Comité de sécurité de l'information
chambre autorité fédérale

DELIBERATION N° 22/025 DU 5 JUILLET 2022 RELATIVE A LA COMMUNICATION DE DONNEES A CARACTERE PERSONNEL PAR LE SPF MOBILITE ET L'OFFICE DES ETRANGERS DU SERVICE PUBLIC FEDERAL INTERIEUR A LA SECTION INSPECTION SOCIALE FLAMANDE DU DEPARTEMENT TRAVAIL ET ECONOMIE SOCIALE AU TRAVERS DE L'APPLICATION MY DIGITAL INSPECTION ASSISTANT (MYDIA)

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, premier alinéa;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données,* en particulier l'article 114 ;

Vu la loi 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*, en particulier l'article 98 ;

Vu la demande du Département Travail et Economie sociale ;

Vu le rapport du service publique fédéral Stratégie et Appui;

Vu le rapport de monsieur Daniel Haché.

I. OBJET DE LA DEMANDE

1. Le département d'inspection sociale flamande du département du travail et de l'économie sociale a été autorisé par la chambre sécurité sociale et santé du Comité de sécurité de l'information par délibération no 22/158 du 7 juin 2022 à consulter les bases de données du réseau de sécurité sociale via l'application My Digital Inspection Assistant (MyDia). Il s'agit des bases de données suivantes:
- Le registre national et les registres banque carrefour;
- Le répertoire des employeurs;
- La base de données DIMONA et le fichier du personnel;
- Le cadastre LIMOSA;
- La base de données GOTOT;
- La banque de données déclaration de chantier;
- La base de données «enregistrement de présence» (Checkin@work);

- La base de données des «prestations de chômage»;
- La base de données «Certificats multifonctionnels» (centres publics d'action sociale);
- Le répertoire général des travailleurs indépendants;
- La base de données DMFA;
- La base de données à caractère personnel relatives à l'incapacité de travail.

2. L'Inspection sociale flamande du Département du travail et de l'économie sociale souhaite désormais avoir la possibilité de consulter également deux autres bases de données (en dehors du réseau de sécurité sociale) via l'application My Digital Inspection Assistant (MyDia) :

- la base de données sur l'immatriculation des véhicules (SPF Mobilité) et

- la plateforme Single Permit relative au permis de séjour et de travail (SPF Intérieur).

3. L'accès aux données à caractère personnel de la base de données du DIV du SPF Mobilité et concerne l'identification de la personne (juridique) au nom de laquelle un véhicule particulier est immatriculé: prénom, nom, date de naissance, adresse, numéro NISS et numéro d'entreprise du titulaire du véhicule. La recherche peut être effectuée à l'aide de la plaque d'immatriculation ou du numéro de châssis. Ces informations doivent permettre aux inspecteurs sociaux d'établir un lien entre l'employé, d'une part, et l'employeur ou le client, d'autre part. Cet accès a déjà été autorisé par la délibération n° 20/017 du 7 juillet 2020 de la chambre autorité fédérale du Comité de sécurité de l'information. La délibération actuelle concerne donc la nouvelle application MyDia par laquelle l'accès est obtenu.

4. L'accès aux données de la plateforme Single Permit sur le permis de séjour et de travail par le biais de l'application MyDia permettra aux inspecteurs sociaux de vérifier la situation des travailleurs/travailleurs non salariés relative à la résidence sur le territoire belge (i.e. le permis de séjour) et des documents dont ils disposent à cet égard et, par extension, si leur emploi est réglementé et si toutes les dispositions pertinentes ont été respectées. L'accès sollicité est limitée à la décision de séjour positive ou négative concernant la personne concernée. L'accès aux mêmes données par l'Office national de la sécurité sociale, le service public fédéral Emploi, travail et concertation sociale, l'Office national de l'emploi, et l'Institut national d'assurances sociales pour travailleurs indépendants a été autorisé pour la même finalité, dans l'exercice de leurs compétences respectives, par délibération n° 21/019 du 6 juillet 2021 du comité de la sécurité de l'information.

