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

CSI/CSSS/24/456

DÉLIBÉRATION N° 24/222 DU 3 DÉCEMBRE 2024 PORTANT SUR LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL DU RÉSEAU DE LA SÉCURITÉ SOCIALE PAR UNE INSTITUTION DE SÉCURITÉ SOCIALE À UNE ORGANISATION, À UNE ENTREPRISE OU À UN PROFESSIONNEL INDIVIDUEL SUR LA BASE D'UN MANDAT ACCORDÉ PAR UNE PERSONNE PHYSIQUE

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, § 1er ;

Vu la demande des institutions de sécurité sociale concernées;

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

Vu le rapport du président.

A. OBJET

1. Il existe diverses situations où une organisation, une entreprise ou un professionnel individuel (dénommés ci-après « mandataires à titre professionnel »), dans le cadre d'une relation avec une personne physique et moyennant l'obtention d'un consentement et l'acceptation d'un mandat de cette personne, souhaite (dans le cadre de son fonctionnement, de sa prestation de services, de ses plateformes en ligne ou applications, ...) traiter des données à caractère personnel du réseau de la sécurité sociale concernant cette personne et ce en dehors du contexte d'une mission prévue par la réglementation.

2. Le Comité de sécurité de l'information a été invité à établir une série de lignes directrices générales en matière communication de données à caractère personnel du réseau de la sécurité sociale à des mandataires à titre professionnel, sur la base d'un mandat accordé par l'intéressé.

B. EXAMEN

Compétence du Comité de sécurité de l'information

3. Il s'agit d'une communication de données à caractère personnel par des institutions de sécurité sociale à des mandataires à titre professionnel, qui doit faire l'objet d'une délibération de la chambre sécurité sociale et santé du Comité de sécurité de l'information, 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,*.

Licéité du traitement

4. En vertu de l'article 6 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* (dénommé ci-après RGPD), le traitement de données à caractère personnel n'est licite que si, et dans la mesure où, au moins une des conditions mentionnées à cet article est remplie.

5. La communication précitée de données à caractère personnel est légitime en ce sens que l'intéressé, par l'octroi d'un mandat, a donné son consentement pour le traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques et que le mandataire à titre professionnel a accepté de respecter les conditions fixées dans le mandat. Sur la base du mandat, qui peut être qualifié au niveau juridique comme un contrat entre des parties, il existe donc une base juridique pour le traitement, au sens de l'article 6, 1, alinéa 1er, du RGPD,

Principes du traitement de données à caractère personnel

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 ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités (principe de limitation de la finalité), elles doivent être adéquates, pertinentes et être limitées à ce qui est nécessaire pour la finalité pour lesquelles elles sont traitées (principe de minimisation des données), elles ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (principe de limitation de la conservation) et elles doivent être traitées à l'aide de mesures techniques ou organisationnelles appropriées de façon à garantir une sécurité adéquate et à les protéger contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle (principe d'intégrité et de confidentialité).

7. Vu la nature de la demande qui lui est soumise, le Comité de sécurité de l'information ne peut se prononcer en tant que tel sur le respect des principes de limitation des finalités, de minimisation des données et de limitation de la conservation (la demande porte en effet de manière générale sur le traitement de données à caractère personnel non précisées à des fins non précisées pour les besoins de mandataires à titre professionnel).

8. La présente délibération sert par conséquent uniquement de cadre général à respecter lorsque des données à caractère personnel sont communiquées, sur la base d'un mandat de la personne concernée, par des institutions de sécurité sociale à des mandataires à titre professionnel, mais elle ne porte nullement préjudice à la compétence du Comité de sécurité de l'information de se prononcer, au cas par cas, sur de telles communications de données à caractère personnel.

9. Contrairement aux échanges de données à caractère personnel entre des acteurs du réseau de la sécurité sociale, qui sont basés sur des relations entre l'assuré social et les

institutions de sécurité sociale qui sont connues des pouvoirs publics et établies dans le répertoire des références de la Banque Carrefour de la sécurité sociale, les relations entre l'intéressé et les mandataires à titre professionnel ne sont pas connues des pouvoirs publics. Il n'est pas question d'un répertoire des références qui indique qu'une personne est cliente auprès d'une banque, d'un assureur, d'un courtier, d'une organisation de la société civile déterminé(e). Par ailleurs, les relations peuvent être limitées à une seule fois ou être 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).

10. L'intéressé est le seul à pouvoir confirmer l'existence d'une telle relation. Dans un souci de transparence, l'intéressé doit aussi avoir une vue de l'usage de ses données à caractère personnel par les mandataires à titre professionnel. Il est pourvu en un moyen simple permettant à l'intéressé d'accorder un mandat à un mandataire à titre professionnel avec lequel il a une relation de sorte que celui-ci puisse obtenir ses données à caractère personnel. L'intéressé peut à tout moment vérifier les mandats actifs enregistrés et y mettre fin s'il le souhaite.

