

**Comité de sécurité de l'information
Chambres réunies**

DELIBERATION N° 25/003 DU 4 MARS 2025 RELATIVE A LA COMMUNICATION DE DONNEES A CARACTERE PERSONNEL ISSUES DU REGISTRE CENTRAL DES INTERDICTIONS DE GERER PAR LE SERVICE PUBLIC FEDERAL JUSTICE A L'OFFICE NATIONAL DE SECURITE SOCIALE DANS LE CADRE DE L'EXECUTION DE SES MISSIONS LEGALES D'INSPECTION

Vu la 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, § 1er, alinéa 3 ;

Vu la demande de l'Office national de sécurité sociale;

Vu le rapport d'auditorat du SPF BOSA ;

Vu le rapport du président

I. OBJET DE LA DEMANDE

1. La présente délibération concerne la communication de données à caractère personnel issues du Registre central des interdictions de gérer par le Service public fédéral Justice (SPF Justice) à l'Office national de sécurité sociale (ONSS) en vue de l'exécution de ses missions d'inspection déterminées par la loi.
2. Par la loi du 4 mai 2023, un Registre central des interdictions de gérer a été créé sous la responsabilité du SPF Justice. Il s'agit d'un système de traitement automatisé tenu sous l'autorité du ministre de la Justice, qui assure, conformément aux dispositions de la présente loi, l'enregistrement, la conservation et la modification des données concernant les décisions rendues à propos de personnes auxquelles une interdiction de gérer est imposée. (art. 3) La finalité du Registre central des interdictions de gérer est la mise à disposition des données qui y sont enregistrées afin de permettre aux services publics et aux tiers de vérifier si les administrateurs, gérants, commissaires, délégués à la gestion journalière, membres d'un comité ou conseil de direction ou d'un conseil de surveillance ou liquidateurs d'une personne morale, les représentants pour l'activité de la succursale ou les candidats à la nomination dans de telles fonctions ne sont pas frappés d'une interdiction d'exercer ces fonctions. (art. 5)
3. Sont inscrites dans le Registre central des interdictions de gérer :
 - 1° l'interdiction d'exercer une activité ou une fonction conformément aux articles 1er, 1erbis et 2 de l'arrêté royal n° 22 du 24 octobre 1934 relatif à l'interdiction judiciaire faite à certains condamnés et faillis d'exercer certaines fonctions, professions ou activités ;

2° l'interdiction d'exercer une activité ou une fonction conformément à l'article 3quater de l'arrêté royal n° 22 du 24 octobre 1934 relatif à l'interdiction judiciaire faite à certains condamnés et faillis d'exercer certaines fonctions, professions ou activités, et l'interdiction aux faillis, ou personnes assimilées, d'exercer certaines fonctions, professions ou activités conformément à l'article XX.229 du Code de droit économique.

4. L'inscription des interdictions de gérer contient les données suivantes :
- 1° le prénom, le nom, la date et le lieu de naissance de la personne condamnée, ou, lorsqu'il s'agit d'une personne morale, sa dénomination, sa forme légale et son numéro d'entreprise ; le condamné qui dispose d'un numéro du registre national ou auquel un numéro d'identification du registre bis a été attribué en application de l'article 4, § 2, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, est en outre désigné avec ce numéro ;
 - 2° l'indication du juge ou du tribunal qui a prononcé la décision ; la mention et la date du prononcé en audience publique ;
 - 3° la date de début et de fin de l'interdiction ;
 - 4° le cas échéant, la dénomination et le numéro d'entreprise de la personne morale pour laquelle le condamné agissait ;
 - 5° les motifs de l'interdiction.

5. Les données suivantes du Registre central des interdictions de gérer sont disponibles via Internet jusqu'à l'expiration du délai de l'interdiction de gérer :
- 1° le prénom et le nom de la personne condamnée ou, s'il s'agit d'une personne morale, la dénomination, la forme légale et le numéro d'entreprise ;
 - 2° la date de début et de fin de l'interdiction.

