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

CSI/CSSS/19/004

DÉLIBÉRATION N° 19/004 DU 15 JANVIER 2019 RELATIVE À L'UTILISATION DE DONNÉES À CARACTÈRE PERSONNEL DU RÉSEAU DE LA SÉCURITÉ SOCIALE PAR LA PERSONNE CONCERNÉE MÊME AU MOYEN D'UNE APPLICATION D'UNE TIERCE PARTIE PRIVÉE

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 son article 15, § 1er ;

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 la demande de l'association sans but lucratif SIGEDIS;

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

Vu le rapport de monsieur Bart Viaene.

A. OBJET

1. L'association sans but lucratif SIGEDIS fait constater que les individus ont le droit de savoir quelles données à caractère personnel les concernant sont conservées par elle. Elle leur offre donc un meilleur aperçu de leur situation professionnelle et financière grâce aux applications en ligne sécurisées *mycareer.be* et *mypension.be.* SIGEDIS estime cependant que les individus ne sont pas obligés d'exercer leur droit d'information exclusivement au moyen des applications développées et choisies par les pouvoirs publics. En vertu du principe de la portabilité des données, qui est régi par le 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 individus ont, par ailleurs, le droit de faire transférer, à certaines conditions, leurs données à caractère personnel à un partenaire de leur choix.

2. Divers tiers sont, pour l'instant, en train de développer des applications qui permettent au citoyen (généralement, mais pas exclusivement, le client ou le client potentiel) de consulter ses données dans une source déterminée, éventuellement en même temps que des données provenant d'autres sources et éventuellement avec une prestation de services supplémentaire, qui n'est pas nécessairement de nature publique telle que la fourniture d'avis financiers ou la gestion de portefeuilles. Les cas d'usage peuvent être très variés selon SIGEDIS. Songeons notamment aux cas suivants (énumération non limitative).

- Une personne souhaite que l'état de constitution de sa pension complémentaire soit ajouté à l'aperçu global de son portefeuille financier offert par la banque.

- Une personne souhaite avoir recours à un simulateur d'optimalisation de carrière sans qu'elle ne doive introduire elle-même des données de carrière ou les fournir par mail ou sur support papier à un collaborateur du prestataire de services.

- Une personne souhaite acheter un produit financier et sa banque doit établir et actualiser régulièrement à cet effet, notamment sur la base des réserves de sa pension complémentaire, un profil d'investisseur en fonction de l'évolution de la situation financière.

- Une personne souhaite obtenir une analyse faite sur mesure de sa situation financière qui tienne compte de sa constitution de pension réelle dans le premier et le deuxième pilier et de son revenu social ou fiscal réel et donc ses données doivent être téléversées une seule fois.

- Une personne souhaite obtenir régulièrement, en fonction de la modification périodique de sa situation financière, une mise à jour de son analyse financière, de sorte que des options d'investissement puissent lui être offertes lorsque celles-ci deviennent à nouveau intéressantes suite à la modification de sa situation.

- Une personne souhaite consulter l'aperçu de sa carrière dans l'application de confiance de sa propre organisation de la société civile plutôt que dans l'application de la sécurité sociale (mycareer.be).

- Une personne souhaite utiliser la plateforme européenne Find Your Pension afin d'obtenir un aperçu global des droits de pension qu'elle a dans l'intervalle constitués dans les différents pays où elle a travaillé, parmi lesquels la Belgique.

3. En fonction de la situation, l'application du tiers peut donc combiner la visualisation des données propres de la personne concernée avec un traitement spécifique (comme en cas de simulation). Dans chacune des situations, la personne concernée peut décider, à l'instar des possibilités qui lui sont offertes dans les applications des pouvoirs publics, d'enregistrer (ou de ne pas enregistrer) ses données localement, dans l'application du tiers ou sur l'appareil qu'il a utilisé pour utiliser l'application. Il peut, par ailleurs, s'agir d'un usage unique des données (visualisation, simulation, ...). Toutefois, une relation de longue durée entre la personne concernée et le tiers (ou son application) est également possible (par exemple dans une relation entre la banque et le client). Dans ce cas, il est également possible que

l'application actualise régulièrement les données, même à des moments où la personne concernée n'est pas connectée, afin d'actualiser l'offre de services d'accompagnement et d'informer la personne concernée sur la présence de nouvelles possibilités.

