données anonymes contenues dans l'en-tête/l'enveloppe des messages échangés entre les administrations aux fins de la production de statistiques sur les échanges européens via l'EESSI. Les données suivantes contenues dans l'en-tête peuvent être utilisées à des fins statistiques: numéro d'identification du DES (le numéro unique identifiant un DES donné), type de DES, version du DES, numéro d'identification du flux, type de flux, version du flux, informations concernant l'origine du DES (pays, PA, institution d'émission du DES), informations concernant la destination du DES (pays, PA, institution de destination), numéro d'identification de la catégorie de prestations, informations concernant les délais (date d'envoi des données et date d'échéance du DES le cas échéant), type d'action (notification, demande, réponse, révision, annulation ou réclamation). Le numéro d'identification du DES est traité comme un numéro de référence de fichier unique pour des étapes de traitement intermédiaires et il ne figure pas dans les statistiques finales qui font uniquement apparaître des données agrégées.

Les **exigences en matière de sécurité** dans l'EESSI **(...)**

3. Analyse juridique

3.1. Contrôle préalable

Applicabilité du règlement (CE) n° 45/2001 («le règlement»): le traitement de données notifié, dans la mesure où il concerne les activités de la Commission, relève du champ d'application du règlement et de la supervision du CEPD.[12]

La Commission sera considérée comme responsable du traitement qu'elle entreprend dans l'EESSI. Comme l'a souligné le groupe de travail «Article 29» dans son avis sur les notions de responsable du traitement et de sous-traitant[13], la détermination du ou des responsables du traitement doit reposer sur une analyse factuelle plutôt que théorique. Compte tenu des informations disponibles, le CEPD comprend que la Commission contribue à définir les finalités et les moyens utilisés pour traiter les données à caractère

[12] Pour chaque administration compétente, le droit applicable est sa propre législation en matière de protection des données (en conformité avec la directive 95/46/CE) et son activité est supervisée par sa propre autorité nationale/régionale chargée de la protection des données.

[13] Avis 1/2010 du groupe de travail «Article 29» sur les notions de «responsable du traitement» et de «sous-traitant», adopté le 16 février 2010.

personnel dans l'EESSI en participant, ayant voix consultative, à la commission administrative. En outre, la Commission est également responsable de l'infrastructure centrale et de la garantie de la sécurité des données échangées via l'infrastructure commune. De ce fait, la Commission européenne partage certaines responsabilités et obligations en tant que responsable du traitement en ce qui concerne l'EESSI, en application du règlement (CE) n° 45/2001.

La transmission de données à caractère personnel via un système d'échange électronique géré par la Commission constitue un traitement de données à caractère personnel; le fait que les données soient cryptées ne change rien à la conclusion selon laquelle les données transmises sont des données à caractère personnel, étant donné qu'elles concernent «*une personne physique identifiée ou identifiable*» (article 2, point a), du règlement). Le traitement des données est effectué par une institution de l'Union européenne dans l'exercice d'activités qui relèvent du champ d'application du droit de l'UE (article 3, paragraphe 1, du règlement, lu à la lumière du traité de Lisbonne). Le traitement des données est automatisé. Dès lors, le règlement (CE) n° 45/2001 s'applique.

Fondement du contrôle préalable: en vertu de l'article 27, paragraphe 1, du règlement, *«les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités sont soumis au contrôle préalable du contrôleur européen de la protection des données»*. L'article 27, paragraphe 2, du règlement contient une liste de traitements qui sont susceptibles de présenter de tels risques. Les échanges d'informations dans l'EESSI comprennent des données à caractère personnel relatives à la santé. Le traitement de données relatives à la santé est soumis au contrôle préalable du CEPD, conformément à l'article 27, paragraphe 2, point a), du règlement.

Portée de l'avis: les recommandations formulées dans le présent avis s'adressent à la Commission eu égard à son rôle dans la conception et l'exploitation de l'infrastructure de l'EESSI dans la mesure où ce traitement facilite l'échange d'informations sensibles entre administrations compétentes et qu'il est soumis à un contrôle préalable pour la raison susmentionnée.

Bien que le présent avis n'analyse pas le niveau de respect de la protection des données dans l'EESSI à l'échelle nationale, la plupart des recommandations formulées dans le présent avis peuvent faciliter le respect des règles en matière de protection des données par les utilisateurs du système, tels que les administrations compétentes des États membres. Par conséquent, les recommandations formulées par le CEPD à l'égard de la Commission devraient contribuer à garantir un niveau global élevé de protection des données dans l'EESSI.

