Comité de sécurité de l'information
Chambre sécurité sociale et santé

CSI/CSSS/19/244

DÉLIBÉRATION N° 19/126 DU 2 JUILLET 2019 PORTANT SUR LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL PAR LES INSTITUTIONS BELGES DE SÉCURITÉ SOCIALE À DES INSTITUTIONS DE SÉCURITÉ SOCIALE D'AUTRES ETATS MEMBRES DE L'UNION EUROPÉENNE, DANS LE CADRE DU PROJET EESSI (ELECTRONIC EXCHANGE OF SOCIAL SECURITY INFORMATION)

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, en particulier l'article 15;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier l'article 114;

Vu la loi du 5 septembre 2018 *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, notamment l'article 97;

Vu le rapport de la Banque Carrefour de la sécurité sociale;

Vu le rapport de monsieur Bart Viaene.

A. OBJET

1. Le Règlement (CE) n° 883/2004 du Parlement européen et du Conseil du 29 avril 2004 *portant sur la coordination des systèmes de sécurité sociale* et le Règlement (CE) n° 987/2009 du Parlement européen et du Conseil du 16 septembre 2009 *fixant les modalités d'application du règlement (CE) n° 883/2004 portant sur la coordination des systèmes de sécurité sociale* contiennent des dispositions relatives à la coopération mutuelle entre les institutions de sécurité sociale des Etats membres de l'Union européenne et à l'échange électronique de données à caractère personnel entre ces institutions. Les autorités compétentes coopèrent dans la mesure où elles se fournissent tous les renseignements relatifs aux mesures prises en exécution du Règlement et aux modifications de leur réglementation qui peuvent avoir un impact sur l'exécution du Règlement et elles s'aident lors de l'application du Règlement comme s'il s'agissait de l'application de leur propre réglementation. Les Etats membres sont encouragés à avoir davantage recours aux nouvelles

technologies pour l'échange de données à caractère personnel qui sont nécessaires à l'application du Règlement et du règlement d'application.

2. Afin d'offrir aux assurés sociaux une protection sociale plus efficace et de réduire les charges administratives, l'Union européenne prévoit, dans un futur proche, un échange obligatoire de données à caractère personnel en matière de sécurité sociale par la voie électronique. Cette décision se concrétise dans le projet (« *Electronic Exchange of Social Security Information* »), un réseau électronique européen sécurisé qui relie les différentes institutions entre elles et qui a pour objet d'améliorer, au niveau international, l'échange direct de données à caractère personnel confidentielles et fiables et de simplifier la vie des assurés sociaux qui se déplacement librement au sein de l'Union européenne en garantissant le bénéfice permanent de leurs droits. Le projet est suivi pour la Belgique par le service public fédéral Sécurité sociale (en tant que représentant au sein de la Commission administrative pour la Coordination des systèmes de sécurité sociale) et par la Banque Carrefour de la sécurité sociale (en tant représentant au sein de la Commission technique responsable des aspects informatiques). Le système sera mis en place dans le courant du deuxième semestre de 2019.

3. En vertu de la réglementation précitée, tous les Etats membres de l'Union européenne sont obligés de fournir des efforts, tant au niveau technique que sur le plan juridique et administratif, de sorte que l'ensemble des institutions de sécurité sociale puissent se connecter au système central de l'EESSI. Toutes les institutions belges de sécurité sociale (fédérales et régionales) doivent se connecter à la porte d'accès (*access point*) auprès de la Banque Carrefour de la sécurité sociale, afin de pouvoir échanger, au niveau européen, des données à caractère personnel avec les institutions de sécurité sociale d'autres Etats membres. Elles auront, à cet effet, recours à l'application web RINA (« *Reference Implementation for a National Application* »"), en ce qui concerne les organisations qui échangent de petits volumes, ou à une application nationale propre, qui permet un échange de données à caractère personnel d'application à application.

4. Le projet EESSI est basé sur des *business use cases* (BUC, à définir comme des flux, processus ou scénarios). À l'heure actuelle, 145 au total, répartis parmi les catégories suivantes (comparables avec les différentes branches de la sécurité sociale).

catégories	*nombre de BUC*
processus de base	
AWOD: Accident at Work & Occupational Diseases	26
FB: Family Benefits	4
H: Horizontal	13
LA: Legislation Applicable	6
M: Miscellaneous	5
P: Pensions	9
R: Recovery	7
S: Sickness	25
UB: Unemployment Benefits	4
→ total	**122**
sous-processus	

H-sub: Horizontal Sub-Processes	11
AD-Sub: Administrative Sub-Processes	12
→ total	**23**

5. L'échange de données à caractère personnel entre les Etats membres de l'Union européenne a, par ailleurs, lieu au moyen de divers messages structurés, appelés *structured electronic documents* (SED), environ deux cents cinquante à l'heure actuelle.

