Comité de sécurité de l'information
Chambres réunies

DELIBERATION N° 21/013 DU 6 JUILLET 2021 RELATIVE A LA COMMUNICATION DES DONNEES ANONYMISEES PAR LE SERVICE PUBLIC FEDERAL STRATEGIE ET APPUI (SPF BOSA) A L'ASSOCIATION DES INSTITUTIONS SECTORIELLES (AIS) CONCERNANT L'UTILISATION DE L'EBOX PAR LES ASSURES SOCIAUX AFFILIES, AVEC L'INTERVENTION DE LA BANQUE CARREFOUR DE LA SECURITE SOCIALE (BCSS) COMME ORGANISATION INTERMEDIAIRE POUR L'ANONYMISATION DES DONNEES

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 article 15, §2, deuxième alinéa ;

Vu loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral, en particulier l'article 35/1, §1, quatrième alinéa;

Vu la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, en particulier l'article114 ;

Vu la loi 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, en particulier l'article 95, 97 et 98 ;

Vu le rapport du service publique fédéral Stratégie et Appui;

Vu le rapport de M. Bart PRENEEL et M. Bart VIAENE.

I. OBJET DE LA DEMANDE

1. L'Association d'Institutions Sectorielles (AIS) est une association d'organisations gérées de manière paritaire en charge de droits sociaux ou d'indemnités sociales complémentaires sur base de données provenant du réseau de la Sécurité Sociale.

2. L'AIS organise un réseau secondaire en vue d'assurer vers leurs membres le flux des données sociales disponibles sur le réseau primaire de la Banque Carrefour de la Sécurité Sociale. Ces flux de données servent de base pour l'octroi des indemnités complémentaires de la sécurité sociale pour les différents secteurs et/ou pour la création d'un plan de pension sectoriel complémentaire.

3. L'AIS et ses membres souhaitent utiliser la boîte aux lettres électronique sécurisée «eBox Citoyen» pour la communication de documents aux citoyens. Le service eBox est fourni par le service public fédéral Stratégie et Appui. L'eBox est un service permettant aux expéditeurs

d'échanger de manière sécurisée des messages électroniques avec des citoyens. Les expéditeurs des messages électroniques sont les utilisateurs dans le sens de la Loi eBox (y compris les instances publiques, les institutions de sécurité sociale, les acteurs des soins de santé) qui mettent les messages à la disposition des citoyens, qui sont les destinataires. La communication électronique par le biais de l'eBox présente un degré élevé de sécurité de l'information et d'irréfutabilité. Si le citoyen choisit d'utiliser l'eBox, il devra s'enregistrer et il lui sera explicitement demandé de marquer son accord sur la réception électronique de messages des expéditeurs connectés (via My eBox Burger).

4. Compte tenu de l'utilisation de l'eBox, l'AIS voudrait tout d'abord savoir quel pourcentage des assurés sociaux appartenant à chacune des institutions sectorielles ont déjà donné leur consentement de recevoir des documents par l'intermédiaire de l'eBox.

5. Afin de fournir ces informations sur les consentements eBox accordées à l'AIS, la procédure d'anonymisation suivante est prévue par la Banque Carrefour de la Sécurité Sociale (BCSS) dans son rôle légal d'intégrateur de services dans le secteur de la sécurité sociale, du gestionnaire des répertoires de référence dans le secteur de la sécurité sociale et de l'organisation intermédiaire pour l'anonymisation des données à caractère personnel:
- la BCSS établit une liste des numéros d'identification de la sécurité sociale (NISS) des assurés sociaux concernés par fonds affilié à l'AIS
- la BCSS transfère la liste de NISS (sans information sur l'affiliation) au SPF BOSA
- le SPF BOSA complète la liste des informations sur le consentement des citoyens concernés ou non
- le SPF BOSA transfère la liste complète à la BCSS
- la BCSS calcule par institution membre de l'AIS le pourcentage des assurés sociaux concernés ayant donné leur consentement
- la BCSS transfère le résumé (pourcentage des consentements par institution membre) à l'AIS.