De surcroît, comme indiqué à la page 4 ci-dessus, le CEPD souligne qu'avant que tout traitement soit entrepris par la Commission (PMO) en qualité d'administration compétente faisant fonction d'utilisateur du système EESSI aux fins de permettre aux personnes de faire valoir leurs droits de sécurité sociale, le responsable du traitement concerné devrait lui notifier le traitement en question en vue d'un contrôle préalable, en vertu de l'article 27, paragraphe 2, point a), du règlement.

3.2. Licéité du traitement

L'article 5 du règlement énonce des critères permettant de rendre le traitement de données à caractère personnel licite. Aux termes de l'article 5, point a), le traitement est licite s'il

est «*nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités… ou d'autres actes législatifs adoptés sur la base de ces traités*».

La base juridique du traitement entrepris par la Commission figure dans le règlement de base relatif à la coordination en matière de sécurité sociale et à l'article 4, paragraphe 2, du règlement d'application (CE) n° 987/2009, qui dispose que «*[l]a transmission de données entre les institutions ou les organismes de liaison s'effectue par voie électronique, soit directement, soit par l'intermédiaire des points de contact, dans un cadre sécurisé commun capable de garantir la confidentialité et la protection des échanges de données*».

Quant à la nécessité du traitement, le CEPD note que la facilitation de la libre circulation des travailleurs est un but légitime poursuivi par l'Union européenne depuis la fondation des Communautés européennes, qui comprend notamment la coordination des systèmes de sécurité sociale au sein de l'UE. L'article 48 du traité sur le fonctionnement de l'UE expose les compétences de l'UE dans le domaine de la coordination en matière de sécurité sociale. Qui plus est, le droit à la sécurité sociale est un droit fondamental protégé à l'article 34 de la Charte des droits fondamentaux de l'UE. Par conséquent, les mesures mises en place au niveau de l'UE pour coordonner les systèmes de sécurité sociale des États membres de l'UE pourraient être considérées nécessaires à la garantie de l'exercice effectif de ce droit fondamental.

Le CEPD apprécie que le traitement, qui comprend des catégories spéciales de données, repose sur une base juridique solide. Le CEPD constate que le règlement de base relatif à la coordination en matière de sécurité sociale a été complété par le règlement d'application qui prévoit des mesures d'application générales et que les modalités spécifiques du traitement sont clairement énoncées dans les décisions adoptées par la commission administrative[14].

3.3. Traitement portant sur des catégories particulières de données

Dans le contexte de l'EESSI, des données à caractère personnel relatives à la santé et les données susceptibles de révéler l'orientation sexuelle des personnes (telles que l'état civil) sont traitées. Le traitement de données à caractère personnel relatives à la santé ou à la vie sexuelle est interdit à l'article 10, paragraphe 1, du règlement sauf exceptions prévues à l'article 10, paragraphe 2, 3 ou 4, du règlement.

Aux termes de l'article 10, paragraphe 4, du règlement, «*sous réserve de garanties appropriées, et pour un motif d'intérêt public important, des dérogations (...) peuvent être prévues par les traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités ou, si cela s'avère nécessaire, sur décision du CEPD*». Le traitement entrepris par la Commission est mis en œuvre afin de garantir l'application des règlements européens relatifs à la coordination en matière de sécurité sociale, qui permettra aux citoyens de faire valoir effectivement leurs droits de sécurité sociale. Le traitement est donc effectué pour un motif d'intérêt public important, conformément aux règlements européens relatifs à la coordination en matière de sécurité sociale. Le CEPD considère que le traitement de catégories particulières de données par la Commission dans le contexte de l'exploitation de l'infrastructure EESSI est justifié au titre de l'article 10, paragraphe 4, du règlement.

[14] Mentionnées à la note de bas de page 5.

Cependant, compte tenu du rôle limité de la Commission dans le traitement de ces données, le CEPD estime qu'il est approprié d'exiger de la Commission qu'elle transmette uniquement des données cryptées, de manière à ce qu'elle n'ait pas accès au contenu des données sensibles qui transitent via l'EESSI.

