

**Comité de sécurité de l'information
chambres réunies
(sécurité sociale et santé/autorité fédérale)**

DELIBERATION N° 24/001 DU 6 FEVRIER 2024 RELATIVE A LA COMMUNICATION DES DONNEES A CARACTERE PERSONNEL PAR LA BANQUE CARREFOUR DES ENTREPRISES DU SPF ECONOMIE A L'OFFICE NATIONAL DE SECURITE SOCIALE EN VUE DE L'IDENTIFICATION UNIVOQUE DES ENTITES ENREGISTREES ET POUR DETERMINER QUI EXERCE DES FONCTIONS RESPONSABLES CONCERNANT CES ENTITES ENREGISTREES, DANS LE CADRE DE L'EXERCICE DES MISSIONS LEGALES D'INSPECTION SOCIALE

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* ;

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, § 1^{er}, alinéa 3;

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

Vu le rapport d'auditorat du SPF BOSA ;

Vu le rapport de monsieur B. VIAENE et monsieur D. HACHE ;

A. OBJET DE LA DEMANDE

1. L'Office national de sécurité sociale (ci-après "ONSS") souhaite la communication des données à caractère personnel par la Banque Carrefour des Entreprises du SPF Economie (ci-après "BCE") en vue de l'identification unique des entités enregistrées et de déterminer qui exerce les fonctions responsables à l'égard de ces entités enregistrées, dans le cadre de l'exercice des missions légales relatives à l'inspection sociale.
2. La BCE est gérée par le SPF Economie. Il centralise les données de base des entreprises et de leurs unités d'établissement respectives, les diffuse aux administrations compétentes et attribue un numéro d'identification unique à chaque acteur. Les détails de son fonctionnement sont décrits dans le livre III «Liberté d'établissement, de prestation de service et obligations générales des entreprises» du Code de droit économique. L'accès aux données de la BCE peut être accordé aux autorités, administrations, services ou autres instances pour

autant que ces données soient nécessaires à l'exécution de leurs missions légales ou réglementaires.

3. Les informations envisagées relatives entreprises inscrites à la CBE sont nécessaires pour que l'ONSS puisse accomplir les missions légales qui relèvent de sa compétence, en vue de la perception et du recouvrement des cotisations de sécurité sociale dues, et en vue de la prévention, de la détermination, de la poursuite et de la sanction des éventuelles infractions, en ce qui concerne le service d'inspection de l'ONSS. L'ONSS vérifie si les employeurs signalent correctement leurs employés et recherche activement les phénomènes de fraude (et d'autres formes possibles d'abus et d'exploitation).
4. L'une des missions légales de l'Inspection de l'ONSS est de contrôler le respect de la législation sociale sur la base des dispositions contenues dans le livre 1, titre 2 du Code pénal social :
 - Dans l'exercice de leurs fonctions, les inspecteurs sociaux peuvent, à toute heure du jour et de la nuit, sans préavis, pénétrer librement dans tous les ateliers ou autres lieux soumis à leur surveillance ou dans lesquels ils peuvent raisonnablement suspecter la présence de personnes. sont soumis aux dispositions de la législation qu'ils contrôlent. Ils peuvent également procéder à toute enquête, inspection ou interrogatoire, ainsi qu'obtenir toutes informations qu'ils estiment nécessaires pour s'assurer que les dispositions de la législation qu'ils contrôlent sont effectivement respectées.
 - Tous les services de l'Etat sont tenus, vis-à-vis des inspecteurs sociaux et à leur demande, de leur fournir tous renseignements que ces derniers estiment utiles au contrôle du respect de la législation dont ils sont chargés, ainsi que de leur produire, pour en prendre connaissance, tous les supports d'information et de leur en fournir des copies sous n'importe quelle forme.
5. L'ONSS a besoin des informations décrites ci-dessous afin de :
 - obtenir les données des entités enregistrées, dont la base de données BCE est la seule source authentique ;
 - détecter certains phénomènes de fraude se manifestant dans des réseaux d'entreprises liées entre elles par des détenteurs de fonctions, des adresses, etc. ;
 - croiser les données reçues de la BCE dans son entrepôt de données avec les sources de données de l'ONSS afin d'établir des modèles de risques pour la détection et la lutte contre la fraude sociale et/ou le non-paiement correct des cotisations sociales.
6. Conformément à la possibilité légale prévue par la loi du 15 janvier 1990 portant création et organisation d'une banque-carrefour de la sécurité sociale, les données reçues concernant les entreprises seront intégrées dans un entrepôt de données (datawarehouse) permettant à l'ONSS d'effectuer des processus de fouille de données (datamining) et d'association de données (datamatching), y compris le profilage au sens de l'article 4, 4) du règlement général sur la protection des données.

7. L'ONSS donne l'exemple suivant : la fraude au paiement est fréquente chez les entreprises liées entre elles par des détenteurs de fonctions et un pool d'employés. Pour détecter plus rapidement cette fraude et identifier l'organisateur, il est nécessaire de cartographier le réseau des entreprises utilisées (sur papier) et de croiser les données sur leurs détenteurs de fonctions avec d'autres données internes disponibles telles que l'emploi et les dettes sociales. Sur la base d'une analyse business et avec la contribution d'experts du domaine, des indicateurs sont déterminés pour ce type de construction frauduleuse. Ces données sont ensuite rassemblées et croisées à l'aide d'un langage de programmation qui transforme les modèles dans les données (conformément aux indicateurs) en informations utiles, consultables via des fichiers de résultats. Ces fichiers de résultats sont mis à la disposition des inspecteurs sociaux et des gestionnaires de dossiers des services concernés de l'ONSS.
8. Afin de réaliser les finalités mentionnés, la communication des catégories de données suivantes est envisagée, concernant toutes les entités enregistrées dans la BCE, y compris les données historiques remontant jusqu'à 10 ans :
- “**Activities**” : Cette catégorie comprend un résumé des activités (codes NACE) de l'entité enregistrée. Il existe différents types d'activités dans la BCE, chacun étant initié et géré par une administration spécifique.¹
 - “**Adresses**” : Cette catégorie comprend les coordonnées postales des entités enregistrées. Cette adresse peut être l'adresse du siège social ou (pour une entreprise personne physique) l'adresse de domicile.²
 - “**Authorizations, Permissions, Professions**” : Cette catégorie englobe les différentes qualités sous lesquelles l'entité enregistrée est connue (telles que assujettie à la TVA, employeur), les autorisations (reconnaisances, permis, licences,...) accordées par l'administration à l'entité enregistrée, et les compétences entrepreneuriales éventuelles que les personnes physiques ont démontrées pour l'entité enregistrée (compétences entrepreneuriales liées à la personne nécessaires pour l'exercice de certaines activités), ainsi que les commerçants ambulants et forains.³