5. Les données à caractère personnel demandées concernent toutes les personnes qui sont confrontées aux inspecteurs du droit social dans l'exécution des tâches de contrôle dans la lutte contre la fraude (sociale) qui leur sont confiées par la réglementation. À cet égard, on peut se référer notamment à l'article 2 du décret du 30 avril 2004 *relatif à l'uniformisation des dispositions en matière de contrôle, de sanction et de peines prévues par la législation du droit social pour lesquelles la Communauté flamande et la Région flamande sont compétentes*. La présence d'une personne sur un lieu de travail ou dans un autre lieu relevant de la compétence d'un inspecteur social suffit pour que l'inspecteur social puisse rechercher des données à caractère personnel de cette personne (il n'y a donc pas de sélection préalable).

6. L'application MyDia permet également aux inspecteurs sociaux de connecter les données personnelles qu'ils consultent dans le réseau de sécurité sociale à un contrôle particulier qu'ils effectuent, en utilisant le service web *FieldInspection*. L'audit se rapporte toujours à une enquête créée par un inspecteur social de coordination et à laquelle d'autres inspecteurs sociaux peuvent avoir accès en tant qu'acteur participant. L'enquête comprend les caractéristiques des inspecteurs sociaux et des contrôles, ainsi que le lien entre les inspecteurs sociaux et les contrôles. Les inspecteurs sociaux peuvent stocker temporairement certaines données à caractère personnel qu'ils ont consultées dans le réseau de sécurité sociale (jusqu'à trois jours) dans une base de données sécurisée (aucune donnée à caractère personnel n'est stockée sur leur appareil mobile). Il ne concerne que les données à caractère personnel identifiant les personnes physiques concernées (notamment le numéro d'identification de la sécurité sociale, le nom et le prénom), complétées par des informations spécifiques relatives aux entreprises (numéro d'immatriculation, numéro et nom de l'entreprise) et aux chantiers (numéro d'entreprise, nom de l'entreprise, numéro de chantier et code postal) et à divers indicateurs (par exemple en ce qui concerne l'existence ou non d'une déclaration).

7. Un ensemble minimal de données à caractère personnel — en ce qui concerne le statut du salarié (à temps plein ou à temps partiel), son incapacité de travail, son permis de séjour et son permis de travail en tant que travailleur étranger et l'identification des véhicules trouvés au chantier — peut également être consulté localement, via MyDia. Les informations structurées sur l'interprétation des constatations par les inspecteurs sociaux peuvent également être stockées temporairement (telles que la détermination de la conformité de l'employeur mentionnée dans la déclaration DIMONA et la déclaration DMFA et l'employeur audité) ainsi que le texte libre à cet égard, chacun avec l'identité de l'inspecteur social concerné et la date et l'heure de l'enregistrement.

8. Les données à caractère personnel ne sont conservées que si l'inspecteur social ajoute volontairement une personne, une entreprise ou un chantier identifié à une inspection. Le stockage est également limité aux données à caractère personnel susmentionnées. Par conséquent, il n'y a pas de copie complète de toutes les données à caractère personnel consultées dans les différentes sources authentiques (par exemple, une déclaration DIMONA sera conservée mais son contenu ne sera pas stocké). L'objectif du stockage dans le système est de permettre à l'inspecteur social de vérifier si une consultation des sources authentiques est nécessaire dans le cadre de l'enquête. Cela se fera ensuite, le cas échéant, par les canaux habituels.

9. Afin de pouvoir procéder à des vérifications nécessaires dans le cadre du traitement des données traitées, par exemple par l'inspecteur social coordinateur, un fichier texte serait créé sur un serveur sécurisé, et non sur l'appareil mobile de l'utilisateur, sur la base des données à caractère personnel enregistrées. Il sera envoyé à l'eBox[1] des inspecteurs sociaux concernés