3.4. Qualité des données

Adéquation, pertinence et proportionnalité: en vertu de l'article 4, paragraphe 1, point c), du règlement, les données à caractère personnel doivent être «*adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement*». Pour garantir la proportionnalité des données échangées, des dispositions spécifiques des règlements relatifs à la sécurité sociale définissent la portée des données qui doivent être échangées entre les administrations compétentes. En pratique, des formulaires standard (documents électroniques structurés) ont été définis par la commission administrative pour chaque type de demande, contenant des champs obligatoires et facultatifs structurés à remplir, limitant ainsi le nombre et les types de données traitées à ce qui est nécessaire pour une demande précise. Les données traitées s'avèrent nécessaires pour évaluer le droit des personnes à des prestations spécifiques de sécurité sociale. Dès lors, les informations présentées au CEPD sur les données traitées semblent satisfaire les exigences visées à l'article 4, paragraphe 1, point c).

Exactitude: l'article 4, paragraphe 1, point d), du règlement dispose que les données à caractère personnel doivent être *«exactes et, si nécessaire, mises à jour»*, et que *«toutes les mesures raisonnables sont prises pour que les données inexactes ou incomplètes soient effacées ou rectifiées»*. La plupart des informations seront transmises d'une administration compétente à une autre. Étant donné que les données ne seront pas, dans la plupart des cas, collectées directement auprès des personnes concernées, les droits d'accès et de rectification sont des moyens importants de garantir l'exactitude des données, dont les personnes concernées devraient pouvoir bénéficier (voir point 3.7).

Loyauté et licéité: l'article 4, paragraphe 1, point a), du règlement prévoit également que les données à caractère personnel doivent être «*traitées loyalement et licitement*». La licéité a déjà été examinée (voir point 3.2), alors que la loyauté sera appréciée dans le contexte des informations fournies à la personne concernée (voir point 3.8).

3.5. Conservation des données

L'article 4, paragraphe 1, point e), du règlement prévoit 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»*.

En ce qui concerne la conservation des messages DES par la Commission, le CEPD est satisfait de la courte durée de conservation de 2 jours prévue pour le transit des messages et du fait que les données conservées soient cryptées. La conservation des messages DES par la Commission est conforme à l'article 4, paragraphe 1, point e), du règlement.

En ce qui concerne la conservation des informations contenues dans les fichiers-journaux, nous comprenons que la Commission conservera les fichiers-journaux des opérations effectuées dans le nœud de coordination, ce qui est nécessaire pour contrôler et comprendre comment certains problèmes techniques ont pu survenir avec un

flux/message précis ou pour vérifier quels événements, le cas échéant, se sont produits à certains moments ou intervalles. Étant donné que ces informations ne sont pour l'instant définies dans aucun document en particulier, le CEPD recommande que les catégories de fichiers-journaux conservés par la Commission dans l'EESSI soient correctement renseignées, ainsi que leurs durées de conservation. Le CEPD insiste sur le fait que, conformément à l'article 37 du règlement, les journaux collectés par la Commission pour l'exploitation de l'infrastructure EESSI «sont effacés dès que possible, et au plus tard six mois après leur collecte». À cet égard, le CEPD note que le délai de conservation de 10 jours fixé dans la politique du centre de données DIGIT satisfait aux exigences du règlement.

En ce qui concerne la conservation de données par la Commission à des fins statistiques, conformément à l'article 4, paragraphe 1, point e), du règlement, la Commission doit s'assurer que les données sont rendues anonymes ou, si cela est impossible, que l'identité des personnes concernées est cryptée. À cet égard, la conservation du numéro d'identification DES pourrait permettre l'identification indirecte de la personne concernée par le message DES; par conséquent, les données stockées à des fins statistiques peuvent ne pas être totalement anonymes. Cependant, le fait que les données DES soient cryptées devrait empêcher la Commission de remonter jusqu'à une personne en particulier.

3.6. Transferts de données

Les données sont échangées entre les autorités compétentes désignées des États membres via l'infrastructure gérée par la Commission. La plupart de ces échanges ont lieu avec des destinataires qui appliquent la directive 95/46/CE et doivent donc être analysés conformément à l'article 8 du règlement, tandis que d'autres ont lieu avec des destinataires qui ne relèvent pas de ladite directive et doivent donc être analysés conformément à l'article 9 du règlement.