¹ Il s'agit des données suivantes : le numéro d'entreprise de l'établissement, le code NACE de l'activité, la version de la nomenclature NACE (2003 ou 2008), le type d'activité (activité principale, activité secondaire, activité auxiliaire), la date de début de l'activité, la date de fin de l'activité. Les actions d'office effectuées sur l'activité (radiation, inscription, modification).

² Il s'agit des données suivantes : type d'adresse de l'entreprise (par exemple, adresse du siège social, adresse de la succursale), la langue dans laquelle l'adresse est enregistrée, le régime linguistique de la commune, les codes de rue, le nom de la rue, le numéro de maison, le code postal, le numéro de boîte aux lettres, la commune, le pays de l'adresse, le code pays, l'état (pour certaines adresses étrangères), les détails (informations supplémentaires telles que les noms des zones industrielles ou des bâtiments), la date de début et de fin de l'adresse, les actions administratives effectuées sur l'adresse (radiation d'office, inscription ou modification).

³ Il s'agit des données suivantes : code d'identification de la qualité; autorisation ou compétence professionnelle exercée; date d'inscription de la qualité ou de l'autorisation; numéro d'entreprise de l'établissement; dans le cas où une compétence entrepreneuriale ou une autorisation d'établissement est décrite, le code de la phase dans laquelle se trouve la qualité ou l'autorisation : ceci spécifie la phase du dossier auprès de l'autorité compétente; administration délivrant la qualité ou l'autorisation; indicateur indiquant si une exemption a été obtenue pour la compétence entrepreneuriale; date de début de la qualité, de l'autorisation, de la compétence entrepreneuriale, de la qualité de commerçant ambulant ou de forain;

- “**LinkedEnterprises**” : Cette catégorie comprend les liens entre les entités enregistrées ainsi que les liens entre l'entité enregistrée et ses unités d'établissement.⁴
- “**Enterprise**” : Cette catégorie concerne l'identification des entités enregistrées.⁵
- “**ForeignIdentifications**” : Cette catégorie comprend le numéro d'identification attribué à une entreprise étrangère dans le registre de son pays d'origine.⁶
- “**Functions**” : Cette catégorie comprend les fonctions potentielles exercées par les entités enregistrées au sein de l'entreprise.⁷
- “**JurForms**” : Cette catégorie indique le type d'entité enregistrée qui peut être créé par des personnes morales et des entreprises sans personnalité juridique.⁸
- “**JurSits**” : Cette catégorie concerne l'état juridique de l'entité enregistrée à tout moment de son cycle de vie.⁹

date de fin de la qualité, de l'autorisation, de la compétence entrepreneuriale, de la qualité de commerçant ambulant ou de forain; durée de la qualité ou de l'autorisation (le cas échéant); motif de cessation de la qualité, de l'autorisation, de la compétence entrepreneuriale, de la qualité de commerçant ambulant ou de forain; numéro d'identification de sécurité sociale; nom de famille et prénom de la personne ayant démontré la compétence entrepreneuriale, du commerçant ambulant ou du forain; les actions administratives effectuées sur la compétence entrepreneuriale (radiation, inscription, modification).

⁴ Il s'agit des données suivantes : le numéro d'entreprise ou le numéro d'établissement des entités; le code du lien entre deux entités (tel que scission, fusion, ...), la raison de la cessation du lien entre deux entreprises, la date de début du lien entre les entités enregistrées / unités d'établissement, la date de fin du lien entre les entités enregistrées / unités d'établissement.

⁵ Il s'agit des données suivantes : le numéro d'entreprise, la date d'inscription de l'entreprise, le type d'entreprise (entreprise personne physique, personne morale, entreprise sans personnalité juridique), la date de création de l'entité enregistrée ; la date de cessation de l'entité enregistrée ; le statut indiquant le stade du cycle de vie de l'entité enregistrée (actif, cessé, ...) ; le capital social actuel de l'entreprise ; le code monétaire dans lequel le capital social déclaré est exprimé ; si l'entreprise a été créée pour une durée limitée, cette durée en nombre d'années sera également indiquée.

⁶ Il s'agit des données suivantes : le code pays du registre des entreprises étrangères, le code du registre étranger, le nom du registre étranger, le numéro d'entreprise dans le registre étranger.

⁷ Il s'agit des données suivantes : le code de la fonction exercée, la date de début et de fin de la fonction dans l'entité enregistrée, la raison de la cessation de la fonction, le numéro d'identification de l'entité enregistrée exerçant la fonction, le nom de famille de la personne exerçant la fonction (en cas de personne physique) ; le prénom de la personne exerçant la fonction (en cas de personne physique) ; le numéro d'identification de la sécurité sociale, renseigné uniquement lorsque le numéro de personne est requis ; le numéro d'entreprise de l'entreprise personne physique en cas de syndic professionnel ; le numéro d'entreprise de l'établissement (dans le cas où une fonction d'établissement est décrite) ; les actions administratives effectuées sur la fonction (radiation, inscription, modification).