II. TRAITEMENT DE LA DEMANDE

A. RECEVABILITE DE LA DEMANDE ET COMPETENCE DU COMITE

6. Toute communication de données sociales à caractère personnel par une institution de sécurité sociale autre que celle visée à l'article 2, alinéa 1er, 2°, a), à un service public fédéral, à un service public de programmation ou à un organisme fédéral d'intérêt public autre qu'une institution de sécurité sociale doit faire l'objet d'une délibération préalable des chambres réunies du comité de sécurité de l'information. (Article 15, §2, deuxième alinéa de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*). En outre, la communication de données à caractère personnel par des services publics et des institutions publiques de l'autorité fédérale à des institutions de sécurité sociale visées à l'article 2, alinéa 1er, 2°, b) à f), de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* doit faire l'objet d'une délibération préalable des chambres réunies du comité de sécurité de l'information. (article 35/1, §1, quatrième alinéa, de la loi du 15 août 2012 *relative à la création et à l'organisation d'un intégrateur de services fédéral*).

7. Le Comité de la sécurité de l'information note que la BCSS (pour l'AIS et les institutions sectorielles) et le SPF BOSA échangent des données à caractère personnel, qui sont rendues anonymes par l'intermédiaire de la BCSS, de sorte que seules les données anonymes (sous forme de pourcentages par fonds) sont transmises à l'AIS.

8. Le Comité de sécurité de l'information considère donc qu'il est compétent pour donner son avis sur la demande.

B. QUANT AU FOND

B.1. RESPONSABILITE

9. Conformément à l'article 5.2 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* (règlement général sur la protection des données, ci-après 'RGDP'), le SPF BOSA (instance qui transfert les données) et la BCSS (instance destinataire) en tant que responsables du traitement sont responsables du respect des principes du RGPD et devraient être en mesure de le démontrer. Le Comité de sécurité de l'information note que l'AIS ne reçoit que des données anonymes sous la forme de pourcentages par fonds affilié.

10. Le Comité de sécurité de l'information rappelle que les responsables du traitement doivent tenir un registre des activités de traitement effectuées sous ses responsabilités dans les conditions prévues à l'article 30 du RGPD.

B.2. LICEITE

11. Conformément à l'article 5.1 a) RGPD, les données à caractère personnel doivent être traitées d'une manière licite à l'égard de la personne concernée. Cela signifie que le traitement envisagé doit être fondé sur l'un des motifs juridiques énoncés à l'article 6 RGPD.

12. Conformément à l'article 3 de la loi du 27 février 2019 *relative à l'échange électronique de messages par le biais de l'eBox* le SPF BOSA est chargé d'offrir une eBox pour personnes physiques. L'article 9 de la loi précitée stipule expressément que le SPF BOSA est le responsables du traitement pour le traitement des données à caractère personnel qui sont nécessaires pour la gestion et la garantie du bon fonctionnement de l'eBox qu'il offre. Compte tenu de ce qui précède, le Comité de sécurité de l'information considère la communication des données à caractère personnel décrites dans les paragraphes 3 et 4 de cette délibération afin d'informer les institutions sectorielles en tant qu'expéditeurs potentiels de messages via l'eBox de manière anonyme des consentements effectivement accordées par l'institution membre de l'AIS, nécessaire à l'exécution d'une mission d'intérêt public (c'est-à-dire la gestion et le bon fonctionnement de l'eBox) dont est investi le SPF BOSA comme le responsable du traitement (article 6.1 e) RGDP).

B.3. LIMITATION DES FINALITES

13. Article 5.1 b) RGPD ne permet le traitement de données à caractère personnel que pour des fins déterminées, explicites et légitimes (principe de finalité). En outre, les données ne peuvent pas faire l'objet d'un traitement ultérieur d'une manière incompatible avec ces objectifs. Le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré,

conformément à l'article 89, paragraphe 1, RGDP comme incompatible avec les finalités initiales.