[1] En premier lieu, l'eBox professionnelle serait utilisée puisqu'elle est strictement personnelle et accessible uniquement au titulaire, par opposition aux eBox entreprises. Plus tard, les eBox entreprises pourraient être utilisées, dans la mesure où elles peuvent être compartimentées d'une manière unique au bénéfice des inspecteurs sociaux. L'eBox professionnelle est la boîte aux lettres électronique pour les professionnels proposée sur le portail de la sécurité sociale sous la rubrique «fonctionnaires et autres professionnels» et est intégrée au *Federal Authentication Service* (FAS), où l'accès est réglementé par le gestionnaire de gestion des accès de l'organisation, qui met les utilisateurs sous

et stocké pendant trois jours, puis automatiquement supprimé. Sur la base de ce fichier texte (limité) (avec l'identité des parties concernées et les commentaires sur la recherche), les inspecteurs sociaux peuvent consulter les sources de données à caractère personnel authentiques. Le service web *FieldInspection* n'est donc ni une source de données à caractère personnel authentique ni une copie d'une source de données à caractère personnel authentique. Le système assure le retrait automatique après trois jours. L'application mobile MyDia offre ainsi aux différents inspecteurs sociaux un outil efficace dans l'exécution de leurs tâches de suivi respectives. Ils peuvent mener leurs activités de lutte contre la fraude sociale de manière efficace par la consultation immédiate et sécurisée des données à caractère personnel dans le réseau de sécurité sociale et leur stockage temporaire sécurisé.

10. Dans le domaine politique Travail et Economie sociale, le Département du Travail et Economie sociale est responsable du suivi et de la supervision de la réglementation. À cette fin, la section Inspection sociale flamande a été créée au sein de l'organisation. Les inspecteurs qui lui sont nommés vérifient si les conditions fixées par la législation pour bénéficier d'un régime ou d'un régime particulier sont effectivement (toujours) remplies. Dans le cadre de cette mission, certaines données à caractère personnel doivent être vérifiées. S'il apparaît qu'une condition n'est pas (plus) respectée, l'inspecteur social peut établir un rapport dans lequel il peut consigner les constatations, les interrogatoires et les infractions constatées. Celle-ci est accompagnée de la notification nécessaire à l'intéressé en vue de sauvegarder ses droits. La détection des infractions donnera lieu, le cas échéant, à une procédure pénale, à l'imposition d'une amende administrative, à l'abrogation d'une faveur ou d'un statut ou au recouvrement des sommes versées.

11. Le décret susmentionné du 30 avril 2004 contient d'autres règles relatives au fonctionnement de l'Inspection sociale flamande. En vertu de l'article 6, § 1, 6°, les inspecteurs social ont le pouvoir d'établir un rapport, qui enregistre toutes les constatations et les auditions ainsi que les infractions constatées à l'encontre de la législation susmentionnée et contient au moins certains éléments bien définis (tels que le lieu et la durée de l'infraction, le résumé des faits, l'identité des acteurs et la législation applicable). En vertu de l'article 7, paragraphe 2, les inspecteurs sociaux disposent, dans l'exercice de leurs fonctions, de larges pouvoirs, y compris le droit d'effectuer toute enquête, inspection et audition des personnes concernant des faits pertinents et d'obtenir toutes les informations qu'ils jugent nécessaires pour assurer le respect effectif des dispositions de la législation dont ils sont soumis.

12. Le demandeur relève que l'identification immédiate (correcte et sans ambiguïté) sur le terrain apporte une valeur ajoutée importante, telle que le contrôle des personnes en séjour irrégulier, la détection de faux travailleurs et de faux travailleurs indépendants qui cherchent illégalement à obtenir un titre de séjour ou une prestation sociale et de vérifier si les personnes interrogées bénéficient d'une prestation. Lorsqu'un inspecteur sur place interroge une personne, il tente de les identifier dans MyDia et consulte les données pour vérifier s'il n'y a pas d'anomalie. S'il consulte par erreur les données d'une personne qui n'est pas la personne interrogée, il ajuste ses critères de recherche et ne conserve aucune donnée, tandis que les *logs* de sécurité enregistrent que l'inspecteur a consulté les données de cette personne. Si la

---

une capacité professionnelle en gestion des utilisateurs et des accès (UAM). Lorsqu'un nouveau document est affiché dans l'eBox professionnelle, l'inspecteur reçoit une notification dans sa boîte aux lettres professionnelle.