Les données relatives aux décisions visées à paragraphe 3, 2°, sont disponibles via Internet pour les membres du grand public. Les données relatives aux décisions visées à paragraphe 3, 1°, sont disponibles via Internet uniquement après l'identification électronique au moyen d'une carte d'identité électronique ou des moyens d'authentification spécifiques. ; l'utilisation du numéro de registre national est autorisée à cette fin.

6. La loi du 4 mai 2023 précitée prévoit également un accès aux données du Registre central des interdictions de gérer pour les instances (publiques) expressément mentionnées dans la loi, qui requièrent la connaissance de ces données dans le cadre de leurs missions prévues par la loi, y compris les agents de niveau A de l'Office national de Sécurité sociale, nommément désignés par écrit. Les agents de niveau A peuvent déléguer cette faculté à une ou plusieurs personnes qui relèvent de leur autorité, désignées nommément et par écrit. Les modalités d'accès doivent faire l'objet d'un protocole d'accord au sens de l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel entre le responsable du traitement du Registre central des interdictions de gérer et le demandeur.

Ce protocole contient également les mesures appropriées pour protéger les droits et libertés des personnes concernées dont notamment celles relatives :

- 1° à la journalisation des accès ;
- 2° à l'obligation d'être tenu au secret professionnel ou au devoir de confidentialité ;
- 3° aux mesures techniques et organisationnelles relatives à la gestion des accès.

La journalisation des accès doit au minimum permettre d'établir qui a eu accès quand, à quelles données, à partir de quel poste et pour quelles finalités l'accès a été réalisé.

L'identité des auteurs de toute demande de consultation du Registre central des interdictions de gérer est enregistrée dans un système de contrôle. Ces informations sont conservées pendant six mois.

7. En exécution de la loi précitée du 4 mai 2023, le SPF Justice et l'ONSS ont conclu, en date du 9 décembre 2024, un protocole concernant la communication de certaines données à caractère personnel issues du Registre central des interdictions de gérer.
8. L'ONSS vise la communication des données suivantes en vue de l'exécution de ses missions légales :
 - Le numéro de registre national ou le numéro bis de la personne concernée ;
 - Les données relatives à l'interdiction de gérer, à savoir :
 - o la date de début et la date de fin de l'interdiction de gérer ;
 - o le cas échéant, la dénomination et le numéro d'entreprise de la personne morale pour laquelle le condamné agissait ;
 - o les motifs de l'interdiction de gérer (cf. point 3 de la présente délibération).
9. L'utilisation du numéro de registre national comme moyen d'identification par l'ONSS dans le cadre de l'accomplissement des missions qui, dans les limites des législations dont elle assure l'application, relèvent de ses compétences, ainsi que pour l'exécution des missions qui lui sont imposées par ou en vertu d'une disposition légale ou réglementaire relative à la sécurité sociale, est expressément autorisée par l'arrêté royal du 5 décembre 1986 *régulant l'utilisation du numéro d'identification du Registre national des personnes physiques par les organismes d'intérêt public relevant du Ministère de la Prévoyance sociale*.
10. L'ONSS est responsable des missions essentielles suivantes (telles que déterminées, entre autres, par les articles 5 et 8/8 de la loi du 27 juin 1969 portant révision de l'arrêté-loi du 28 décembre 1944 concernant la sécurité sociale des travailleurs) :
 - l'encaissement correct et en temps voulu des cotisations sociales ;
 - la collecte et le contrôle des données relatives aux salaires et au temps de travail ;
 - l'accompagnement des employeurs et des prestataires de services sociaux dans leurs déclarations ;
 - le financement du système de sécurité sociale ;
 - le soutien de la politique régionale en matière de groupes cibles par la perception des cotisations ;
 - la gestion de la sécurité sociale des marins, des expatriés et du Fonds social Maribel.
11. Outre le contrôle des déclarations des employeurs, l'ONSS détecte également la fraude sociale, et les missions en matière de lutte contre la fraude, ainsi que le contrôle et la gestion des risques, revêtent une importance particulière.
 - Lutte contre la fraude : Il s'agit de l'une des priorités du gouvernement fédéral, et l'ONSS y joue un rôle clé. L'ONSS contribue à la détection, au contrôle et à la lutte contre la fraude et les abus. L'attention est portée sur trois types de risques :
 - le non-paiement des cotisations sociales ;

