

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

CSI/CSSS/19/050

DÉLIBÉRATION N° 19/032 DU 5 FÉVRIER 2019 PORTANT SUR L'UTILISATION DE DONNÉES À CARACTÈRE PERSONNEL DU RÉSEAU DE LA SÉCURITÉ SOCIALE PAR LES ÉTABLISSEMENTS DE CRÉDITS ET LES PRESTATAIRES DE PRODUITS ET DE SERVICES FINANCIERS (ET LEURS AGENCES ET FILIALES RESPECTIVES) AU PROFIT DES CLIENTS CONCERNÉS (ACTUELS ET PROSPECTIFS)

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, § 1^{er} ;

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. Par sa délibération n° 19/004 du 15 janvier 2019, la chambre sécurité sociale et santé du Comité de sécurité de l'information a décidé, suite à une question de l'association sans but lucratif SIGEDIS, que le traitement de données à caractère personnel issues du réseau de la sécurité sociale par l'intéressé même, au moyen d'applications qui sont offertes par une tierce partie, doit toujours avoir lieu dans le respect des dispositions de cette délibération. En effet, cette délibération fait office de cadre général qu'il y a lieu de respecter, toutefois, celle-ci ne porte pas préjudice à la compétence du Comité de sécurité de l'information qui peut se prononcer, au cas par cas, sur ce type de traitement de données à caractère personnel. Cela signifie que toute organisation (le cas échéant, un groupe d'organisations) qui développe une application pour offrir au citoyen la possibilité de consulter ses données à caractère personnel dans une source déterminée du réseau de la sécurité sociale, éventuellement en même temps que des données à caractère personnel d'autres sources et avec une prestation de services

supplémentaire, doit obtenir à cet effet, au préalable, une délibération du Comité de sécurité de l'information.

2. La présente délibération concerne l'utilisation de données à caractère personnel du réseau de la sécurité sociale (en particulier des données à caractère personnel de l'association sans but lucratif SIGEDIS) par les établissements de crédits agréés par la Banque nationale de Belgique (voir <https://www.nbb.be/fr/supervision-financiere/controle-prudentiel/domaines-de-contrôle/etablissements-de-credit/listes-7>), les prestataires de divers produits et services financiers (voir <https://www.fsma.be/fr/quels-prestataires-peuvent-vous-offrir-des-produits-et-services-financiers> et <https://www.fsma.be/fr/node/7164>) et leurs agences et filiales respectives. Ils souhaitent procéder au traitement de données à caractère personnel de clients actuels et de clients prospectifs, qui doivent donner leur consentement à cet effet, en vue de compléter les données qu'ils offrent déjà à la consultation, de fournir des avis financiers et de formuler des propositions commerciales adéquates (il s'agit de personnes qui ont déjà une relation contractuelle avec le prestataire de services ou qui souhaitent avoir recours à une offre précontractuelle, sans engagement, du prestataire de services). L'initiative émane de l'intéressé même: il choisit le prestataire de service de manière autonome et décide ensuite d'avoir ou non recours aux services proposés en rapport avec le traitement des données à caractère personnel issues du réseau de la sécurité sociale.
3. Le traitement demandé a trait à des données à caractère personnel que le citoyen peut déjà consulter lui-même dans la partie « ma pension complémentaire » de mypension.be. Il s'agit, par combinaison existante d'organisme de pension, d'organisateur, et de plan de pension, du compte de pension complémentaire mentionnant la dernière réserve acquise connue, la prestation acquise, la prestation attendue, ainsi que les dates de calcul et d'évaluation y associées, le niveau de financement, les couvertures décès éventuelles et les événements éventuels qui ont une influence sur les valeurs précitées (telles qu'un paiement partiel).

Renseignements généraux sur les pensions complémentaires de la personne concernée (affiliée en tant que salarié et/ou indépendant): la date d'évaluation (l'année à laquelle les renseignements ont trait), la réserve totale (le montant entretemps épargné pour l'ensemble des pensions complémentaires), la rente indicative mensuelle totale (le montant de la pension que rapporterait par approximation la réserve totale pour la personne affiliée), la couverture décès totale (le montant que percevraient les bénéficiaires lors du décès de la personne affiliée), l'assurance complémentaire totale contre le risque d'accident (l'indication selon laquelle les bénéficiaires ont droit ou non à une allocation supplémentaire en cas de décès de la personne affiliée dans un accident) et la rente d'orphelin supplémentaire totale (l'indication selon laquelle les enfants bénéficient déjà d'une rente d'orphelin supplémentaire lors du décès de la personne affiliée).