4. SIGEDIS souhaite offrir au citoyen la possibilité de consulter ses données de manière sécurisée dans des applications de prestataires de services privés choisis par lui-même ou de les faire traiter par ces applications, sans que l'intégrité de sa vie privée ne soit compromise. Elle invite par conséquent le Comité de sécurité de l'information, et non uniquement pour elle-même, mais aussi pour toutes les autres institutions de sécurité sociale, à définir les principes qui sont valables pour la transmission de données d'un assuré social qui sont consultables au moyen d'une application développée par une institution de sécurité sociale ou qui font l'objet d'un droit de consultation par une tierce partie qui offre des applications ou des services à ce même assuré social. Sans préjudice de l'application 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*, il faudrait respecter ces principes chaque fois que des données d'un assuré social issues du réseau de la sécurité sociale sont communiquées à une tierce partie qui offre des applications ou des services à la personne concernée.

B. EXAMEN

5. Il s'agit d'une communication de données à caractère personnel par des institutions de sécurité sociale (dont SIGEDIS) à des tiers (prestataires de services privés) qui, 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*, doit faire l'objet d'une délibération de la chambre sécurité sociale et santé du comité de sécurité de l'information.

6. 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 (principe de la limitation des finalités), elles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (principe de la 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 (principe de la 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).

7. Vu la nature de la demande lui soumise, le Comité de sécurité de l'information ne peut se prononcer sur le respect des principes de limitation des finalités, de minimisation des données et de limitation de la conservation (en effet, la demande porte, d'une manière générale, sur le

traitement de données à caractère personnel non précisées à des finalités non précisées pour les besoins de prestataires de services non précisés).

La présente délibération sert par conséquent uniquement de cadre général qu'il faut toujours respecter en cas de communication de données issues du réseau de la sécurité sociale à une tierce partie qui offre des applications ou des services à la personne concernée. Pour le surplus, elle ne porte nullement préjudice à la compétence du Comité de sécurité de l'information qui doit se prononcer sur ce type de communications de données au cas par cas. Par groupe d'organisations similaires qui poursuivent le même but, le Comité de sécurité de l'information doit donc évaluer séparément quelles données ces dernières peuvent traiter dans ce cas général (selon les règlements en vigueur).

8. Il est toutefois essentiel que la consultation ait effectivement lieu à l'initiative de la personne concernée, quelle que soit l'instance qui offre l'application et quel que soit le cadre de services plus large offert. Lors du traitement des données à caractère personnel, toute opération intervient à l'initiative de la personne en question et moyennant son consentement (par exemple au moyen d'un pop-up avec la preuve que le citoyen a cliqué après une authentification suffisamment forte). La tierce partie convient explicitement avec la personne concernée quelle est la portée de l'intervention et informe la personne concernée sur ses interventions éventuelles. La personne concernée est totalement libre de (ne pas) donner son accord et elle peut aussi retirer ou modifier son consentement à tout moment. La tierce partie conserve toutes les preuves utiles du consentement de la personne concernée et les tient à la disposition des sources authentiques des données en vue de leur consultation.

Il y a, en outre, lieu d'observer que le traitement de données à caractère personnel dans ce cadre général puise sa légitimité dans la présente délibération du Comité de sécurité de l'information qui, en vertu de l'article 46, § 2, de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, a une portée générale contraignante entre les parties et envers les tiers et ne peut être contraire aux normes juridiques supérieures, et non dans le consentement de la personne concernée.