⁸ Il s'agit des données suivantes : le code de la forme juridique, la date de début et de fin de la forme juridique pour la personne morale ou l'entreprise sans personnalité juridique, les actions administratives effectuées sur la forme juridique (radiation, inscription ou modification), la raison de l'inscription de l'action administrative.

⁹ Il s'agit des données suivantes : le service qui a modifié l'état juridique, le code reflétant l'état juridique de l'entreprise (par exemple, création juridique, état normal, clôture de faillite), la date de début et de fin de l'état juridique concerné de l'entreprise, le statut que l'entreprise a eu/avait pendant la durée de l'état juridique (actif, en faillite, ...), l'historique des événements de l'état juridique de l'entreprise (Annulation de la faillite, réhabilitation, ...).

- “**Denominations**”: Cette catégorie concerne le(s) nom(s) de l'entreprise, éventuellement dans différentes langues si applicable.¹⁰

9. Les destinataires des données envisagées sont :

- Les services impliqués dans l'élaboration des analyses, en particulier les data scientists, les ingénieurs de données et les analystes business de la Direction Datamining de la Direction générale des services d'inspection, pour les finalités suivantes :
 - o Le développement de code pour croiser les données et modéliser les données, y compris le développement de modèles de prédiction.
 - o La conversion des relations et des motifs dans les données en informations utiles sous forme de fichiers de résultats et de visualisations.
 - o La vérification et la validation des analyses dans le contexte business spécifique.
 - o La surveillance de la qualité des données.
- Les utilisateurs des fichiers de résultats et des visualisations, spécifiquement les inspecteurs sociaux et les gestionnaires de dossiers de la Direction générale des services d'inspection, de la Direction générale de l'Identification et du Contrôle, de la Direction générale des Services de Recouvrement, de la Direction générale des Services Juridiques, de la Direction générale des Services Financiers et Statistiques, de la Direction générale de la Sécurité Sociale d'Outre-mer, des Marins et de la Sécurité Sociale Maritime. Les inspecteurs et les gestionnaires de dossiers sont les utilisateurs finaux des analyses. Ils peuvent consulter les résultats dans le cadre de l'exercice de leurs missions légales spécifiques via des fichiers ou des visualisations, mais ils n'ont par ailleurs pas accès à l'ensemble des données faisant l'objet de cette délibération.

Un inspecteur effectuant une enquête auprès d'un employeur pour vérifier l'application correcte de la réglementation sociale relevant de sa compétence conformément aux dispositions du Code pénal social, pourra consulter le réseau d'entreprises liées et de leurs détenteurs de fonctions via une représentation graphique du réseau dans laquelle sont également incluses les données BCE de l'employeur. Cette visualisation ne montre que les entreprises faisant partie du réseau selon les règles établies dans l'analyse business.

Un gestionnaire de dossier de ces services consultant un fichier de résultats n'aura accès qu'aux données des employeurs présentant un risque accru après analyse des indicateurs.

- En application du Code pénal social, les fichiers de résultats sont également communiqués, sur présentation d'une apostille, aux auditorats du travail, aux parquets et aux inspecteurs sociaux des institutions compétentes (c'est-à-dire d'autres services d'inspection sociale).

10. Conformément à l'article 14 de la loi du 15 janvier 1990 portant création et organisation de la Banque-Carrefour de la Sécurité Sociale, l'ONSS est en principe tenue d'assurer les échanges de données à caractère personnel avec l'intervention de la Banque-Carrefour de la

¹⁰ Il s'agit des données suivantes : le type de nom (par exemple, dénomination sociale, abréviation, nom commercial) ; la langue dans laquelle le nom est enregistré ; le nom lui-même de l'entreprise ; la date de début et de fin du nom ; les actions administratives effectuées sur les noms (radiation, inscription, modification).

Sécurité Sociale (BCSS). Cependant, le même article 14 stipule que la chambre de sécurité sociale et de santé du comité de sécurité de l'information peut prévoir une exemption de son intervention dans la mesure où cette intervention ne peut pas apporter de valeur ajoutée.

11. Les parties concernées estiment que la Banque-Carrefour de la Sécurité Sociale ne peut pas apporter de valeur ajoutée à l'échange de données envisagé. Des contraintes techniques strictes empêcheraient le traitement des données via la BCSS en tant qu'organisation intermédiaire. Un traitement efficace de grands ensembles de données, comme celui requis pour la construction de modèles de risques, nécessite l'accès aux données de la BCE décrites via un fichier "full extract" contenant toutes les entités enregistrées de la base de données de la BCE. Un échange de données via la BCSS est possible uniquement sur une base de consultation et via un service web. Cela signifie que les données devraient être demandées pour chaque entité enregistrée individuelle. De plus, le service web limite le nombre de consultations autorisées à un quota mensuel de 80 000. Sur la base de ce qui précède, l'ONSS demande à être exemptée de l'intervention de la BCSS.

II. TRAITEMENT DE LA DEMANDE

A. RECEVABILITE ET COMPETENCE DU COMITE

12. La communication de données à caractère personnel par les services publics et les institutions publiques du gouvernement fédéral aux institutions de sécurité sociale visées à l'article 2, paragraphe 1, 2°, a), de la loi du 15 janvier 1990 portant création et organisation de la Banque-Carrefour de la Sécurité Sociale nécessite une délibération préalable des chambres réunies du comité de sécurité de l'information dans la mesure où les responsables du traitement de l'entité communicante, de l'entité réceptrice et de la Banque-Carrefour de la Sécurité Sociale, en application 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, ne parviennent pas à un accord sur la communication ou à condition qu'au moins l'un de ces responsables du traitement demande une délibération et en informe les autres responsables du traitement. Dans ces cas, la demande est introduite d'office conjointement par les responsables du traitement concernés.
13. Le Comité de sécurité de l'information prend note du fait que le SPF Économie a donné son accord écrit concernant la communication des données par la BCE à l'ONSS¹¹. Cependant, le Comité de Sécurité de l'Information constate qu'aucun protocole au sens de l'article 20 de la loi susmentionnée du 30 juillet 2018 n'a été établi par l'ONSS et le SPF Économie, et que l'ONSS a soumis une demande.
14. Enfin, l'exemption de l'intervention de la BCSS, conformément à l'article 14 de la loi du 15 janvier 1990 portant création et organisation de la Banque-Carrefour de la Sécurité Sociale, dans la mesure où cette intervention ne peut pas apporter de valeur ajoutée, nécessite une délibération de la chambre de sécurité sociale et santé du Comité de sécurité de l'information.
15. Eu égard à ce qui précède, le Comité de Sécurité de l'Information est compétent pour se prononcer sur la demande en question.