Distinction entre travailleurs et indépendants: la réserve de pension totale en tant que travailleur, la réserve de pension totale en tant qu'indépendant, la couverture décès totale en tant que travailleur, la couverture décès totale en tant qu'indépendant, l'assurance complémentaire totale contre le risque d'accident en tant que travailleur, l'assurance complémentaire totale contre le risque d'accident en tant qu'indépendant, la rente d'orphelin complémentaire totale en tant que travailleur et la rente d'orphelin complémentaire totale en tant qu'indépendant.

Renseignements sur le plan de pension externe (géré par un organe de pension externe): le numéro d'entreprise et la dénomination sociale de l'organisateur, le numéro d'entreprise et la dénomination sociale de l'organisme de pension (un fonds de pension ou un assureur), le type de plan de pension, le statut d'affiliation (« actif » ou « dormant »), la réserve de pension (au niveau du plan de pension), la nature et la date de l'événement spécifique qui a eu lieu au cours de l'année d'évaluation et la date d'affiliation.

Renseignements relatifs au compte pension: la réserve de pension au niveau du compte, la couverture décès au niveau du compte, la garantie minimale au niveau du compte (le montant garanti à la personne affiliée lors de son départ à la retraite ou de sa sortie), le niveau de financement actuel au niveau du compte (la capacité de financement de l'organisme de pension) et la prestation attendue au niveau du compte.

Renseignements relatifs au compte pension - couverture du type « vie »: le type de couverture, l'origine des cotisations (cotisations des travailleurs, cotisations patronales, cotisations personnelles ou cotisations de la société), la formule de calcul des réserves, la base pour la capitalisation des réserves auprès de l'assureur, la base pour la capitalisation des réserves auprès du fonds de pension, les réserves acquises, la garantie minimale, le niveau de financement actuel, la prestation acquise et la prestation escomptée.

Renseignements relatifs au compte de pension - couverture de type « décès »: le type de couverture (l'indication selon laquelle le volet du compte pension a trait à une couverture en cas de décès de la personne affiliée avant sa pension), la couverture décès (le montant que percevraient les bénéficiaires en cas de décès de la personne affiliée), l'indication de l'assurance complémentaire contre le risque d'accident et l'indication de la rente d'orphelin complémentaire.

Renseignements relatifs au plan de pension interne (non gérés par un organe de pension externe): le numéro d'entreprise et la dénomination sociale de l'organisateur, le type de plan de pension, la date de validité du plan de pension, la date d'entrée en vigueur du plan de pension, la promesse de pension (l'indication selon laquelle une pension a ou non été promise dans le cadre d'un plan de pension interne) et la couverture décès promise (l'indication selon laquelle une couverture décès a ou non été promise dans le cadre d'un plan de pension interne).

4. La consultation et le traitement de ces données à caractère personnel sont soumis à deux conditions.

D'une part, il faut qu'il y ait un accord à ce propos entre la personne concernée et les établissements de crédits et les prestataires de produits et services financiers (ainsi que leurs agences et filiales). L'accord régit uniquement la relation entre ces parties et détermine notamment la finalité et la durée du traitement. Lors de la consultation et de la mise à jour des données à caractère personnel, les établissements de crédits et les prestataires de produits et services financiers (ainsi que leurs agences et filiales) vérifient toujours la validité du consentement des clients (actuels et prospectifs). Ce consentement est valable pour la période convenue avec la personne concernée ou jusqu'à son retrait explicite par la personne

concernée (dans ce cas, l'accès aux données à caractère personnel demandées cesse immédiatement d'exister).

D'autre part, il y a la relation Sigedis - citoyen - sous-traitant. Cette relation n'est pas contractuelle et est tout d'abord et principalement régie par l'autorisation n° 19/004 du 15 janvier 2019 (dont la présente demande d'autorisation constitue une précision). Cette autorisation dispose que la communication des données par Sigedis est autorisée pour autant que la première condition (l'existence d'une relation entre le citoyen et l'établissement ou le prestataire) soit et reste remplie et pour autant que le citoyen ait confirmé cette relation (selon les modalités définies dans le présent document). Pour des raisons de sécurité, l'accès aux données qui en résultent a une durée de validité maximale de deux ans.