11. Il est essentiel que la communication ait effectivement lieu sur la base d'un mandat accordé par l'intéressé dans le cadre d'une relation. La communication sur la base d'un mandat est à distinguer de la communication de données à caractère personnel nécessaires à l'exécution des missions légales.

12. La communication de données à caractère personnel dans le cadre d'une relation s'effectue moyennant un mandat standardisé accordé par l'intéressé. La portée de chaque (type de) mandat susceptible d'être accordé doit être approuvée par le Comité de sécurité de l'information dans une délibération spécifique, dans laquelle les finalités de l'échange de données à caractère personnel, le type de données à caractère personnel, la durée de conservation des données à caractère personnel et la durée de validité d'un mandat sont définis et dans laquelle il est par ailleurs précisé quelles mesures de sécurité doivent être prises lors du traitement des données. Le CSI se basera pour la délibération, le cas échéant, sur l'analyse d'impact relative à la protection des données réalisée par l'instance qui sollicite une délibération au CSI.

13. L'octroi d'un mandat s'effectue moyennant un consentement éclairé de l'intéressé. Ceci signifie que l'intéressé, lors de l'octroi du mandat, est informé par le système - dans un langage claire - des aspects suivants : la portée du mandat, l'identité du mandataire à titre professionnel, l'application d'un niveau d'authentification 400 ou supérieur dans le cadre du *Federal Authentication Service* lors de l'octroi du mandat, la possibilité de révoquer le mandat et le fait que l'octroi ou la révocation d'un mandat sont enregistrés.

14. Préalablement à toute communication de données à caractère personnel en provenance du réseau de la sécurité sociale à un mandataire à titre professionnel, le mandat doit être contrôlé. A cet effet, la Banque Carrefour de la sécurité sociale mettra à disposition un système de vérification (elle sera le responsable du traitement dans le cadre de cette application).

15. Il est interdit de traiter des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle ou l'orientation sexuelle d'une personne. C'est

la raison pour laquelle, lors de la communication de données à caractère personnel à des tiers, il convient de toujours veiller à ne pas transmettre de données à caractère personnel (sensibles) spécifiques de l'intéressé dans la demande à l'institution de sécurité sociale (sans toutefois porter préjudice au contrôle de l'existence d'une relation et de l'octroi d'un mandat). A titre d'exemple, il est fait référence au cas où une personne est affiliée à une mutualité et a accordé un mandat à cette mutualité : le Collège intermutualiste national (l'organisation qui agit comme gestionnaire du réseau secondaire des mutualités) interviendra dans le traitement de données à caractère personnel et garantira que l'institution de sécurité sociale compétente (le fournisseur des données à caractère personnel demandées) ne puisse pas retrouver l'identité de la mutualité.

16. En raison de cette exigence, la Banque Carrefour ne peut pas inclure ces informations (sensibles) spécifiques dans son système de vérification et les institutions de sécurité sociale qui disposent déjà de ces informations en tant qu'institution de gestion d'un réseau secondaire de sécurité sociale, sont tenues d'effectuer les contrôles nécessaires. Ces organisations sont les responsables du traitement respectifs en ce qui concerne l'application de leur système de vérification.

17. Chaque système de vérification doit prévoir les fonctionnalités précitées (cf. les numéros 12, 13 et 14). Le système de vérification autorise la communication de données à caractère personnel au moyen d'un token transmis à l'utilisateur ou à l'application du mandataire à titre professionnel. Dans la mesure où cela est nécessaire, l'identité du demandeur est pseudonymisée dans le token. Le token mentionne toujours des informations sur le système de vérification de sorte à ce que son authenticité puisse être vérifiée par l'institution de sécurité sociale qui fournit les données.

18. Pour des raisons de transparence, la Banque Carrefour de la sécurité sociale développe un système qui offre au citoyen un aperçu de tous les mandats actifs. Pour ce faire, l'organisation fera appel aux différents systèmes de vérification, sans que les informations des systèmes de vérification ne lui soient toutefois transmises. L'aperçu des mandats actifs concerne les mandats qui, conformément aux délibérations du Comité de sécurité de l'information, ont été accordés et qui ont été enregistrés de manière électronique dans le système, indépendamment de la manière dont ils ont été accordés.

19. Toute application d'un mandataire à titre professionnel 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 le login sécurisé, le niveau de sécurité de l'application du mandataire à titre professionnel doit satisfaire aux exigences les plus strictes en matière d'authentification (c'est-à-dire l'équivalent du niveau 400 ou supérieur au sein du *Federal Authentication Service* lorsque l'intéressé consulte ces données), à l'instar des applications des pouvoirs publics *mycareer.be* et *mypension.be*.

20. La communication de données à caractère personnel par des institutions de sécurité sociale doit s'effectuer dans le respect des normes de sécurité de l'information du réseau de la sécurité sociale (les « normes de sécurité minimales »), établies par le Comité général de coordination de la Banque Carrefour de la sécurité sociale, et le traitement

ultérieur par le mandataire à titre professionnel doit s'effectuer moyennant des garanties de sécurité équivalentes.

