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

CSI/CSSS/26/002

DÉLIBÉRATION N° 26/002 DU 3 FÉVRIER 2026 RELATIVE AUX BONNES PRATIQUES EN MATIÈRE DE COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL ISSUES DU RÉSEAU DE LA SÉCURITÉ SOCIALE AUX MANDATAIRES NON PROFESSIONNELS SUR LA BASE D'UN MANDAT CONFÉRÉ 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 46 ;

Vu le règlement (UE) n° 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* ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* ;

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

Vu le rapport du président.

I. OBJET DE LA DEMANDE

1. Dans certaines situations, une personne physique (ci-après: l'*intéressé*) peut choisir d'autoriser une autre personne physique (ci-après le *mandataire non professionnel*) à accéder à ses données à caractère personnel dans le réseau de la sécurité sociale. Il peut s'agir par exemple d'aide offerte par un membre de la famille, un partenaire ou une personne de confiance pour l'exécution de tâches administratives ou numériques.

2. Le Comité de sécurité de l'information a été invité à établir une série de lignes directrices générales relatives à la communication de données à caractère personnel du réseau de la sécurité sociale à des mandataires non professionnels, sur la base d'un mandat conféré par la personne concernée dans le cadre de l'offre d'une aide.

II. COMPÉTENCE

3. En vertu de l'article 46, § 1er, de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, la chambre sécurité sociale et santé du Comité de sécurité de l'information peut formuler les bonnes pratiques qu'elle juge utiles pour l'application et le respect de la présente loi et de ses mesures d'exécution et des dispositions fixées par ou en vertu de la loi visant à la protection de la vie privée à l'égard des traitements de données à caractère personnel relatives à la sécurité sociale.

4. Le Comité de sécurité de l'information s'estime par conséquent compétent pour formuler des bonnes pratiques déterminant le cadre de l'échange d'informations comme défini dans le présent document.

III. BONNES PRATIQUES

5. 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,* 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.

6. La communication précitée de données à caractère personnel par des institutions de sécurité sociale 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 non-professionnel a accepté de respecter les conditions fixées dans le mandat. Sur la base du mandat, qui peut être qualifié au niveau juridique de contrat entre des parties, il existe donc une base juridique pour le traitement.

7. Le mandat conféré concerne une représentation immédiate – comme défini à l'article 1.8 du Code civil – de l'intéressé par un mandataire non professionnel (il y a représentation immédiate lorsqu'une personne est habilitée à accomplir un acte juridique avec un tiers au nom et pour le compte d'une autre personne).

8. Les présentes bonnes pratiques constituent un cadre général à respecter lorsque des données à caractère personnel sont communiquées, sur la base d'un mandat de l'intéressé, par des institutions de sécurité sociale à des mandataires non professionnels dans le cadre d'une offre d'aide à l'intéressé. Pour le surplus, elles ne portent toutefois 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 les acteurs du réseau de la sécurité sociale, qui sont basés sur des relations entre les institutions de sécurité sociale et l'assuré social qui sont connues des autorités (telles qu'elles sont enregistrées dans le répertoire des références de la Banque Carrefour de la sécurité sociale), les relations entre l'intéressé et les mandataires non professionnels ne sont pas connues des autorités.

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 non-professionnels. Il est pourvu en un moyen simple permettant à l'intéressé d'accorder un mandat à un mandataire non-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 de données à caractère personnel ait effectivement lieu sur la base d'un mandat accordé par l'intéressé dans le cadre d'une relation avec le mandataire non professionnel. Une telle communication de données à caractère personnel est à distinguer de la communication de données à caractère personnel nécessaires à l'exécution des missions réglementaires.

12. La communication de données à caractère personnel dans le cadre d'une relation s'effectue moyennant un mandat standardisé accordé par l'intéressé. Le modèle de mandat standard est fixé par le Comité de sécurité de l'information et comprend les catégories de données concernées, les fonctionnalités proposées, la durée du mandat et une description des finalités pour lesquelles le mandat est conféré. A la lumière de ceci, le Comité de sécurité de l'information peut, le cas échéant, définir des mesures techniques de protection supplémentaires.