Le demandeur observe, par ailleurs, que les données à caractère personnel relatives aux pensions complémentaires seraient, excepté par les applications des établissements et des prestataires, uniquement traitées par les conseillers financiers (en vue de la fourniture d'avis financiers aux intéressés) et par les collaborateurs des services centraux (en vue du soutien des activités commerciales de l'organisation).

B. EXAMEN

5. Il s'agit d'une communication de données à caractère personnel par une institution de sécurité sociale (l'association sans but lucratif SIGEDIS) à des tiers (les établissements de crédits, les prestataires de produits et services financiers et leurs agences et filiales) qui, en vertu de l'article 15, § 1^{er}, 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 (principe d'intégrité et de confidentialité).

Limitation des finalités

7. La communication poursuit une finalité légitime, à savoir fournir des avis financiers et formuler des propositions commerciales adéquates aux clients actuels et aux clients prospectifs, pour autant qu'ils aient donné leur consentement préalable à cet effet. Le Comité de sécurité de l'information constate que les établissements de crédits et les prestataires de produits et de services financiers (ainsi que leurs agences et filiales) souhaitent avoir recours, moyennant le consentement des personnes concernées, à certaines données à caractère personnel du réseau de la sécurité sociale, afin de pouvoir offrir efficacement leurs services. Le traitement de données à caractère personnel intervient par conséquent toujours dans le cadre d'une relation déterminée entre la personne concernée et le destinataire.
8. La consultation des données à caractère personnel doit, sans restrictions, intervenir à l'initiative de la personne concernée même et, en ce qui concerne la relation avec l'établissement ou le prestataire, avec son consentement, d'une part, et, en ce qui concerne Sigedis, après sa confirmation de l'existence de cette relation (voir infra), d'autre part. Les établissements de crédits et les prestataires de produits et de services financiers (et leurs agences et filiales) se mettent explicitement d'accord avec la personne concernée sur la portée de leur intervention et l'informent de leurs interventions éventuelles. Ils conservent les preuves du consentement de la personne concernée et les communiquent, le cas échéant, à l'association sans but lucratif SIGEDIS, à la Banque Carrefour de la sécurité sociale et au Comité de sécurité de l'information. Ils traitent les données communiquées uniquement pour la fourniture d'avis financiers et la formulation de propositions commerciales adéquates à la personne concernée. Si la personne concernée indique qu'elle ne souhaite pas accepter les propositions commerciales, les données communiquées sur la base de la présente délibération ne peuvent plus être traitées.

Minimisation des données

9. Les données à caractère personnel sont pertinentes et non excessives par rapport à cette finalité. Elles se limitent aux renseignements relatifs aux comptes de pensions complémentaires de la personne concernée et à la communication de la dernière réserve acquise connue, de la prestation acquise, de la prestation escomptée, des dates de calcul et d'évaluation y associées, du niveau de financement et des couvertures décès éventuelles et des événements pertinents.
10. Ces données à caractère personnel doivent permettre aux organisations autorisées de fournir des informations correctes à leurs clients actuels et prospectifs et de formuler, sur la base d'informations correctes et complètes, des propositions financières adéquates relatives à leur situation financière, et ce dans les limites du consentement qu'ils ont donné.

Limitation de la conservation

11. Le cas échéant, les établissements de crédits, les prestataires de produits et de services financiers et leurs agences et filiales ne conservent pas les données à caractère personnel au-delà du délai nécessaire à la réalisation des finalités en vigueur. Si les données à caractère personnel ne servent plus à la fourniture d'avis financiers et à la formulation de propositions commerciales appropriées, elles doivent être détruites.

12. Les données à caractère personnel relatives aux pensions complémentaires qui sont consultées, en ce qui concerne les établissements et les prestataires, avec le consentement de la personne concernée, et, en ce qui concerne Sigedis, après la confirmation par la personne concernée, de cette relation avec l'établissement ou le prestataire, ne sont en aucun cas conservées au-delà de l'expiration de la validité de ce consentement (par le fait que le délai convenu prend fin ou par le retrait du consentement par l'intéressé même).