- la violation de la législation en matière de sécurité sociale ;
- la détection du dumping social et d'autres abus transfrontaliers (traite des êtres humains).
- Contrôle des risques : L'ONSS effectue également des contrôles. Ces contrôles fréquents sont organisés dans différentes entreprises et secteurs. Sur la base de certaines actions ou à la suite d'une plainte, les inspecteurs sociaux se rendent sur place afin de mettre en évidence d'éventuels cas de fraude.
- Gestion des risques :
Dès qu'une fraude sociale est constatée, l'ONSS mobilise des moyens pour permettre un recouvrement. À cette fin, l'ONSS travaille en étroite collaboration avec les instances judiciaires, ce qui lui permet de :
 - procéder à des saisies et, si nécessaire, à des citations à comparaître à court terme ;
 - effectuer des saisies-arrêts sur des comptes et avoirs financiers ;
 - établir la responsabilité solidaire et conjointe du véritable responsable ;
 - engager des procédures correctionnelles.

12. Conformément au Code pénal social, les inspecteurs sociaux, notamment ceux de l'ONSS, doivent :

- exécuter le plan stratégique et le plan d'action opérationnel pour la lutte contre la fraude sociale, le travail illégal et le dumping social (art. 2) ;
- recueillir des renseignements et procéder à toute enquête, tout contrôle et toute audition, ainsi qu'obtenir toutes les informations qu'ils jugent nécessaires afin de s'assurer que les dispositions de la législation dont ils assurent le contrôle sont effectivement respectées (art. 25) ;
- demander à d'autres administrations de leur communiquer des informations.

L'article 55 du Code pénal social stipule à cet égard que sans préjudice de l'article 44/1 de la loi du 5 août 1992 sur la fonction de police, [...] tous les services de l'État, y compris les parquets et les greffes des cours et de toutes les juridictions, les provinces, les communes, les associations auxquelles elles appartiennent, les établissements publics qui en dépendent, ainsi que tous les établissements publics et institutions coopérantes de sécurité sociale, sont tenus de fournir aux inspecteurs sociaux, à leur demande, toutes les informations qu'ils jugent utiles pour contrôler le respect de la législation dont ils ont la charge, ainsi que de présenter à leur consultation tout support d'information et d'en fournir des copies sous quelque forme que ce soit.

13. En ce qui concerne l'accès aux données du Registre central des interdictions de gérer, l'ONSS souhaite, dans le cadre des enquêtes menées sur la base de la loi du 6 juin 2010 introduisant le Code pénal social, être en mesure de vérifier que l'employeur faisant l'objet de l'enquête n'est pas soumis à une interdiction de gérer, d'en faire la déclaration lorsqu'il est constaté qu'il poursuit ses activités ou crée une autre société malgré l'interdiction, ainsi que d'identifier les différentes entités liées à une personne faisant l'objet d'une enquête, afin de constituer un dossier complet sur la fraude sociale commise.

14. Lorsque l'ONSS engage une action en responsabilité contre un gérant, il souhaite pouvoir consulter ce registre afin de renforcer son argumentation si la personne concernée y figure, ainsi que de vérifier l'exactitude des données par cette consultation.
15. La communication des données par le SPF Justice se fera selon les principes de l'intégration des services, tels que définis par la loi du 15 août 2012 portant création et organisation d'un intégrateur de services fédéral (avec l'intervention du SPF BOSA) et par la loi du 15 janvier 1991 portant création et organisation d'une banque-carrefour de la sécurité sociale (avec l'intervention de la BCSS).
16. L'accès par l'ONSS est demandé pour une durée indéterminée, les consultations étant effectuées de manière ponctuelle en fonction de la réalisation des enquêtes menées par les inspecteurs sociaux concernés dans le cadre de l'exécution de leurs missions légales.