B. QUANT AU FOND

¹¹ Décision du 15 septembre 2023.

B.1. RESONSABILITE

16. Conformément à l'article 5.2 du Règlement général sur la protection des données (ci-après dénommé «RGPD»), le SPF Economie (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 5.1 du RGPD et doivent être en mesure de le démontrer¹².
17. Le responsable du traitement doit, conformément au RGPD, satisfaire à un certain nombre d'obligations. Dans la présente délibération, les principales obligations sont examinées. À cet égard, le Comité de Sécurité de l'Information souligne que le responsable du traitement doit tenir un registre des activités de traitement conformément aux dispositions de l'article 30 du RGPD.

B.2. LICEITE

18. Conformément à l'article 5.1 a) du RGPD, les données à caractère personnel doivent être traitées de manière licite à l'égard de la personne concernée. Cela signifie que le traitement doit reposer sur l'un des fondements légaux énumérés à l'article 6 du RGPD.
19. Le Comité de Sécurité de l'Information constate que la communication envisagée de données à caractère personnel est nécessaire à l'exécution d'une mission d'intérêt public ou à l'exercice de l'autorité publique dont est investi le responsable du traitement (article 6.1 e) du RGPD).
20. L'article 5bis de la loi du 15 janvier 1990 portant création et organisation de la Banque-Carrefour de la Sécurité sociale stipule expressément que les institutions de sécurité sociale et les services d'inspection sociale, en vue de la prévention, de la constatation, de la poursuite et de la répression des infractions à la réglementation sociale relevant de leurs compétences respectives, ainsi que pour le recouvrement des montants relevant de leurs compétences respectives, peuvent collecter, traiter et fusionner toutes les données nécessaires à

¹² Les données à caractère personnel doivent être:

- 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).

l'application de la législation sur le droit du travail et la sécurité sociale dans un entrepôt de données qui leur permet d'effectuer des processus de datamining et de datamatching, y compris le profilage au sens de l'article 4, 4), du règlement général sur la protection des données.

21. Le Comité de sécurité de l'information constate tout d'abord que la communication de données par la Banque-Carrefour des Entreprises du SPF Économie est autorisée conformément à l'article III.29 et suivants du Code de droit économique, qui prévoit que l'accès aux données de la BCE peut être accordé aux autorités, administrations, services ou autres organismes, dans la mesure où ces données sont nécessaires à l'exécution de leurs missions légales ou réglementaires.
22. Les missions de l'ONSS sont déterminées par la loi du 27 juin 1969 portant révision de l'arrêté-loi du 28 décembre 1944 concernant la sécurité sociale des travailleurs, ainsi que par ses arrêtés d'exécution. Les missions des inspecteurs sociaux sont expressément définies dans diverses lois et arrêtés royaux. Le Comité de sécurité de l'information a reçu un aperçu détaillé de la législation qui décrit les missions et responsabilités spécifiques des inspecteurs sociaux, entre autres :
 - Art. 60 du décret royal du 18 juillet 2002 relatif aux mesures visant à promouvoir l'emploi dans le secteur non marchand
 - Art. 4bis, dernier alinéa du décret royal n° 499 du 31 décembre 1986 relatif à la sécurité sociale des jeunes défavorisés
 - Art. 13 du décret royal du 16 mai 2003 relatif à l'exécution du Chapitre 7 du Titre IV de la loi-programme du 24 décembre 2002 (I), concernant l'harmonisation et la simplification des régimes de réductions des cotisations de sécurité sociale.
 - Art. 21 de la Loi du 4 juillet 2021 portant des mesures temporaires de soutien en raison de la pandémie de COVID-19 (MB 13/7/2021)
 - Art. 44 de la Loi du 2 avril 2021 portant des mesures temporaires de soutien en raison de la pandémie de COVID-19 (MB 13/04/2021)
 - Art. 6/5 du décret royal du 1er juillet 2011 relatif à l'application des articles 16, 13°, 17, 20, 63, 70 et 88 du Code pénal social et fixant la date d'entrée en vigueur de la loi du 2 juin 2010 portant des dispositions en matière de droit pénal social
 - Art. 5 de la Loi du 3 avril 1995 portant des mesures en faveur de l'emploi
 - Art. 60 du décret royal du 18 juillet 2002 relatif aux mesures visant à promouvoir l'emploi dans le secteur non marchand.
 - Art. 12, paragraphe 5 du décret royal du 19 décembre 2001 relatif à la promotion de l'emploi des demandeurs d'emploi de longue durée
 - Art. 20 du décret royal du 27/04/2007 portant dispositions générales d'application des mesures en faveur de l'emploi des jeunes dans le secteur non marchand découlant de la loi du 23 décembre 2005 relative au pacte générationnel
 - Art. 2 du Décret royal du 1er juillet 2011 portant application des articles 16, 13°, 17, 20, 63, 70 et 88 du Code pénal social et fixant la date d'entrée en vigueur de la loi du 2 juin 2010 portant des dispositions en matière de droit pénal social
 - Art. 18 du décret royal du 17 février 2005 portant exécution des dispositions de la loi du 3 mai 2003 réglementant le contrat de travail pour le service en mer pour la pêche et améliorant le statut social du pêcheur