13. Le mandat ne doit pas nécessairement se limiter à une seule application du portail de la sécurité sociale. Le mandat soutient le mandataire non professionnel dans l'aide offerte à l'intéressé. Un mandat peut donc concerner plusieurs applications dans la mesure où celles-ci correspondent, au niveau thématique, à l'aide offerte.

14. 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 clair - des aspects suivants : la portée du mandat, l'identité du mandataire non 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.

15. Préalablement à toute communication de données à caractère personnel en provenance du réseau de la sécurité sociale à un mandataire non 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).

16. Dans un souci de transparence, la Banque Carrefour de la sécurité sociale développe un système qui offre au citoyen un aperçu de tous les mandats actifs. L'aperçu des mandats actifs concerne les mandats qui ont été accordés conformément aux bonnes pratiques formulées par le Comité de sécurité de l'information et qui ont été enregistrés de manière électronique dans le système, indépendamment de la manière dont ils ont été accordés.

17. La communication de données à caractère personnel doit faire l'objet d'un logging et les acteurs doivent procéder à une répartition des tâches précise permettant de reconstituer la totalité de la chaîne de communication de données à caractère personnel. Ceci implique notamment des accords précis entre les acteurs concernés 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 entre les acteurs, de manière sécurisée par la voie électronique, les résultats des authentifications, vérifications et contrôles ;

- qui conserve quels loggings ;

- comment garantir en cas d'investigation - soit par un organe de contrôle, soit à la demande de l'intéressé - qu'un tracing complet (« qui, quoi, quand, où, pourquoi ? ») soit possible (« quelle personne a eu recours à quel service / quelle transaction concernant quelle personne à quel moment, via quel canal et pour quelle finalité ? »).

18. Lorsqu'un mandataire non professionnel souhaite utiliser l'application web mise à la disposition par l'institution de sécurité sociale compétente, il doit s'authentifier par un moyen d'authentification du niveau d'authentification 400 ou supérieur au sein du *Federal Authentication Service*. Le mandataire non professionnel accepte, préalablement à l'utilisation de l'application, les conditions d'utilisation et s'engage à respecter les bonnes pratiques et les éventuelles mesures supplémentaires imposées en application du point 12. Le mandataire non professionnel est tenu à cet égard, d'une part, de poursuivre uniquement les objectifs prévus dans le mandat et, d'autre part, de refuser sans plus le mandat lorsque l'utilisation de ce mandat engendrerait un conflit d'intérêts ou lui permettrait d'en tirer un avantage personnel, que ce soit ou non au détriment de l'intéressé. En acceptant ces conditions d'utilisation, le mandataire non professionnel assume la responsabilité de l'exécution correcte du mandat.

19. Lorsqu'un mandataire non professionnel ne respecte pas les conditions du mandat, il est automatiquement considéré comme un responsable du traitement pour les données à caractère personnel reçues et il est soumis aux règles imposées 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*.

20. Lorsqu'il offre son aide à l'intéressé, le mandataire non professionnel agit dans l'intérêt de la personne concernée. Ceci signifie que le mandataire non professionnel ne sollicitera jamais un mandat ou ne s'accordera jamais un mandat si cela n'est pas nécessaire pour l'offre d'aide convenue.

21. Le mandataire non 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.

22. Le traitement de données à caractère personnel issues du réseau de la sécurité sociale est effectué, pour le surplus, dans le respect 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 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.*

IV. CONCLUSION

23. 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 des mandataires non professionnels disposant d'un mandat de l'intéressé, telle que décrite dans la présente délibération, doit toujours être effectuée conformément aux bonnes pratiques formulées.

24. Ces bonnes pratiques constituent 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 non professionnel dans le cadre d'une relation, mais elles ne portent 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 présente délibération entre en vigueur le 18 février 2026.

Michel DENEYER
Président