personne est en règle de manière générale, l'inspecteur doit conserver l'identifiant de l'entreprise et l'ID technique ainsi qu'un certain nombre de *flags* pour indiquer que la personne a été identifiée sur le site et que la personne apparaît dans le résumé. Si la personne n'est pas en règle de manière générale, l'inspecteur conserve les mêmes données dans MyDia, mais établit également un rapport et remplit un formulaire papier pour le suivi de l'enquête. Lorsque l'inspecteur ferme le contrôle (il a 24 heures de temps pour cela, puis le contrôle est automatiquement fermé), les données sont envoyées à l'eBox et elles sont disponibles via le service web *FieldInspection*. Il ne concerne toujours que les données d'identification d'entreprise et les données d'identification technique et un certain nombre d'indicateurs, mais pas les données commerciales des services consultés.

13. De retour au bureau, l'inspecteur peut demander la liste des personnes identifiées sur les lieux avec quelques *flags* pour indiquer les mesures à prendre. Il a trois jours pour récupérer ces données, après quoi son travail sera perdu. Les données sont physiquement supprimées, à la fois de l'eBox et de *FieldInspection*. Ils ne sont pas archivés parce qu'ils sont destinés à être stockés dans les applications commerciales de l'inspecteur lorsqu'ils sont récupérés. Ces applications commerciales sont la source authentique du résultat de l'audit. Si d'autres recherches sont nécessaires, l'inspecteur devra utiliser DOLSIS (ou un autre service) pour consulter les sources authentiques. MyDia n'est pas une option.

14. MyDIA est une application visant à soutenir le travail sur le terrain (les actions de contrôle dans les lieux où les salariés ou les travailleurs indépendants sont actifs, dans les secteurs où il y a une forte probabilité d'infractions) des inspecteurs sociaux. Ces contrôles sont souvent intensifs et prennent beaucoup de temps et nécessitent un niveau élevé de préparation et de coordination de la part des participants. Les actions de contrôle sur le terrain sont généralement des actions communes et nécessitent une approche multidisciplinaire, ce qui signifie que, en fonction de l'ampleur du contrôle et des problèmes suspectés, plusieurs services d'inspection participent. MyDIA offre à ces différents services d'inspection un outil transversal qui soutient la coopération multidisciplinaire et rend l'approche des contrôles sur place plus efficace. En outre, la qualité des échanges est également améliorée car tous les participants ont la même vision de l'information. De cette façon, une interprétation commune des résultats obtenus est également obtenue, car chaque personne a accès aux mêmes informations et est proposée de manière uniforme.

15. Le Département du travail et de l'économie sociale appelle à une délibération d'une durée indéfinie. Les tâches de l'Inspection sociale flamande, sur la base de l'arrêté du 30 avril 2004 *relatif à l'uniformisation des dispositions en matière de contrôle, de sanction et de pénal prévues par la législation du droit social pour lesquelles la Communauté flamande et la Région flamande sont compétentes,* ne sont pas limitées dans le temps.

16. Les données à caractère personnel ne seront conservées que temporairement si l'inspecteur social ajoute volontairement une personne, une entreprise ou un chantier à un contrôle. Le stockage ne se fait pas sur l'appareil mobile et se limite aux données susmentionnées. À la fin de la vérification, un fichier texte est créé sur un serveur sécurisé (et non sur l'appareil mobile de l'utilisateur) basé sur les données enregistrées. Il est envoyé à l'eBox des inspecteurs du droit social concernés et y est stocké pendant trois jours, puis automatiquement supprimé. Ce fichier texte (avec l'identité des parties concernées et les

commentaires sur le dossier) peut être utilisé pour consulter les sources authentiques de données à caractère personnel. Le service web *FieldInspection* n'est en aucun cas une source authentique ou une copie d'une source authentique. Le système assure le retrait automatique du rapport de la base de données temporaire FieldInspection (après 24 heures) et de l'eBox (après 72 heures). Le stockage électronique temporaire des données constitue une alternative sécurisée à la gestion des fichiers papier.