catégories	*nombre de SED*
processus de base	
AWOD: Accident at Work & Occupational Diseases	51
FB: Family Benefits	17
H: Horizontal	20
LA: Legislation Applicable	12
M: Miscellaneous	6
P: Pensions	18
R: Recovery	23
S: Sickness	81
UB: Unemployment Benefits	30
→ total	**258**
sous-processus	
H-Sub: Horizontal Sub-Processes	
AD-Sub: Administrative Sub-Processes	
→ total	**15**

6. Les organisations belges suivantes participent au projet EESSI: l'Institut national d'assurance maladie-invalidité (processus P, M, R, S et H), l'Institut national d'assurances sociales pour travailleurs indépendants (processus LA, P, R et H), l'Office national de sécurité sociale (processus FB, LA, S, P, H et UB), le Service fédéral des Pensions (processus P, R et H), FEDRIS et les assureurs accidents du travail (processus AWOD et H), l'Office national de l'emploi (processus UB et H), les services régionaux d'emploi (processus UB et H), les organismes assureurs (processus AWOD, P, M, R, S et H) et l'organe interrégional pour les prestations familiales ORINT et les caisse d'allocations familiales (processus FB et H). Ces organisations s'échangent des données à caractère personnel avec leurs homologues respectifs d'autres Etats membres de l'Union européenne. À cet effet, il y a, en principe, lieu de désigner, par BUC et par pays, un organe de liaison unique (l'organe par défaut pour un BUC déterminé).

7. Par sa délibération n° 01/33 du 10 avril 2001, le Comité de surveillance près la Banque Carrefour de la sécurité sociale (le prédécesseur du Comité de sécurité de l'information) a déjà autorisé les institutions belges de sécurité sociale à communiquer des données à caractère personnel à des institutions étrangères de sécurité sociale, dans le cadre de l'application du Règlement (CEE) n) 1408/71 du Conseil du 14 juin 1971 *relatif à l'application des régimes de sécurité sociale aux travailleurs salariés, aux travailleurs non salariés et aux membres de leur famille qui se déplacent à l'intérieur de la Communauté* (dans l'intervalle abrogé et remplacé par le Règlement précité (CE) n° 883/2004) et du Règlement (CEE) n° 574/72 du Conseil du 21 mars 1972 *fixant les modalités d'application*

du règlement (CEE) n° 1408/71 relatif à l'application des régimes de sécurité sociale aux travailleurs salariés, aux travailleurs non salariés et aux membres de leur famille qui se déplacent à l'intérieur de la Communauté (dans l'intervalle abrogé et remplacé par le Règlement précité n°987/2009).

8. Le Comité de surveillance a estimé qu'il était opportun, dans le cadre d'une coopération internationale efficace, de prévoir une seule délibération générale autorisant les institutions belges de sécurité sociale à communiquer, moyennant le respect de quelques conditions aisément applicables, des données à caractère personnel à des institutions étrangères de sécurité sociale. Les conditions suivantes ont été fixées en la matière: l'institution de sécurité sociale étrangère motive la requête de communication de données à caractère personnel (en mentionnant la finalité et éventuellement le fondement de la réglementation), elle identifie les personnes concernées de manière univoque, la communication intervient dans le respect des règles relatives à la protection de la vie privée, seules les données à caractère personnel qui sont nécessaires pour répondre adéquatement à la demande sont communiquées par l'institution belge de sécurité sociale et les données à caractère personnel sont utilisées par l'institution étrangère de sécurité sociale pour les seules finalités mentionnées dans sa requête.

9. Dans sa délibération, le Comité de surveillance a cependant observé, de manière explicite, que son autorisation n'a pas trait aux communications à des institutions étrangères de sécurité sociale qui se déroulent au moyen d'un flux de données à caractère personnel électronique institutionnalisé par le biais du réseau de la Banque Carrefour de la sécurité sociale et qu'il doit, à nouveau, être consulté pour ces flux de données à caractère personnel.

10. La présente délibération vise donc à créer un cadre pour la communication - obligatoire - de données à caractère personnel par les institutions belges de sécurité sociale à leurs homologues respectifs dans les autres Etats membres de l'Union européenne, par la voie électronique, en application du système EESSI.

B. EXAMEN DE LA DEMANDE

11. Dans la mesure où la communication de données à caractère personnel est réalisée par une institution belge de sécurité sociale belge, elle doit, en vertu de l'article 15, § 1er, de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, faire l'objet d'une délibération de la chambre sécurité sociale et santé du comité de sécurité de l'information.

12. En vertu du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE,* les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes et elles ne peuvent pas être traitées ultérieurement d'une manière incompatible avec ces finalités (limitation des finalités), elles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données), elles doivent être conservées sous une forme permettant

l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (limitation de la conservation) et elles doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité).

Limitation des finalités

13. La communication précitée poursuit, de manière générale, l'application efficace du régime de sécurité sociale des personnes qui se déplacent au sein de l'Union européenne et dont les droits sont par conséquent définis en étroite collaboration entre les institutions de sécurité sociale compétentes des Etats membres de l'Union européenne.