II. TRAITEMENT DE LA DEMANDE

A. COMPETENCE DU COMITE

17. Conformément à l'article 35/1, §1, troisième alinéa, de la loi du 15 août 2012 portant création et organisation de l'intégrateur de services fédéral, 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°, a), 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, dans la mesure où les responsables du traitement de l'instance qui communique, de l'instance destinatrice et de la Banque-carrefour de la sécurité sociale ne parviennent pas, en exécution de l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, à un accord concernant la communication ou au moins un de ces responsables du traitement demande une délibération et en a informé les autres responsables du traitement.
18. Le Comité de sécurité de l'information constate qu'une demande a été introduite sur la base d'un protocole conclu entre le SPF Justice et l'ONSS. Étant donné que ce protocole n'a pas été conclu par la BCSS, le comité se considère compétent pour se prononcer sur la demande.

B. QUANT AU FOND

B.1. RESPONSABILITE

19. Conformément à l'article 5.2 du règlement général sur la protection des données¹, ci-après 'RGDP', le SPF Justice (l'instance qui communique les données) et l'ONSS (l'instance qui reçoit les données) – en tant que responsables du traitement – sont responsables du respect des principes énoncés à l'article 5, paragraphe 1, du RGPD et doivent être en mesure de le démontrer².

¹ 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.

² Les données à caractère personnel doivent être:

B.2. LICEITE

20. 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.
21. Le Comité constate que la communication des données à caractère personnel est légitime, car elle est nécessaire pour satisfaire à une obligation légale incombant aux SPF Justice et l'ONSS en tant que responsables du traitement (art. 6, 1, c) du RGPD). En effet, l'article 11 de la loi du 4 mai 2023 relative au Registre central des interdictions de gérer prévoit expressément que les fonctionnaires de l'ONSS ont accès au Registre central dans le cadre de leurs missions légales pour lesquelles la connaissance des données issues du Registre central des interdictions de gérer est requise. Les missions de l'ONSS sont expressément définies par diverses législations, notamment la loi du 27 juin 1969 portant révision de l'arrêté-loi du 28 décembre 1944 relative à la sécurité sociale des travailleurs. Les services d'inspection exercent en outre leurs missions d'inspection et de contrôle conformément aux dispositions du Code pénal social.
22. Le Comité de sécurité de l'information rappelle que, conformément à l'article 10 du RGPD, les données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes ne peuvent être traitées, sur la base de l'article 6, paragraphe 1, du RGPD, que sous le contrôle de l'autorité publique ou si le traitement est autorisé par le droit de l'Union ou le droit national, qui doit prévoir des garanties appropriées pour les droits et libertés des personnes concernées. Les registres complets des condamnations pénales ne peuvent être tenus que sous le contrôle de l'autorité publique. Le Comité de sécurité de l'information prend acte du fait que la création du Registre central des interdictions de gérer, ainsi que la communication envisagée et le traitement ultérieur des données issues de ce registre, sont réalisés sous le contrôle et la responsabilité des services publics fédéraux concernés.

-
- a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);
 - b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; 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, comme incompatible avec les finalités initiales (limitation des finalités);
 - c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);
 - d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);
 - e) 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; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);
 - f) 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).

B.3. LIMITATION DE FINALITES

23. Article 5.1 b) RGPD ne permet le traitement de données à caractère personnel que pour des fins déterminées, explicites et légitimes. En outre, les données ne peuvent pas faire l'objet d'un traitement ultérieur d'une manière incompatible avec ces objectifs.
24. La communication a pour objectif de permettre à l'ONSS d'exécuter ses missions d'inspection. Dans le cadre des enquêtes menées par l'ONSS sur la base de la loi du 6 juin 2010 introduisant le Code pénal social, celle-ci souhaite être en mesure de vérifier que l'employeur n'est pas soumis à une interdiction de gérer, d'en faire la déclaration lorsqu'il est constaté qu'il poursuit ses activités ou crée une autre société, ainsi que d'identifier les différentes entités liées à une personne faisant l'objet d'une enquête, afin de constituer un dossier complet sur la fraude sociale commise. Lorsque l'ONSS engage une action en responsabilité contre un gérant, elle souhaite pouvoir consulter ce registre afin de renforcer son argumentation si la personne concernée y figure, ainsi que de vérifier l'exactitude des données en sa possession grâce à cette consultation.
25. Le Comité estime que la communication des données envisagées poursuit un objectif déterminé, explicitement défini et légitime au regard des éléments précités. Il rappelle que les données demandées ne peuvent être traitées qu'exclusivement à ces fins.