15. Les données à caractère personnel ne sont accessibles qu'aux employés désignés de l'Inspection sociale flamande (le personnel chargé du suivi et de l'application de la réglementation). En aucun cas des tiers n'ont accès aux données à caractère personnel.

16. Afin de s'acquitter de ses tâches, le Département du travail et de l'économie sociale souhaite un accès permanent à certaines données à caractère personnel provenant du réseau de sécurité sociale. Après tout, les différents contrôles sont effectués tout au long de l'année.

II. TRAITEMENT DE LA DEMANDE

A. RECEVABILITE DE LA DEMANDE ET COMPETENCE DU COMITE

17. En vertu de l'article 35/1, §1, premier alinéa, de la loi du 15 août 2012 *à la création et à l'organisation d'un 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 tiers autres que les institutions de sécurité sociale visées à l'article 2, alinéa 1er, 2°, 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 une délibération préalable de la chambre autorité fédérale du comité de sécurité de l'information, dans la mesure où les responsables du traitement de l'instance qui communique et des instances destinatrices 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.

18. Le Comité de sécurité de l'information prend note du fait qu'aucun protocole n'a été établi entre les parties concernées et qu'une demande d'admission a été présentée. La demande est recevable et le Comité se considère compétent.

B. QUANT AU FOND

B.1. RESPONSABILITE

19. Conformément à l'article 5.2 du Règlement général sur la protection des données[2] (ci-après dénommé «RGPD»), le SPF Finances (l'instance qui communique les données) et le Bureau fédéral du plan (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 démontrer[3].

[2] 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 (règlement général sur la protection des données)

[3] Les données à caractère personnel doivent être:

20. Le RGPD impose toute une série d'obligations qui incombent aux responsables de traitement. A cet égard, le présent rapport passe en revue les principales obligations qui sont prévues explicitement par le RGPD mais rappelle et insiste à ce stade-ci de son analyse sur celle qui impose à tout responsable du traitement de tenir un registre des activités de traitement conformément et dans le respect des modalités prévues à l'article 30 du RGPD.

B.2. LICEITE

21. 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.

22. Le Comité note que le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis (article 6.1 c RGDP). Le décret du 30 avril 2004 *relatif à l'uniformisation des dispositions en matière de contrôle, de sanction et de droit pénal contenues dans la législation du droit social relevant de la compétence de la Communauté flamande et de la Région flamande* régit les compétences des inspecteurs sociaux de l'Inspection sociale flamande du Département du travail et de l'économie sociale. Ils peuvent établir un compte rendu de l'ensemble des constatations et auditions ainsi que des infractions constatées aux règles mentionnées, ainsi que des pouvoirs étendus dans l'exercice de leurs fonctions, tels que le droit d'effectuer des enquêtes, des contrôles et des interrogatoires de personnes sur des faits pertinents et d'obtenir les informations qu'ils jugent nécessaires pour vérifier que les règles placées sous leur contrôle sont effectivement respectées. Les inspecteurs sociaux sont chargés du contrôle et de la supervision des lois fédérales et des décrets et décrets d'application du Conseil flamand et des décrets d'application énumérés aux articles 2 et 3 dudit décret. En ce qui concerne plus particulièrement l'accès à la base de données des permis uniques de l'Office des étrangers,

---

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).

le Comité de sécurité de l'information note que, à l'article 2, §1, 57°, le décret susmentionné du 30 avril 2004 fixe les pouvoirs des inspecteurs chargés du contrôle et de la surveillance de la loi du 30 avril 1999 sur l'emploi des travailleurs étrangers.

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 (principe de finalité).