- Art. 1 du Décret royal du 31 juillet 2020 désignant les fonctionnaires chargés de surveiller le respect de la loi du 12 juin 2020 sur le travail dans le secteur de la pêche.
 - Art. 1 du décret royal du 4 août 2014 désignant les fonctionnaires chargés de surveiller le respect de la loi du 13 juin 2014 portant exécution et contrôle de l'application de la Convention sur le travail maritime de 2006 et de ses arrêtés d'exécution
 - Art. 10 du décret royal du 23/01/2003 portant exécution des articles 15 et 17 de la loi du 05/09/2001 visant à améliorer le taux d'emploi des travailleurs
 - Art. 1 du décret royal du 30/09/1980 désignant les fonctionnaires et agents chargés de surveiller l'exécution du décret royal n° 5 du 23 octobre 1978 relatif à la tenue de documents sociaux et à ses arrêtés d'exécution
 - Art. 4 du Décret royal du 1er juillet 2011 portant application des articles 16, 13°, 17, 20, 63, 70 et 88 du Code pénal social et fixant la date d'entrée en vigueur de la loi du 2 juin 2010 portant des dispositions en matière de droit pénal social
 - Art. 2/1 du décret royal du 28 août 2002 désignant les fonctionnaires chargés de surveiller le respect de la loi du 4 août
 - Art. 2 du décret royal du 8 mars 1990 portant exécution des dispositions de la loi-programme du 22 décembre 1989 relatives au contrôle des dérogations à l'horaire de travail normal des travailleurs à temps partiel
 - Art. 36 du décret royal du 9 juin 1999 portant exécution de la loi du 30 avril 1999 relative à l'emploi de travailleurs étrangers
 - Article 11 de la loi du 30 avril 1999 relative à l'emploi de travailleurs étrangers
 - Code pénal: articles 433 quinquies à 433 octies et 433 decies à 433 duodecies (traite des êtres humains)
 - Art. 81 de la Loi du 15 décembre 1980 relative à l'accès au territoire, au séjour, à l'établissement et à l'éloignement des étrangers
 - etc.
- 23.** Également, il convient de faire référence aux articles 55 et 56 du Code pénal social qui déterminent la communication d'informations aux inspecteurs sociaux par d'autres administrations, ainsi que l'utilisation de ces informations (voir paragraphe 4).
- 24.** L'échange électronique des données est également expressément prévu à l'article 15/4 du Code pénal social :
- "Art. 15/4. 1 L'échange de données*
- § 1. Afin de permettre aux services chargés de lutter contre la fraude sociale d'échanger de manière permanente les données nécessaires, conformément aux dispositions prévues dans ce code, les fonctionnaires dirigeants des services d'inspection sociale visés à l'article 15/2 désignent un inspecteur social en tant que membre effectif et un inspecteur social en tant que remplaçant, chargés de veiller à cet échange de données dans le respect des dispositions énumérées aux articles 54 à 57 de ce code. Si possible, cet échange de données se fera au moyen d'une plateforme électronique.*
- § 2. La plateforme électronique visée au paragraphe précédent peut recueillir, recevoir, coordonner et traiter les informations nécessaires à la lutte contre le travail illégal et la fraude sociale, et les transmettre aux institutions publiques et aux institutions de sécurité sociale collaborantes, aux inspecteurs sociaux des services d'inspection sociale, ainsi qu'à tous les fonctionnaires chargés de la surveillance d'une autre législation ou de l'application*

d'une autre législation, dans la mesure où ces informations leur sont utiles dans l'exercice de la surveillance qui leur est confiée ou pour l'application d'une autre législation. Les fonctionnaires dirigeants des services d'inspection visés à l'article 15/2 désignent le fonctionnaire responsable du traitement de ces données. »

25. Au vu de ce qui précède, le Comité de sécurité de l'information estime que la communication envisagée est licite.

B.3. LIMITATION DES FINALITES

26. L'article 5.1 b) du RGPD autorise le traitement des données personnelles uniquement à des fins déterminées, explicites et légitimes (principe de finalité).
27. Le Comité de sécurité de l'information prend note du fait que la communication envisagée de données personnelles vise un but spécifique, explicite et légitime, à savoir l'identification unique des entités enregistrées et la détermination de qui exerce des fonctions responsables à l'égard de ces entités enregistrées, dans le cadre de l'exercice des missions légales en matière d'inspection sociale.

B.4. MINIMISATION DES DONNEES

28. 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 («minimisation des données»).

29. La nécessité du traitement des catégories de données personnelles est justifiée par l'ONSS de la manière suivante :

- "Activities" (aperçu des activités) : L'activité d'une entreprise peut faire partie d'un modèle de risque dans le cadre de la lutte contre la fraude. Il est nécessaire de connaître le secteur d'une entreprise, que ce soit pour une sélection plus ciblée (secteurs à risque), pour élaborer des modèles de risque et comme enrichissement des listes de résultats. Sans les données de la BCE, l'ONSS dispose uniquement de ces informations pour les entreprises enregistrées en tant qu'employeurs, et uniquement pour le code d'activité attribué par l'ONSS. Le(s) code(s) d'activité peut ou peuvent différer entre les données de l'ONSS et de la BCE.

- "Adresses" (données d'adresse) : Chaque inspecteur est compétent pour une région spécifique, donc l'identification de la région est nécessaire. La BCE est la seule source complète et correcte de données d'adresse et de leur historique. Ces informations ne sont pas entièrement présentes dans l'ONSS. En particulier, l'ONSS n'a pas les données d'adresse des entreprises qui ne sont pas des employeurs (ou qui ne sont pas déclarées comme employeurs). Les indicateurs connus de fraude incluent : le partage d'une adresse avec une entreprise frauduleuse, les déménagements fréquents, les déménagements selon un modèle typique (par exemple, "de lieu A à lieu B") et plusieurs entreprises radiées à la même adresse.