14. La coordination de la sécurité sociale dans l'Union européenne intervient selon les principes suivants: l'assuré social tombe sous le régime d'un seul pays et paie donc uniquement des cotisations dans un seul pays; il a les mêmes droits et obligations que les ressortissants du pays dans lequel il est assuré; lorsqu'il prétend à une allocation, il est, le cas échéant, tenu compte des périodes antérieures au cours desquelles il était assuré, travaillait ou habitait dans d'autres pays et lorsqu'il a droit à une allocation d'un pays, il la reçoit généralement aussi s'il habite dans un autre pays.

15. Le Comité de sécurité de l'information constate que les Etats membres de l'Union européenne sont tenus, en vertu du Règlement (CE) précité n° 883/2004, de recourir davantage aux nouvelles technologies pour l'échange mutuel des données à caractère personnel nécessaires, mais que ce recours doit avoir lieu dans le respect des règles de protection de la vie privée des institutions de sécurité sociale concernées et de l'Union européenne.

16. Le Règlement (CE) n° 987/2009 précité contient aussi des dispositions relatives à la coopération entre les organes compétents. Ils fournissent ou échangent, dans les meilleurs délais, toutes les données à caractère personnel qui sont nécessaires à la détermination des droits et des obligations des personnes auxquelles le règlement de base s'applique. L'échange de données à caractère personnel intervient par la voie électronique, soit directement, soit indirectement, via les points d'accès, dans un environnement commun sécurisé garantissant la confidentialité et la protection des données à caractère personnel échangées.

Minimisation des données et limitation de la conservation

17. Vu la nature et l'ampleur du projet EESSI, il n'est pas possible de se prononcer, dans le cadre de la présente délibération, sur le respect des principes de minimisation des données et de limitation de la conservation lors de l'échange d'environ trois cents SED.

18. Le Comité de sécurité de l'information constate cependant que les organes concernés doivent, en vertu du Règlement (CE) n° 883/2004 et du Règlement (CE) n° 987/2009, lors de leurs échanges mutuels de données à caractère personnel toujours respecter la réglementation relative à la protection de la vie privée. Ils tombent, d'ailleurs, tous sous le champ

d'application du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*.

19. Les parties doivent donc en particulier veiller à ce qu'elles communiquent exclusivement les données à caractère personnel qui sont nécessaires à l'application de la sécurité sociale par le destinataire et qui ont trait à une personne connue en tant qu'assuré social auprès du destinataire.

20. Le destinataire peut conserver les données à caractère personnel aussi longtemps que nécessaire pour l'exécution de ses missions et doit les détruire ensuite, dans les meilleurs délais.

Intégrité et confidentialité

21. Vu la nature des données à caractère personnel partagées entre les différentes institutions de sécurité sociale, la communication et leur enregistrement doivent être protégés de la sorte que la confidentialité et l'intégrité des données à caractère personnel soient garanties. Chaque institution de sécurité sociale prévoit, à cet effet, des contrôles d'accès et limite les droits des utilisateurs au minimum nécessaire à l'exécution de leurs missions.

22. Les institutions de sécurité sociale qui ont recours aux services veillent à ce que les émetteurs des messages électroniques soient correctement identifiés. Les mesures nécessaires sont prises de sorte que la réception et/ou l'envoi d'un message électronique soit incontestable.

23. Cette délibération porte uniquement sur les communications de données à caractère personnel par les institutions belges de sécurité sociale dans le cadre du projet EESSI. Les communications de données à caractère personnel par des institutions de sécurité sociale à d'autres Etats membres de l'Union européenne ne doivent pas faire l'objet d'une délibération préalable du Comité de sécurité de l'information, mais sont soumises à la réglementation (européenne et nationale propre) en matière de protection de la vie privée.

24. Lors du traitement des données à caractère personnel, il y a lieu de tenir compte de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* et de toute autre réglementation relative à la protection de la vie privée, en particulier du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* et de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*.

Par ces motifs,

la chambre sécurité sociale et santé du comité de sécurité de l'information

conclut que les communications de données à caractère personnel par les institutions belges de sécurité sociale à des institutions de sécurité sociale d'autres Etats membres de l'Union européenne, dans le cadre du projet EESSI, dans le cadre de la coopération mutuelle conformément aux dispositions du Règlement (CE) n° 883/2004 *portant sur la coordination des systèmes de sécurité sociale* et du Règlement (CE) n° 987/2009 du Parlement européen et du Conseil du 16 septembre 2009 *fixant les modalités d'application du règlement (CE) n° 883/2004 portant sur la coordination des systèmes de sécurité sociale*, telles que décrites dans la présente délibération, sont autorisées moyennant le respect des mesures de protection des données qui ont été définies, en particulier les mesures en matière de limitation de la finalité, de minimisation des données, de limitation de la durée de conservation des données et de sécurité de l'information.

Bart VIAENE