La Commission prend part à des transferts de données à des tiers qui relèvent de la directive 95/46/CE (États membres de l'UE et pays de l'EEE qui appliquent la directive). L'article 8, point a), du règlement dispose que les transferts de données sont possibles «si le destinataire démontre que les données sont nécessaires à l'exécution d'une mission effectuée dans l'intérêt public ou relevant de l'exercice de l'autorité publique». En l'espèce, les transferts de données relèvent clairement des missions des administrations de sécurité sociale compétentes; ils respectent donc l'article 8, point a), du règlement.

En outre, les transferts de données peuvent également avoir lieu avec des pays qui ne relèvent pas de la directive 95/46/CE, à savoir la Suisse. Ces transferts doivent être analysés à la lumière de l'article 9 du règlement. L'article 9 prévoit notamment que le transfert de données ne peut avoir lieu que pour autant qu'un niveau de protection adéquat soit assuré dans le pays du destinataire et que ce transfert vise exclusivement à permettre l'exécution des missions qui relèvent de la compétence du responsable du traitement. La Suisse bénéficie d'une décision de la Commission relative à la constatation du caractère adéquat de la protection des données à caractère personnel[15] qui reconnaît qu'elle assure un niveau de protection adéquat. Les données sont transférées uniquement aux administrations de sécurité sociale aux fins de l'exécution de leurs missions. L'article 9 du règlement est donc respecté.

[15] Décision 2000/518/CE de la Commission du 26.7.2000 – JO L 215/1 du 25.8.2000.

3.7. Droits des personnes concernées

L'article 12 de la directive 95/46/CE et les articles 13 et 14 correspondants du règlement prévoient un droit d'accès, à la demande de la personne concernée, aux données la concernant ainsi qu'un droit de rectification et d'effacement dans certaines circonstances.

Le CEPD fait observer que des mesures ont été prises par la Commission pour faciliter l'exercice des droits des personnes concernées dans un contexte transfrontière, en désignant l'administration à laquelle la demande a été soumise en tant que point de contact pour l'exercice de ces droits. La Commission ne jouera cependant aucun rôle dans l'octroi de droits dans l'EESSI aux personnes concernées; en cas de demande, elle dirigera uniquement la personne concernée vers le point de contact.

Le CEPD approuve la solution présentée par la Commission et la désignation d'un «guichet unique» pour l'exercice des droits des personnes concernées, ce qui devrait faciliter l'exercice effectif de leurs droits dans un contexte transfrontière. Le CEPD insiste sur le fait qu'il incombera à ce point de contact de s'assurer du plein respect des droits des personnes concernées. Le plein exercice des droits des personnes concernées dans un contexte transfrontière nécessitera notamment la mise en place de procédures entre les administrations compétentes pour 1) procéder à la vérification en bonne et due forme de l'information contestée, et 2) informer toutes les administrations concernées de toute demande de rectification/suppression qui a été satisfaite.

3.8. Information des personnes concernées

Les administrations compétentes sont tenues au titre des articles 10 et 11 de la directive 95/46/CE de fournir aux personnes concernées certaines informations sur le traitement. Les dispositions correspondantes du règlement (articles 11 et 12) définissent des exigences similaires pour la Commission, en ce qui concerne les données qu'elle traite.

Le CEPD relève qu'en plus de la notification spécifique relative à la protection des données qui doit être communiquée par les autorités compétentes lorsqu'une personne soumet une demande, la Commission a adopté sa propre notification relative à la protection des données fournissant des informations sur le traitement de données dans l'EESSI, qui sera publiée sur le site web de l'EESSI. La notification relative à la protection des données de la Commission contient tous les éléments énumérés aux articles 11 et 12 du règlement. Le CEPD approuve cette mesure qui contribue à accroître la transparence du traitement et fournit des informations utiles aux personnes concernées afin de faciliter l'exercice de leurs droits en matière de protection des données.

3.9. Traitement pour le compte du responsable du traitement

Le CEPD considère généralement qu'un sous-traitant est une organisation extérieure à laquelle l'institution ou l'organe de l'UE confie certaines missions. Cependant, en raison des effectifs importants de la Commission, le CEPD a accepté le fait que la Commission ait établi en bonne et due forme un système de délégation du rôle du responsable du traitement au sein de son organisation.

Le CEPD note que le projet d'ANS standard avec DIGIT qui lui a été soumis renferme des clauses qui satisferaient aux exigences de l'article 23 du règlement. Cependant, le CEPD insiste sur le fait que, comme indiqué à l'article 23, paragraphe 2, du règlement, le traitement en sous-traitance «*doit être régi par un contrat ou un acte juridique qui lie le*

sous-traitant au responsable du traitement». Le CEPD invite dès lors la DG EMPL à signer l'ANS avec DIGIT dès que possible et en tout état de cause avant que le système ne devienne pleinement applicable.