B.4. PRINCIPE DE PROPORTIONNALITE

B.4.1. Minimisation de données

26. L'article 5.1 c) 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.
27. L'ONSS justifie le traitement des données à caractère personnel envisagées comme suit :
 - Le numéro de registre national / numéro Bis : Il s'agit des données nécessaires à l'identification de la personne concernée, permettant de vérifier l'identité des personnes soumises à une interdiction de gérer. L'ONSS a été autorisé à utiliser le numéro de registre national par l'arrêté royal du 5 décembre 1986.
 - Données relatives à l'interdiction de gérer (la date de début et de fin de l'interdiction, le cas échéant la dénomination et le numéro d'entreprise de la personne morale pour laquelle le condamné agissait, ainsi que le motif de l'interdiction) : Ces données sont indispensables pour l'exercice de la mission d'inspection.
28. Dans le cadre de l'accès aux données précitées, il est envisagé une consultation de la situation actuelle au moment de la recherche, ainsi que des modifications et de l'historique jusqu'à dix ans avant la recherche. L'historique est indispensable pour l'exécution des missions d'inspection et d'éventuelles procédures judiciaires, en tenant compte des délais de prescription en cours.
29. Conformément à l'article 11, 5° de la loi précitée du 4 mai 2023, l'accès est exclusivement accordé aux agents de niveau A de l'Office national de sécurité sociale, désignés nominativement et par écrit. Ceux-ci peuvent toutefois déléguer cette compétence à une ou plusieurs personnes également désignées nominativement et par écrit, placées sous leur autorité, comme le prévoit l'article 11, alinéa 3 de la loi précitée du 4 mai 2023.

30. Le cas échéant, les données reçues peuvent être communiquées aux instances judiciaires compétentes en cas d'engagement d'une procédure judiciaire.

B.4.2. Limitation de conservation

31. 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 strictement nécessaire aux finalités pour lesquelles elles sont traitées.
32. Le Comité de sécurité de l'information prend acte du fait que les données reçues sont conservées en tenant compte des exigences relatives à l'application de la récidive et à la révocation d'une suspension accordée, avec une durée de conservation maximale d'un an après la prescription de toutes les créances relevant de la compétence de l'ONSS ou, le cas échéant, après le paiement intégral de tous les montants y afférents.

B.5. TRANSPARANCE

33. Conformément à l'article 14 du Règlement général sur la protection des données (RGPD), le responsable du traitement est tenu de fournir à la personne concernée certaines informations relatives au traitement des données à caractère personnel qui ne sont pas obtenues auprès de cette dernière. Ces informations ne sont toutefois pas requises si l'obtention ou la communication des données est expressément prescrite par le droit de l'Union ou le droit national applicable au responsable du traitement, et que ce droit prévoit des mesures appropriées pour protéger les intérêts légitimes de la personne concernée (art. 14.5 du RGPD). À cet égard, il convient de se référer à l'article 11 de la loi précitée du 4 mai 2023, qui prévoit expressément la possibilité de communiquer les données à caractère personnel concernées à l'ONSS, dans la mesure où ces données sont nécessaires à l'exécution de ses missions légales.
34. Le Comité de sécurité de l'information constate que la réglementation applicable prévoit effectivement des mesures appropriées pour protéger les intérêts légitimes de la personne concernée. Les parties impliquées sont donc dispensées de l'obligation de notification aux personnes concernées.