24. Le projet MyDIA s'inscrit dans le cadre des différentes actions déjà entreprises ces dernières années pour améliorer la coopération transversale entre les inspections sociales et la lutte contre la fraude sociale. L'application mobile fournit aux inspecteurs du droit social concernés un outil permettant d'accéder aux données personnelles les plus récentes en ligne rapidement, facilement et en toute sécurité, d'identifier les personnes qui n'ont pas de documents d'identité officiels sans avoir à faire appel à la police et de faciliter la préparation et le suivi. Ils peuvent ainsi gagner du temps à effectuer des contrôles, à détecter les anomalies et à fournir un retour d'information aux organisations compétentes. Ils peuvent également trouver rapidement des informations sur les chantiers et les employés qui y sont présents, tels que le type d'employé disponible dans DIMONA et LIMOSA, l'enregistrement effectif des présences dans Checkin@work, la chaîne de sous-traitants et la position d'une entreprise dans cette chaîne. Ils peuvent également vérifier les différentes obligations des parties dans un chantier (salariés, employeurs, indépendants, coordinateurs de chantier, etc.) afin de gagner du temps. Ils peuvent également vérifier si les différents rapports relatifs au chantier ont été établis. En ce qui concerne les travailleurs temporaires, l'utilisateur est responsable de la santé et de la sécurité du travailleur et l'inspecteur social peut rapidement identifier cet utilisateur en utilisant MyDIA.

25. Compte tenu de ce qui précède, le Comité de la sécurité de l'information considère que les finalités de la communication envisagée de données à caractère personnel sont déterminées, explicites et légitimes.

B.4. PROPORTIONALITE

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 («minimisation des données»).

27. Les données à caractère personnel contenues dans la base de données MOVIBIS du SPF Mobilité permettra aux inspecteurs du droit social d'identifier l'employeur des salariés soumis au contrôle dans la mesure où cela n'est pas possible sur la base d'autres moyens. Par conséquent, comme le prévoit la délibération no 20/017 du 7 juillet 2020 de la chambre autorité fédérale du Comité de sécurité de l'information, la communication des données à caractère personnel à partir de la base de données MOVIBIS du SPF Mobilité devrait se limiter à l'identification de la personne (juridique) sur le nom de laquelle un véhicule particulier trouvé au cours d'une inspection est enregistré: prénom, nom, date de naissance, adresse, numéro INSZ et numéro d'entreprise du titulaire du véhicule. La recherche peut être effectuée à l'aide de la plaque d'immatriculation ou du numéro de châssis.

28. Le Comité de sécurité de l'information note en outre que la communication des données prévues par l'Office des étrangers du SPF Intérieur se limite à la décision de séjour positive ou négative concernant la personne concernée. L'accès direct à ces données est nécessaire pour les inspecteurs sociaux afin de pouvoir contrôler l'application des dispositions légales et réglementaires concernant le séjour et l'emploi des travailleurs étrangers et l'exercice d'activités professionnelles indépendantes par des ressortissants étrangers.

29. Seuls les inspecteurs du droit social de l'Inspection sociale flamande (le personnel chargé du contrôle et de l'application de la réglementation) ont accès aux bases de données susmentionnées.

B.4.2. Limitation de conservation

30. En ce qui concerne le délai de conservation, le Comité rappelle que les données à caractère personnel ne doivent plus être conservées sous une forme permettant d'identifier les personnes concernées au-delà des finalités pour lesquelles les données à caractère personnel sont traitées.

31. Les données à caractère personnel ne sont conservées dans la base de données *FieldInspection* que si l'inspecteur social ajoute volontairement une personne, une entreprise ou un chantier identifié à une inspection. Le stockage n'est pas effectué sur l'appareil et est également limité aux données à caractère personnel susmentionnées. Par conséquent, il n'y a pas de copie complète de toutes les données à caractère personnel consultées dans les différentes sources authentiques. À la fin de la vérification, un fichier texte est créé sur la base des données personnelles enregistrées sur un serveur sécurisé. Il est envoyé à l'eBox des inspecteurs sociaux concernés et y est stocké pendant trois jours, puis automatiquement supprimé. Sur la base de ce fichier texte (limité) (avec l'identité des parties concernées et les commentaires sur l'enquête), les inspecteurs du droit social peuvent consulter les sources de données à caractère personnel authentiques. Le système assure le retrait automatique après 72 heures du rapport de l'eBox et après 24 heures de la base de données temporaire *FieldInspection*.

B.5. SECURITE

32. Les données à caractère personnel doivent être traitées en prenant des mesures techniques et organisationnelles appropriées de manière à assurer un niveau de sécurité adéquat, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle («intégrité et confidentialité»).