14. Le traitement décrit a pour objet d'informer les institutions affiliées de l'AIS du nombre d'assurés sociaux par institution affiliée ayant donné son consentement à recevoir des documents par l'intermédiaire de l'eBox Burger. Compte tenu de la nature des institutions concernées, en particulier des institutions de sécurité sociale, et de l'objectif de l'eBox Citoyen, le Comité de sécurité de l'information considère que ce traitement est spécifique, explicitement défini et justifié.

15. Le Comité de sécurité de l'information prend acte du fait que les données sont initialement recueillies par le SPF BOSA dans le cadre de l'enregistrement du consentement des personnes concernées pour l'utilisation de l'eBox Citoyen. Le traitement complémentaire décrit ci-dessus vise un objectif statistique, à savoir fournir le pourcentage d'assurés sociaux par membre de l'AIS qui ont consenti à l'utilisation de l'eBox Citoyen. Conformément à l'article 5.1 b), du RGPD, le traitement ultérieur à des fins statistiques n'est pas considéré comme incompatible avec les objectifs initiaux, pour autant que les conditions de l'article 89.1 du RGPD soient respectées. Cela signifie que les garanties appropriées doivent être prises conformément au RGPD en ce qui concerne les droits et libertés de la personne concernée. Ces garanties devraient garantir que des mesures techniques et organisationnelles ont été prises pour assurer le respect du principe du traitement minimal des données. Ces mesures peuvent inclure la pseudonymisation, à condition que ces objectifs puissent être atteints. Lorsque ces objectifs peuvent être atteints par un traitement ultérieur qui ne permet pas ou ne permet plus l'identification des personnes concernées, ils doivent donc être atteints. En outre, le titre 4 de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel* fixe les conditions de traitement en vue de l'archivage dans l'intérêt public, de la recherche scientifique ou historique ou à des fins statistiques, y compris la nécessité d'utiliser en principe des données anonymes.

16. Le Comité de sécurité de l'information prend note du fait que les données sont anonymisées par une organisation intermédiaire, en particulier la BCSS, avant que le résultat statistique ne soit communiqué au destinataire. Le Comité de sécurité de l'information considère donc que les conditions énoncées à l'article 89.1 du RGPD sont remplies.

B.4. TRANSPARANCE

17. Conformément à l'article 5.1 a), du RGPD, les données à caractère personnel doivent également être traitées de manière loyale et transparente au regard de la personne concernée. L'article 12 du RGPD oblige le responsable du traitement à prendre les mesures appropriées pour fournir toute information visée aux articles 13 et 14 du RPGD (c'est-à-dire les informations à communiquer lorsque les données sont collectées auprès de l'intéressé ou non auprès de l'intéressé) ainsi que pour procéder à toute communication au titre des articles 15 à 22 (concernant les droits de l'intéressé) et de l'article 34 (en cas d'infraction) en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples.

18. Le Comité de sécurité de l'information prend note du fait que le citoyen consent expressément à l'utilisation de l'eBox Citoyen et que le SPF BOSA a établi des conditions d'utilisation et une déclaration de confidentialité à cet effet. Le Comité de sécurité de l'information estime approprié que la déclaration de confidentialité de eBox Citoyen indique

explicitement que ses données personnelles peuvent être traitées à des fins statistiques afin de gérer et de rendre accessible l'eBox Citoyen et que les données anonymes sur l'utilisation de l'eBox Citoyen peuvent être partagées sous forme de statistiques avec les expéditeurs et les expéditeurs potentiels de messages via l'eBox Citoyen.