- "Authorizations, Permissions, Professions" (qualifications, autorisations et compétences entrepreneuriales) : Un groupe d'experts d'inspecteurs sociaux a indiqué que la présence ou l'absence de certaines qualifications, autorisations et compétences entrepreneuriales, nécessaires pour l'exercice de certaines activités, sont des indicateurs forts pour distinguer d'une part les entreprises/employeurs présentant un risque élevé de fraude de paiement, de fraude déclarative et d'infractions à la législation sociale, et d'autre part les entreprises/employeurs où ce risque est significativement plus faible. Des analyses a

posteriori, régulièrement répétées dans le temps, sur les enquêtes clôturées des inspecteurs sociaux de l'ONSS, l'ont également démontré statistiquement.

- "LinkedEnterprises" (les liens entre les entités enregistrées et entre l'entité enregistrée et ses établissements) : La BCE est la seule source permettant d'identifier la relation entre le siège social et les unités d'établissement. Cette catégorie permet à l'ONSS de recueillir des informations sur les unités d'établissement. Ces données sont également nécessaires pour déterminer quelles entreprises ont des unités d'établissement à la même adresse, qui crée des unités d'établissement, et la scission, l'absorption et le transfert d'unités d'établissement.

- "Enterprise" (l'identification des entités enregistrées) : Cette catégorie est essentielle pour croiser les données avec d'autres bases de données. C'est la source unique des données de démarrage des entités enregistrées et pour vérifier si elles sont actives ou non. Avec ces informations, l'ONSS peut par exemple déterminer depuis combien de temps une entité enregistrée est connue de la BCE. Pour un employeur, cette date peut précéder de loin la date d'affiliation à l'ONSS.

- "ForeignIdentifications" (le numéro d'identification d'une entreprise étrangère) : Ces données sont nécessaires pour l'identification plus précise des entreprises entre/dans plusieurs sources/applications.

- "Functions" (les fonctions/mandats possibles exercés par les entités enregistrées) : Cette catégorie est la source unique des données sur les mandataires. Cette information est nécessaire pour construire des réseaux de mandataires partagés entre des entreprises. Lorsqu'une personne a ou avait un mandat dans une entreprise impliquée dans une fraude de paiement, il est très pertinent de savoir dans quelles autres entreprises elle a également un mandat, car cela peut être une indication d'une structure frauduleuse.

- "JurForms" (le type d'entité enregistrée qui peut être créé par des personnes morales et des entreprises sans personnalité juridique) : L'historique des changements de forme juridique est uniquement disponible dans ce fichier. La source interne de l'ONSS n'est pas complète. Ces données sont nécessaires pour construire des indicateurs de risque liés à l'activité d'une entreprise. Cela permet à l'ONSS, entre autres, de faire la distinction entre les secteurs public et privé avec des informations plus détaillées que celles disponibles dans les bases de données internes de l'ONSS. Certains phénomènes de fraude concernent uniquement le secteur public ou privé, rendant ces informations nécessaires.

- "JurSits" (la situation juridique de l'entité enregistrée) : Ces données sont nécessaires pour sélectionner les employeurs actifs ou inactifs et les employeurs faillis ou non faillis. Le nombre de faillissements (par mandataire ou adresse) est un élément important pour détecter certaines constructions frauduleuses. La sélection des entreprises actives augmente également l'efficacité de nos actions de contrôle. Ces données contiennent également un historique de la situation juridique des entreprises telle que connue de la BCE. Cela permet à l'ONSS, entre autres, d'obtenir des informations correctes et complètes sur la procédure de faillite. La procédure complète de faillite peut prendre beaucoup de temps, et dans les bases de données internes, l'ONSS ne connaîtrait que la date finale, alors que la date de début est souvent plus pertinente. Les informations entre la BCE et la base de données de l'ONSS peuvent donc différer.

- "Denominations" (le(s) nom(s) de l'entreprise) : Le nom de l'employeur garantit l'identification correcte et lisible des entreprises concernées et est donc nécessaire.

L'historique des changements de nom est uniquement disponible dans cette table. Les changements fréquents de nom sont également un indicateur de certains phénomènes de fraude.

- 30.** Le Comité de la Sécurité de l'Information constate que le numéro d'identification de la sécurité sociale est communiqué pour l'identification des personnes physiques. Le numéro d'identification de la sécurité sociale est formé soit par le numéro du Registre national, soit par le numéro d'identification attribué par la Banque-Carrefour de la Sécurité Sociale. Contrairement au numéro d'identification attribué par la Banque-Carrefour de la Sécurité Sociale, l'utilisation du numéro de Registre national n'est pas libre et nécessite une autorisation explicite. Le comité de sécurité de l'information constate que l'ONSS est autorisée à utiliser le numéro de Registre national en vertu de l'arrêté royal du 5 décembre 1986 réglant 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. L'ONSS doit veiller à ce que le numéro de Registre national ne soit communiqué qu'aux personnes et aux organismes qui disposent également de l'autorisation requise.
- 31.** L'ONSS vise la communication des données de toutes les entités enregistrées dans la BCE car, dans les applications et processus de l'ONSS, en particulier ceux liés à la détection et à la constatation de la fraude en matière de paiement, de déclaration ou de sécurité sociale, toutes les entreprises sont concernées (pas seulement les employeurs). Étant donné que ces entreprises ne sont pas toujours indiquées avec un numéro BCE dans les applications de l'ONSS, il n'est pas possible de faire une sélection limitée. Toute tentative en ce sens ne serait qu'une approximation et pourrait changer constamment (plusieurs fois par jour). En l'absence d'un numéro BCE, une comparaison (sur la base des coordonnées de nom et d'adresse) avec l'ensemble des données des entités enregistrées dans la BCE est nécessaire pour identifier correctement l'entité enregistrée. Cette comparaison doit être robuste par rapport aux erreurs d'écriture (intentionnelles ou non) et aux changements historiques, et elle est tout sauf triviale. À moins que la BCE ne dispose d'un service performant que l'ONSS pourrait utiliser, pour des milliers de cas par jour, et qui effectue une comparaison adéquate et robuste par rapport à chaque fois l'ensemble de la population des entreprises et de leur historique, la seule solution pratique permettant d'effectuer ces comparaisons nécessaires est la communication des données envisagées pour toutes les entités enregistrées dans la BCE.
- 32.** L'ONSS vise également la communication des données historiques remontant jusqu'à 10 ans dans le passé. Elle a besoin de toutes les situations et modifications qui étaient en vigueur dans la période allant du moment de la demande jusqu'au 1er janvier de l'année se situant 10 ans avant l'année de la demande. Cela correspond à la politique de conservation des données de l'ONSS en matière de recouvrement basé sur les risques et de lutte contre la fraude sociale. Cette politique stipule que si l'ONSS se constitue partie civile dans une affaire pénale, la prescription est prolongée jusqu'à 10 ans (dans des cas exceptionnels, même plus longtemps).
- 33.** Le Comité de sécurité de l'information prend également note du fait que les données incluses dans les fichiers de résultats qui sont communiqués aux destinataires décrits concernent exclusivement les entreprises qui font l'objet de l'exécution de la mission légale du destinataire en question.
- 34.** Suite à la communication initiale du fichier complet de données, l'ONSS vise une communication quotidienne de données. Cela est nécessaire pour maximiser la fiabilité des