33. Le Comité de sécurité de l'information évalue la sécurité du système de consultation des banques de données à caractère personnel du réseau de sécurité sociale avec la possibilité de stocker temporairement un ensemble limité de données à caractère personnel consultées. En outre, elle l'a déjà fait dans sa délibération 20/126 du 31 juillet 2020, modifiée le 7 décembre 2021, sur la consultation de différentes banques de données à caractère personnel par divers services d'inspection sociale (fédéral) par le biais de l'application MYDIA. Avec cette application, les inspecteurs du droit social peuvent lier les données à caractère personnel consultées à un contrôle dont ils sont un acteur participant et stocker pendant trois jours au maximum, ainsi que des informations sur l'interprétation de leurs conclusions. À la fin du contrôle, un fichier texte limité est créé et transmis à l'eBox des inspecteurs compétents sur

la base des données à caractère personnel enregistrées, au cours desquelles ils sont stockés pendant trois jours, puis automatiquement supprimés. Les tiers n'auraient pas accès aux données à caractère personnel ainsi traitées. Le stockage temporaire des données à caractère personnel vise à remplacer le fichier papier actuel (recherche) par un fichier électronique plus sûr (recherche).

34. La communication entre le serveur et l'application sur l'appareil mobile est sécurisée par cryptage. L'utilisateur de l'application est identifié par le serveur avec un outil d'authentification équivalent au niveau 450 tel que déterminé par le Service fédéral d'authentification (FAS). La session est limitée dans le temps et l'utilisateur se connecte à intervalles réguliers.

35. L'accès à l'application et aux informations disponibles sur le dispositif mobile par l'application doit être sécurisé par un *Mobile Device Management* (MDM) ou un système équivalent placé sous le contrôle de l'organisme sous l'autorité duquel les services d'inspection opèrent. Cette obligation incombe au responsable du traitement et il revient également à chaque utilisateur de prendre tous les précautions d'usage lors de l'utilisation de l'application. Au moins les mesures de sécurité suivantes sont appliquées.

- L'application MYDIA et les informations conservées associées sont séparées des applications non professionnelles sur l'appareil mobile au moyen d'un cryptage (containerisation[4]);
- L'accès au contenu est limité à l'utilisateur au moyen d'un mot de passe suffisamment complexe ou au moyen des informations biométriques de l'utilisateur;
- L'organisation a la possibilité d'effacer au moins les contenus de l'appareil mobile en cas de perte ou de vol ou lorsqu'il n'est plus souhaitable de mettre les informations et l'accès à la disposition de l'utilisateur (essuyage à distance);
- Avant le démarrage de l'application et l'accès à l'information, une vérification du système d'exploitation (OS) de l'appareil mobile est effectuée. S'il y a des indices que ce système d'exploitation n'est plus sûr, l'accès aux informations est refusé et les données conservées sont supprimées;
- Il y a une vérification de l'utilisation d'un logiciel de sécurité qui protège l'appareil contre les virus et réduit le risque de piratage;
- Il y a un contrôle sur le *jailbreaking*[5] de l'appareil.

36. L'organisation doit mettre en place les processus nécessaires pour soutenir la sécurité de l'utilisation de l'application. Il développe ou adapte l'*Acceptable Use Policy* en ce qui concerne l'utilisation d'appareils mobiles, avec au moins la protection par mot de passe de l'utilisateur, l'installation d'un programme antivirus, l'utilisation de réseaux WIFI et de points de recharge publics, la désactivation de la possibilité d'accéder à l'appareil via Mass Storage Device (MSD), le *jailbreak* ou l'enracinement de l'appareil, le cryptage de l'appareil, la mise à jour du système d'exploitation et du logiciel, l'installation d'applications et l'octroi de droits d'accès à ces applications. Il réglemente des programmes de sensibilisation

[4] Diviser des parties d'une application en blocs séparés, c'est-à-dire des conteneurs.
[5] Le "craquage" du système d'exploitation.