9. Toute application d'une tierce partie qui a recours à des données à caractère personnel du réseau de la sécurité sociale et qui met ensuite ces données à caractère personnel, après les avoir traitées (ou non), à la disposition de la personne concernée, doit satisfaire aux mêmes standards de sécurité que ceux valables pour des applications similaires des pouvoirs publics. En ce qui concerne la sécurité du login, le niveau de sécurité de l'application de la tierce partie doit satisfaire aux exigences les plus strictes en matière d'authentification (à savoir le niveau 400 ou supérieur au sein du Federal Authentication Service). Ces exigences sont déjà applicables aux applications des pouvoirs publics *mycareer.be* et *mypension.be*.

10. L'échange de données à caractère personnel provenant du réseau de la sécurité sociale doit, par ailleurs, avoir lieu de manière sécurisée et structurée, entre serveurs équipés des certificats utiles, à l'instar de ce qui se passe au sein de la sécurité sociale.

11. Contrairement aux échanges de données à caractère personnel entre les acteurs du réseau de la sécurité sociale, qui sont basés sur les relations entre l'assuré social et les institutions de sécurité sociale connues par les pouvoirs publics, qui sont déterminés dans le répertoire des

références de la Banque Carrefour de la sécurité sociale, les relations entre le citoyen et la tierce partie dans les situations précitées ne sont pas connues par les pouvoirs publics. Il n'est pas question d'un répertoire des références qui indique qu'une personne est cliente d'une banque, d'un assureur, d'un courtier, d'une organisation de la société civile déterminé(e). Par ailleurs, les relations peuvent être uniques ou de très courte durée (par exemple, lorsqu'une simulation ou une offre est demandée par un client prospectif et que celle-ci ne résulte pas, par la suite, dans une relation de longue durée). Le citoyen est le seul à pouvoir confirmer l'existence d'une telle relation. Dans le cadre de la transparence, le citoyen doit aussi avoir une vue sur l'usage de ses données par des tierces parties. C'est la raison pour laquelle le citoyen doit d'abord recevoir un avertissement à l'adresse mail qu'il a enregistrée (par exemple dans son eBox) qu'une application utilise un accès à ses données. Il s'agit dans l'intervalle d'une pratique courante dans de nombreuses applications privées sécurisées telles que LinkedIn, Facebook et le compte Google. Le citoyen est, de cette manière, en mesure de réagir immédiatement lorsque l'accès lui paraît suspect et ne correspond pas aux relations qu'il a avec des parties tierces. Par ailleurs, un simple moyen est prévu pour que le citoyen puisse faire connaître l'existence d'une relation entre le tiers et lui-même, au moyen de la technologie du *Open Authorization*. Il peut aussi, à tout moment, consulter les relations actives qui existent et peut, le cas échéant, y mettre fin, par exemple en tant que réaction à l'avertissement précité qu'il a reçu par mail.

12. La tierce partie qui souhaite utiliser les possibilités prévues à cet effet, devra accepter les conditions d'utilisation, de manière explicite et par écrit, avant un premier échange des données. Étant donné que tout offreur de données peut fixer des restrictions complémentaires, un document par set de données et par offreur de données s'avère opportun.

13. Le tiers se tient à la disposition pour un audit éventuel par le délégué à la protection des données des institutions de sécurité sociale qui constituent la source authentique des données en question.

14. Enfin, lors du traitement des données à caractère personnel, il est tenu 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 le traitement de données à caractère personnel issues du réseau de la sécurité sociale par la personne concernée même, au moyen d'applications offertes par une tierce partie comme décrit dans la présente délibération, doit toujours intervenir conformément aux dispositions de la présente délibération.

La présente délibération fait office de cadre général qu'il y a lieu de respecter lorsque des données issues du réseau de la sécurité sociale sont communiquées à une tierce partie qui offre des applications ou des services à la personne concernée. Toutefois, elle ne porte nullement préjudice à la compétence du Comité de sécurité de l'information qui doit se prononcer sur ce type de communications au cas par cas.

Bart VIAENE