modèles prédictifs développés et des possibilités d'exploration de données. Il est crucial d'avoir accès aux données les plus récentes des entités enregistrées. Cela améliore la qualité et la représentativité des données d'entraînement, l'identification correcte des entités enregistrées concernées, le choix de l'algorithme et le réglage approprié des paramètres du modèle. La réception quotidienne des données permet également à l'ONSS de vérifier l'intégrité technique et la précision des fichiers de données reçus.

35. Compte tenu de ce qui précède, le Comité de sécurité de l'information estime que la communication des données personnelles envisagées est adéquate, pertinente et limitée à ce qui est nécessaire aux fins pour lesquelles elles sont traitées.

B.5. LIMITATION DE CONSERVATION

36. Conformément à l'article 5.1 e) du RGPD, les données personnelles doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une période n'excédant pas celle nécessaire aux fins pour lesquelles les données personnelles ont été obtenues.
37. Conformément à l'article 5ter, §4 de la loi du 15 janvier 1990 portant création et organisation d'une banque-carrefour de la sécurité sociale, les données personnelles relevant de l'application de cet article ne peuvent être conservées plus longtemps que nécessaire pour les finalités pour lesquelles elles sont traitées, y compris les exigences relatives à l'application de la répétition et de la révocation d'un délai accordé, avec une durée maximale de conservation d'un an après la prescription de toutes les créances relevant de la compétence du responsable du traitement, et le cas échéant, le paiement intégral de tous les montants associés à celles-ci.
38. Le Comité de la sécurité de l'information prend acte du fait que les données ne seront pas conservées plus longtemps que nécessaire pour atteindre les objectifs dans le cadre de la lutte contre la fraude découlant de la mission générale de perception correcte et opportune des cotisations de sécurité sociale des travailleurs. Les données envisagées seront conservées par l'ONSS pendant une période maximale de 10 ans. Cette période de 10 ans correspond à la politique de conservation des données de l'ONSS en matière de perception basée sur les risques et de lutte contre la fraude sociale. Cette politique stipule que si l'ONSS se constitue partie civile dans une affaire pénale, la prescription est prolongée de 10 ans (sauf cas exceptionnels).
39. Les fichiers de résultats générés par l'ONSS sur la base des données fournies et transmis aux destinataires mentionnés sont conservés aussi longtemps que nécessaire pour la gestion administrative des dossiers auxquels les données se rapportent. Cette durée de traitement peut varier en fonction du processus (par exemple, les délais de paiement amiables éventuels, le délai de prescription applicable, les délais de recours, etc.). Le traitement d'un dossier en cours nécessite une conservation permettant aux données d'être normalement disponibles et accessibles aux fonctionnaires chargés de la gestion du dossier. Une fois les délais nécessaires pour la gestion administrative du dossier écoulés, une méthode de conservation est mise en place pour conférer aux fichiers de résultats une disponibilité et une accessibilité limitées. Une telle méthode de conservation répond à d'autres finalités éventuelles de la conservation, telles que le respect des dispositions légales en matière de prescription ou l'exécution de contrôles administratifs. Le délai de prescription des dossiers dépend en tout cas du service pour lequel la Direction Datamining effectue les analyses : Inspection,

Contrôle ou Recouvrement. La durée maximale de conservation des fichiers de résultats est de 7 ans pour les dossiers de fraude, prolongée à 10 ans si l'ONSS se constitue partie civile dans une affaire pénale.