suffisants, qui portent les risques liés à l'utilisation des appareils mobiles à l'attention des utilisateurs, ainsi qu'un processus de gestion des incidents, qui tient compte de la perte de dispositifs mobiles et prévoit la suppression des données de l'application et la cessation de l'accès à l'application et aux sources authentiques. Il prévoit que les processus liés à l'évolution des effectifs tiennent également compte de l'attribution et de la suppression de l'accès des utilisateurs via l'appareil mobile et de la suppression des informations. L'organisation prévoit également régulièrement une *data protection impact assessement* pour cette application et prend les mesures appropriées en ce qui concerne les nouveaux risques. Les mesures nécessaires doivent être prises afin que les données collectées dans l'application MyDIA ne puissent pas être copiées et envoyées via une autre application privée sur l'appareil de l'utilisateur.

37. L'échange de données à caractère personnel a lieu en principe avec l'intervention de la Banque Carrefour de la Sécurité Sociale, conformément à l'article 14 de la loi du 15 janvier 1990 *portant création et organisation d'une banque de la sécurité sociale*.

38. L'accès au registre national et aux registres des banques de carrefour, à la base de données DIMONA, à la base de données DMFA, aux données *UnemploymentData et LivingWages*, au registre général des travailleurs indépendants, aux données à caractère personnel sur l'incapacité de travail et aux données à caractère personnel du DIV est une intervention physique, dans laquelle la Banque Carrefour de la Sécurité Sociale joue son rôle classique.

39. L'accès au répertoire employeur, à la base de données LIMOSA, au fichier GOTOT, au fichier de rapports de site, à la base de données «Enregistrement de Présence» (Checkin@work) et à la plateforme *Single Permit* est une intervention non physique, sans préjudice des tâches que l'organisation accomplit habituellement lors de la communication de données personnelles. Dans ce cas, il intervient d'une manière spécifique (technique). Pour chaque autorité utilisant l'application MyDIA, elle applique des règles appropriées en matière de gestion des accès et d'autorisations d'accès. En outre, il est responsable de l'enregistrement de toutes les communications entrantes et sortantes des données personnelles.

40. Dans la mesure où le département du travail et de l'économie sociale s'appuie sur un sous-traitant pour la réalisation de ce projet, les relations entre les deux parties sont pleinement réglementées conformément aux dispositions de l'article 28 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.*

41. Tous les employés de l'Inspection sociale flamande sont tenus par une obligation de confidentialité. Conformément à l'article 8, paragraphe 1, du décret du 30 avril 2004 *relatif à l'uniformisation des dispositions de contrôle, de sanction et de sanction figurant dans les règles de droit social pour lesquelles la Communauté flamande et la Région flamande sont compétentes*, les inspecteurs sociaux prennent les mesures nécessaires pour respecter la confidentialité des informations dont ils ont eu connaissance dans l'exercice de leurs fonctions et ne peuvent les utiliser que pour l'accomplissement de leurs tâches de surveillance et de contrôle.

42. Le département du travail et de l'économie sociale a désigné un délégué à la protection des données en application de l'article 37 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.*

43. Dans le cadre du traitement des données à caractère personnel, les parties tiennent compte de la loi du 15 janvier 1990 *portant création et organisation d'une banque de sécurité sociale* et de toute autre disposition 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 et la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel*.

Par ces motifs,

la chambre autorité fédérale du Comité de sécurité de l'information

conclut que la consultation de la base de données MOBIVIS du SPF Mobilité et de la plateforme Single Permit de l'Office des étrangers du SPF Intérieur par l'Inspection sociale flamande du département du travail et de l'économie sociale par le biais de l'application My Digital Inspection Assistant (MyDia), telle que décrite dans cette délibération, est autorisée moyennant le respect des mesures de protection des données définies, en particulier les mesures en matière de limitation de la finalité, de minimisation des données, de limitation de la durée de conservation des données et de sécurité de l'information.

Daniel HACHE
Président

Le siège de la chambre autorité fédérale du Comité de sécurité de l'information est établi dans les bureaux du SPF Stratégie et Appui à l'adresse suivante: Boulevard Simon Bolivar 30, 1000 Bruxelles.