B.6. SECURITE ET CONFIDENTIALITE

35. Conformément à l'art. 5.1 f) du RGPD, les données personnelles doivent être traitées de manière à assurer une sécurité appropriée par la mise en place de mesures techniques ou organisationnelles, afin de les protéger notamment contre tout traitement non autorisé ou illicite, ainsi que contre toute perte, destruction ou détérioration accidentelle.
36. Selon l'art. 24 du RGPD, les responsables du traitement, en tenant compte de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques de probabilité et de gravité variables pour les droits et libertés des personnes physiques, doivent prendre des mesures techniques et organisationnelles appropriées pour garantir et pouvoir démontrer que le traitement est conforme au règlement.
37. Le SPF Finances dispose d'un délégué à la protection des données et d'un plan de sécurité. Il convient également de se référer à la loi du 3 août 2012 contenant des dispositions relatives au traitement des données à caractère personnel par le Service public fédéral Finances dans le cadre de ses missions. Le Comité de sécurité de l'information prend acte du fait que le

délégué à la protection des données du SPF Finances a rendu un avis positif concernant la communication envisagée.

- 38.** Le Comité de sécurité de l'information prend également acte du fait que l'ONSS a désigné un délégué à la protection des données et que ce dernier a également émis un avis positif concernant la communication des données envisagée.
- 39.** L'ONSS fait partie du réseau étendu de la sécurité sociale et est donc soumis à l'arrêté royal du 12 août 1993 portant organisation de la sécurité de l'information dans les institutions de sécurité sociale. Cela signifie qu'il dispose d'un délégué à la protection des données et d'un plan de sécurité précisant l'ensemble des moyens nécessaires à sa mise en œuvre. Il doit en outre rapporter chaque année au Comité de gestion de la Banque-Carrefour de la Sécurité Sociale (BCSS).
- 40.** Le Comité de sécurité de l'information prend acte du fait que, conformément à l'article 11, quatrième alinéa, de la loi précitée du 4 mai 2023, un système de journalisation (logging) est prévu pour enregistrer :
 - Qui a accédé au registre ;
 - Quand cet accès a eu lieu ;
 - Quelles données ont été consultées ;
 - Depuis quel poste l'accès a été effectué ;
 - À quelles fins l'accès a été réalisé.

Ces données de journalisation sont conservées pendant six mois, comme déterminé explicitement par la loi précitée du 4 mai 2023.

- 41.** Le Comité de sécurité de l'information prend acte du fait que toutes les personnes ayant accès aux données à caractère personnel concernées sont soumis à une obligation de confidentialité, soit statutaire, soit légale.
- 42.** Le Comité de sécurité de l'information prend acte du fait que tant la Banque-Carrefour de la Sécurité Sociale (BCSS), en sa qualité d'intégrateur de services du secteur de la sécurité sociale, que le SPF BOSA, en sa qualité d'intégrateur de services fédéral, interviennent pour l'accès sécurisé aux données. Ils assurent ainsi l'échange sécurisé des données à caractère personnel.
- 43.** Enfin, le Comité de sécurité de l'information souligne que la mise en place de mesures techniques et organisationnelles n'a de sens que si celles-ci sont effectivement mises en œuvre et garantissent l'intégrité et la confidentialité des données à caractère personnel.

Pour ces raisons,

les chambres réunies du comité de sécurité de l'information décident :

Que la communication de données à caractère personnel issues du Registre central des interdictions de gérer par le Service public fédéral Justice à l'Office national de sécurité sociale, dans le cadre de l'exécution de ses missions légales d'inspection, telle que décrite dans la présente délibération, est autorisée, à condition que soient respectées les mesures de protection des données établies dans cette délibération, en particulier les mesures relatives à la limitation des finalités, la minimisation des données, la limitation de la conservation et la sécurité de l'information.

La présente délibération entre en vigueur le 19 mars 2025.

Michel DENEYER
Président

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, Quai de Willebroeck 38, 1000 Bruxelles, et le siège de la chambre Autorité fédérale du Comité de sécurité de l'information est établi dans les bureaux du SPF BOSA, Avenue Simon Bolivar 30, 1000 Bruxelles.