En outre, le CEPD recommande que la Commission réunisse des informations sur les rôles respectifs de DIGIT et de la DG EMPL, G.4, concernant leur accès aux données et leur traitement dans les différents systèmes informatiques de l'EESSI.

3.10. Sécurité des données

La sécurité des données relatives à la santé dans une situation transfrontière est particulièrement importante. La Cour européenne des droits de l'homme a accordé une importance particulière à la confidentialité des données relatives à la santé: «*Le respect de la confidentialité des données relatives à la santé est un principe essentiel dans les systèmes juridiques de l'ensemble des Parties à la Convention. Il est crucial non seulement de respecter la vie privée d'un patient mais également de préserver sa confiance dans le corps médical et dans les services de santé en général*».[16]

Le CEPD relève que les parties prenantes de l'EESSI ont convenu d'adopter des mesures spécifiques pour préserver la confidentialité des informations transitant par l'EESSI compte tenu de la sensibilité des données.

(...)

Le CEPD fait cependant observer que la politique de sécurité est assez détaillée dans certains domaines et qu'elle l'est moins dans d'autres. Le CEPD recommande que la Commission détaille davantage la politique de sécurité dans les domaines requis.

En outre, le CEPD n'a reçu aucune information sur aucun calendrier concret pour les audits du système. Comme indiqué dans la politique de sécurité, un audit permettant de vérifier le respect et l'application de la politique de sécurité et des procédures devrait[17] être entrepris régulièrement, mais il appartient à la commission administrative de décider de la fréquence de ces audits. Le CEPD reconnaît que, pour établir le lien de la théorie à la pratique, il serait très utile de procéder à un ou plusieurs audits de sécurité, au tout début de l'exploitation du système, après des changements importants dans le système, ou périodiquement. L'audit permettrait de se faire une idée du niveau de mise en œuvre de la politique de sécurité et des domaines qui doivent faire l'objet d'améliorations. En tant que tel, il constituerait un outil de gestion précieux. Le CEPD recommande donc que la Commission mette en place un plan d'audit effectif et procède à un ou plusieurs audits de sécurité du système.

4. Conclusions

Le CEPD considère que le traitement n'entraîne aucune violation du règlement (CE) n° 45/2001 pour autant que la Commission tienne pleinement compte des considérations susmentionnées avant que le système EESSI ne devienne applicable. La Commission européenne doit notamment:

[16] CEDH, 17 juillet 2008, *I/Finlande* (requête n° 20511/03), point 38.

[17] Dans la politique de sécurité, l'utilisation de «devrait» implique une forte recommandation (contrairement à un contrôle de sécurité essentiel et obligatoire, et à une recommandation ordinaire).

- transmettre des données cryptées uniquement, de telle sorte qu'elle n'ait pas accès au contenu des données sensibles transitant via l'EESSI;

- correctement renseigner les catégories de fichiers-journaux qu'elle conservera ainsi que leurs durées de conservation;

- contribuer à garantir que les personnes concernées peuvent pleinement faire valoir leurs droits auprès du point de contact correspondant dans l'État membre. Cela nécessitera notamment la mise en place de procédures entre les administrations compétentes pour désigner un point de contact central pour la personne concernée, vérifier l'information contestée, et informer toutes les administrations concernées de toute demande de rectification/suppression qui a été satisfaite;

- conclure un ANS juridiquement contraignant avec DIGIT contenant des clauses appropriées satisfaisant aux exigences visées à l'article 23 du règlement avant que le système ne devienne pleinement applicable;

- réunir des informations sur les rôles respectifs de DIGIT et de la DG EMPL, G.4, concernant leur accès aux données et leur traitement dans les différents systèmes informatiques de l'EESSI;

- compléter la politique de sécurité avec des dispositions plus détaillées, surtout dans les domaines où la politique maintient un niveau élevé;

- mettre en place un plan d'audit effectif et procéder à un ou plusieurs audits de sécurité du système;

- informer le CEPD de toute modification substantielle apportée à la conception du système qui pourrait avoir une incidence sur le niveau de protection des données dans l'EESSI.

Fait à Bruxelles, le 28 juillet 2011

(**signé**)

Giovanni BUTTARELLI
Contrôleur adjoint européen de la protection des données