21. La communication doit faire l'objet d'un logging, qui reflète la répartition des tâches de sorte à pouvoir reconstituer l'ensemble de la chaîne de communication. Ce principe implique notamment des accords précis entre les instances concernées par la prestation de services électronique en ce qui concerne les aspects suivants :

- qui effectue quels authentifications, vérifications et contrôles à l'aide de quels moyens et qui en est responsable;
- comment échanger les résultats des authentifications, vérifications et contrôles entre les instances concernées par la voie électronique et de manière sécurisée;
- qui conserve quels loggings;
- comment garantir en cas d'investigation - soit à l'initiative du mandataire à titre professionnel, soit à l'initiative d'un organe de contrôle suite à un plainte ou une demande de l'intéressé - qu'un *tracing* complet (« *qui, quoi, quand, où, pourquoi ?* ») soit possible (« *quelle personne à eu recours à quel service / quelle transaction concernant quelle personne à quel moment, via quel canal et pour quelle finalité ?* »).

22. Ces accords ne peuvent pas donner lieu à la révélation inutile d'informations (sensibles) spécifiques, au sens de l'article 9 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*, auprès d'une institution de sécurité sociale, par exemple l'appartenance syndicale.

23. L'organisation ou l'entreprise qui souhaite, en tant que mandataire à titre professionnel, avoir recours aux possibilités précitées en faisant appel à une API (Application Programming Interface) à partir d'une application, devra explicitement accepter par écrit les conditions générales d'utilisation mentionnées dans le *Circle of Trust* (COT) ainsi que les conditions spécifiques d'utilisation applicables à un cas déterminé et à une série de de données à caractère personnel déterminées (tels que définies notamment dans la délibération spécifique du Comité de sécurité de l'information), préalablement à la première communication de données à caractère personnel. Par la mise en œuvre d'un COT, l'organisation ou l'entreprise s'engage à prendre les mesures nécessaires de sorte à ce que le réseau de la sécurité sociale puisse avoir confiance à tout moment que seuls des utilisateurs légitimes aient accès aux données à caractère personnel disponibles. Cet aspect ne doit alors pas être imposé dans les applications des acteurs de la sécurité sociale. Celles-ce se limitent à vérifier si l'organisation est effectivement autorisée à traiter les données à caractère personnel dans le cadre précité. L'organisation doit elle-même veiller à ce que les données à caractère personnel soient uniquement utilisées de manière légitime en son sein.

24. Lorsqu'un mandataire à titre professionnel souhaite uniquement utiliser l'application web mise à disposition par l'institution de sécurité sociale compétente, il ne doit pas signer le COT. L'utilisateur individuel doit s'authentifier à l'aide d'un moyen d'authentification de niveau 400 ou supérieur dans le cadre du *Federal Authentification Service*. Par ailleurs, l'utilisateur individuel doit être connu au sein du système de gestion des utilisateurs des organisations, des entreprises et des professionnels et il doit indiquer qu'il agit dans le

cadre de ce rôle. Le mandataire à titre professionnel accepte, dans le cas d'une organisation ou d'une entreprise via l'utilisateur individuel qui agit pour le compte de l'entreprise ou de l'organisation, préalablement à l'utilisation de l'application, les conditions générales d'utilisation ainsi que les conditions spécifiques d'utilisation applicables à une situation déterminée et à une série de données à caractère personnel déterminées (telles que définies dans la délibération spécifique du Comité de sécurité de l'information). En acceptant ces conditions d'utilisation, le mandataire à titre professionnel assume la responsabilité de l'exécution correcte du mandat et du traitement correct des données à caractère personnel de l'intéressé.

25. Le mandataire à titre professionnel 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 à caractère personnel en question ou par l'autorité de contrôle compétente.

26. Lors de la prestation de services à l'intéressé, le mandataire à titre professionnel agira dans l'intérêt de la personne concernée. Ceci signifie que le mandataire à titre professionnel ne sollicitera jamais un mandat ou ne s'accordera jamais un mandat si cela n'est pas nécessaire pour la prestation de services convenue.

27. 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 la communication de données à caractère personnel par des institutions de sécurité sociale à un mandataire à titre professionnel disposant d'une mandat de l'intéressé, telle que décrite dans la présente délibération, doit toujours être effectuée conformément aux dispositions de cette délibération.

La présente délibération constitue un cadre général qu'il y a lieu de respecter lorsque des données à caractère personnel issues du réseau de la sécurité sociale sont communiquées, sur la base d'un mandat de l'intéressé, par des institutions de sécurité sociale à un mandataire à titre professionnel, mais elle ne porte nullement préjudice à la compétence du Comité de sécurité de l'information de se prononcer, au cas par cas, sur ce type de communications de données à caractère personnel.

La délibération de la chambre sécurité sociale et santé du Comité de sécurité de l'information n° 19/004 du 15 janvier 2019 est abrogée.

La présente délibération entre en vigueur le 18 décembre 2024.

Michel DENEYER
Président