Si des données à caractère personnel de clients prospectifs sont traitées, pour lesquels finalement aucune relation contractuelle n'est établie avec le prestataire de services, les données à caractère personnel peuvent néanmoins être traitées au maximum pendant un mois à compter de l'offre précontractuelle du prestataire de services.

Intégrité et confidentialité

13. L'application utilisée par les parties doit satisfaire aux mêmes standards de sécurité que ceux valables pour des applications similaires des autorités. En ce qui concerne la sécurité du login, le niveau de sécurité de l'application 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*. 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.
14. Les parties prennent des mesures organisationnelles de sorte que les données à caractère personnel puissent uniquement être traitées par l'application, les conseillers financiers (pour la fourniture d'avis financiers aux personnes concernées) et les collaborateurs des services centraux (en vue de l'appui des activités commerciales de l'organisation) qui sont spécialement désignés à cet effet et qui se sont engagés à garantir la sécurité et la confidentialité des informations. Ils tiennent une liste de ces personnes qui est actualisée en permanence à la disposition.
15. Les parties mettent en œuvre un système dans lequel la personne concernée (client actuel ou client prospectif) fait d'abord savoir, via la technologie du *Open Authorization*, qu'il existe une relation entre elle-même et le tiers. Elle peut également y consulter les relations actives et, le cas échéant, y mettre fin. Par ailleurs, elle reçoit à l'adresse mail qu'elle a enregistrée un avertissement de l'utilisation d'un accès à ses données à caractère personnel par l'application. Cela lui permet de réagir immédiatement lorsque l'accès lui paraît suspect et ne correspond pas aux relations qu'elle a avec des parties tierces.
16. Afin de garantir le respect de ce qui précède, les parties font appel à un délégué à la protection des données, tel que visé dans 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*. Elles communiquent leur identité au Comité de sécurité de l'information.

17. Les établissements de crédits et les prestataires de produits et de services financiers (et leurs agences et filiales) qui souhaitent avoir recours à la présente délibération doivent s'engager au préalable, de manière explicite, vis-à-vis du Comité de sécurité de l'information, à garantir que les traitements des données à caractère personnel de l'association sans but lucratif SIGEDIS par les collaborateurs qui sont y sont autorisés pour des raisons fonctionnelles soient conformes aux conditions prévues dans la présente délibération (en particulier à celles visées aux points 13-16) et dans la délibération n° 19/ 004 du 15 janvier 2019 (en particulier à celles prévues dans les points 8-13).
18. Ils communiquent à cet effet l'identité de leur délégué à la protection des données et joignent un questionnaire d'évaluation dûment complété relatif aux mesures de référence en matière de sécurité de l'information qui sont applicables à tout traitement de données à caractère personnel. Ce questionnaire est rempli conformément à la vérité et doit permettre d'évaluer la politique de sécurité de l'information.
19. La présente délibération entre seulement en vigueur à l'égard d'un établissement de crédits ou d'un prestataire de produits et de services financiers intéressé (et des agences et filiales respectives), pour autant que l'organisation en ait été informée explicitement par le Comité de sécurité de l'information.
20. 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 du réseau de la sécurité sociale par les établissements de crédits, par les prestataires de produits et de services financiers et par leurs agences et filiales respectives, en vue de l'octroi d'avis financiers et la formulation de propositions commerciales adéquates aux clients actuels et prospectifs, comme décrit dans la présente délibération, est autorisé moyennant le respect des mesures de protection des données 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, ainsi que les mesures visées dans la délibération n° 19/004 du 15 janvier 2019.

Tout établissement de crédits ou prestataire de produits et de services financiers concret qui souhaite faire appel à la présente délibération doit s'engager, au préalable, vis-à-vis du Comité de sécurité de l'information à garantir que les traitements de données à caractère personnel soient conformes aux conditions prévues dans la présente délibération et dans la délibération n° 19/004 du 15 janvier 2019.

Bart VIAENE

Le siège de la chambre sécurité sociale et santé du comité de sécurité de l'information est établi dans les bureaux de la Banque Carrefour de la sécurité sociale, à l'adresse suivante: Quai de Willebroeck 38 - 1000 Bruxelles
--