40. Le Comité de sécurité de l'information estime que les périodes de conservation décrites sont acceptables.

B.6. TRANSPARENCE

41. Conformément à l'article 14 du RGPD, le responsable du traitement est tenu de fournir certaines informations sur le traitement des données au titulaire des données lorsque les données personnelles n'ont pas été obtenues directement auprès du titulaire. Cette obligation ne s'applique cependant pas si l'obtention ou la communication des données est expressément prescrite par le droit de l'Union ou national applicable au responsable du traitement, et si ce droit prévoit des mesures appropriées pour protéger les intérêts légitimes du titulaire des données.
42. Le Comité de sécurité de l'information constate que la communication de données personnelles est couverte par l'article III.29 et suivants du Code de droit économique, en combinaison avec la réglementation décrite aux paragraphes 23 à 27, et fait l'objet de la présente délibération, qui est publiée sur le site web du Comité de sécurité de l'information.
43. L'ONSS se prévaut également de l'exception prévue à l'article 100/14 du Code pénal social, qui lui donne la possibilité de différer, limiter ou exclure le droit à l'information pour ce qui est du traitement de données à caractère personnel, notamment par les services d'inspection sociale, pendant la période pendant laquelle la personne concernée fait l'objet d'un contrôle ou d'une enquête, ou des travaux préparatoires liés réalisés par lesdits services d'inspection dans le cadre de l'exécution de leurs missions légales. Ces dérogations s'appliquent dans la mesure où l'application de ce droit pourrait être préjudiciable au contrôle, à l'enquête ou aux travaux préparatoires, ou menace de compromettre le secret de l'enquête pénale ou la sécurité des personnes.
44. En vue des missions décrites des inspecteurs sociaux, il est impossible qu'ils avisent les employeurs individuels, concernés par les données personnelles mentionnées, du fait que ces données seront collectées et traitées. Leurs missions de police administrative perdraient en effet leur impact si la personne concernée se voyait accorder le droit de prendre connaissance des données le concernant qui sont incluses dans un traitement. Cela serait bien entendu en contradiction avec l'esprit de la législation sur l'inspection du travail ainsi qu'avec les lois et règlements sociaux auxquels les inspecteurs sociaux sont tenus de veiller.
45. Au vu de ce qui précède, le Comité de la sécurité de l'information estime qu'il est acceptable que le SPF Économie et l'ONSS soient dispensés d'une communication d'informations individuelle concernant la communication de données personnelles. Le Comité de la sécurité de l'information prend acte du fait que les deux institutions publient une déclaration de confidentialité sur leurs pages web respectives. Le SPF Économie fait expressément référence à la mise à disposition de données de la BCE entre autres à d'autres organismes gouvernementaux en vertu des articles susmentionnés du Code de droit économique. Le Comité de la sécurité de l'information estime qu'il est approprié que l'ONSS donne des clarifications supplémentaires dans sa déclaration de confidentialité sur les catégories de données personnelles qu'il reçoit et traite de la part d'autres responsables du traitement.

B.7. INTEGRITE ET CONFIDENTIALITE

46. 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.
47. 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
48. Le Comité de sécurité de l'information constate que le traitement des données personnelles par l'ONSS est effectué conformément à la loi du 15 janvier 1990 portant création et organisation d'une Banque-Carrefour de la Sécurité Sociale.
49. Le Comité de sécurité de l'information prend acte du fait que l'ONSS est tenu de respecter les normes de sécurité minimales définies par le Comité de Coordination Générale de la Banque-Carrefour de la Sécurité Sociale.
50. Le Comité de sécurité de l'information souligne les directives de sécurité applicables à tous les organismes fédéraux, y compris le SPF Economie, telles qu'elles sont incluses dans la Politique fédérale de sécurité de l'information (*Federal Information Security Policy*).
51. Le Comité de sécurité de l'information constate que :
 - Le SPF Économie et l'ONSS disposent d'un délégué à la protection des données ;
 - L'ONSS a réalisé une évaluation d'impact sur la protection des données concernant la collecte des données dans le cadre du datawarehouse.
 - Toutes les personnes impliquées dans le traitement des traitements décrits dans cette délibération sont tenues à une obligation légale de confidentialité, en vertu de l'article 28 de la loi du 15 janvier 1990 portant création et organisation de la Banque-Carrefour de la Sécurité Sociale et, en ce qui concerne les inspecteurs sociaux, l'article 58 du Code pénal social.
 - Les journaux nécessaires sont conservés et une gestion intégrée des utilisateurs et des accès est assurée.
52. Le Comité de sécurité de l'information constate en outre que l'ONSS fait appel à un sous-traitant, l'ASBL Smals, qui fournit l'infrastructure informatique pour stocker le flux de données de la BCE, effectuer des calculs avec les données, et assurer l'accès à ces données via des réseaux. L'Informatieveiligheidscomité souligne que l'ONSS doit, conformément à l'article 28 du RGPD, régir le traitement par le sous-traitant dans un accord ou un autre acte juridique en vertu du droit de l'Union ou du droit national qui lie le sous-traitant à l'égard du responsable du traitement, et dans lequel le sujet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, ainsi que les droits et obligations du responsable du traitement, sont décrits.

Par ces motifs,

les chambres réunies du Comité de sécurité de l'information

concluent que la communication de données à caractère personnel issues de la Banque-Carrefour des Entreprises par le SPF Économie à l'Office national de sécurité sociale, en vue de l'identification univoque des entités enregistrées et pour déterminer qui exerce des fonctions responsables concernant ces entités enregistrées, dans le cadre de l'exercice des missions légales d'inspection sociale, est autorisée à condition de respecter les mesures établies pour garantir la protection des données, notamment les mesures liées à l'objectif, à la minimisation des données, à la limitation du stockage et à la sécurité des données, en prenant les mesures techniques ou organisationnelles appropriées pour assurer une protection adéquate, garantissant ainsi que les données sont protégées contre un traitement non autorisé ou illicite, ainsi que contre toute perte, destruction ou altération accidentelles.

Conformément à l'article 14, paragraphe 4, de la loi du 15 janvier 1990 portant création et organisation de la Banque-Carrefour de la Sécurité sociale, le Comité de la sécurité de l'information dispense la communication prévue de l'intervention de la Banque-Carrefour de la Sécurité sociale.

Cette délibération, approuvée par le Comité de la sécurité de l'information le 6 février 2024, entre en vigueur le 21 février 2024.

Daniel HACHE
Chambre autorité fédérale

Bart VIAENE
Chambre sécurité sociale et santé

Le siège de la chambre sécurité sociale et de la 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 (tél. 32-2-741 83 11) et le siège de la chambre autorité fédérale du comité de sécurité de l'information est établi dans les bureaux du SPF BOSA- boulevard Simon Bolivar 30- 1000 Bruxelles (tél. 32-2-740 80 64).