B.4. MINIMISATION DES DONNES

19. L'article 5.1 b) du RGPD dispose que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

20. Le Comité de sécurité de l'information note que le SPF BOSA reçoit de la part de la BCSS une liste des numéros d'identification de la sécurité sociale des personnes qui sont des assurés sociaux d'une institution sectorielle. L'affiliation de l'assuré social à une institution sectorielle particulière n'est pas incluse dans cette liste reçue par le SPF BOSA. Le SPF BOSA complète la liste en indiquant si la personne concernée a ou non consenti d'utiliser l'eBox Citoyen. Cette liste complétée est ensuite de nouveau communiquée à la BCSS par le SPF BOSA. Au cours de la phase suivante, la BCSS calcule le pourcentage de personnes concernées qui ont donné leur consentement à chaque institution membre de l'AIS. Enfin, la BCSS transfère le résultat statistique (le pourcentage de consentements accordés par institution membre) à l'AIS.

21. Compte tenu de ce qui précède, le Comité de sécurité de l'information considère que les données à caractère personnel sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

B.5. LIMITATION DE CONSERVATION

22. Conformément à l'article 5.1 e) du RGPD, les données à caractère personnel ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant la durée nécessaire à la réalisation des finalités pour lesquelles les données à caractère personnel sont traitées. La BCSS, en tant qu'organisme intermédiaire, ne peut conserver les données à caractère personnel que pendant la durée nécessaire à la réalisation de l'analyse statistique et à la communication du résultat au destinataire. Le Comité de sécurité de l'information note une fois de plus que le destinataire (l'AIS) ne reçoit que des données anonymes sous forme de statistiques.

B.6. INTEGRITE ET CONFIDENTIALITE

23. Conformément à l'article 5.1 f) du RGPD, les données à caractère personnel 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.

24. Conformément à l'article 24 du RGPD, les responsables du traitement doivent mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au règlement précité, compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques.

25. Le Comité de sécurité de l'information prend acte du fait que le SPF BOSA déclare avoir pris les mesures techniques et organisationnelles appropriées et a veillé à ce que les infrastructures ICT auxquelles sont connectés les dispositifs utilisés pour le traitement des données à caractère personnel garantissent la confidentialité et l'intégrité des données à caractère personnel. Le Comité de sécurité de l'information prend acte du fait que le SPF BOSA, la BCSS et l'AIS ont désignés un délégué à la protection des données.

26. Le SPF BOSA, la BCSS et l'AIS et leurs collaborateurs sont tenus de respecter la confidentialité en ce qui concerne les données à caractère personnel traitées et les éventuels résultats de leur traitement.

27. Le Comité de sécurité de l'information fait référence aux directives en matière de protection applicables à toutes les institutions publiques fédérales qui sont reprises dans la Politique fédérale sur la sécurité de l'information (*Federal Information Security Policy*).

28. Le Comité de sécurité de l'information prend acte du fait que la BCSS et l'AIS sont tenues de respecter les normes minimales de sécurité fixées par le Comité général de coordination de la Banque carrefour de la sécurité sociale.

29. Lors du traitement des données à caractère personnel, l'organisation doit 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,

le Comité de sécurité de l'information, en chambres réunies,

conclue que la communication des données anonymisées par le service public fédéral Stratégie et Appui à l'Association des Institutions Sectorielles concernant l'utilisation de l'eBox par les assurés sociaux affiliés, avec l'intervention de la Banque Carrefour de la Sécurité Sociale comme organisation intermédiaire pour l'anonymisation des données, est autorisée moyennant le respect des mesures de protection de la vie privée qui ont été définies dans cette délibération 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, et à condition que le SPF BOSA indique explicitement dans la déclaration de confidentialité de eBox Citoyen que les données personnelles peuvent être traitées à des fins statistiques afin de gérer et de rendre accessible l'eBox Citoyen et que les données anonymes sur l'utilisation de l'eBox Citoyen peuvent être partagées sous forme de statistiques avec les expéditeurs et les expéditeurs potentiels de messages via l'eBox Citoyen.

Bart PRENEEL
Chambre autorité fédérale

Bart VIAENE
Chambre sécurité sociale et santé