



CONVENTION DE COMMUNICATION DE DONNÉES

entre

L'INASTI (n° d'entreprise BE 0208.044.709)

et

la Direction générale Transport routier et Sécurité routière (DGTRSR)

1. CADRE ET OBJET DE LA CONVENTION

Accès aux données de la Banque Carrefour des Véhicules (BCV)

La présente convention fixe les règles de la communication de données extraites du fichier de la DIV à INASTI à l'appui de la décision n° 19/007 du Comité de Sécurité de l'Information (CSI).

2. LES RESPONSABLES DU TRAITEMENT

Au sens de du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 privée, les responsables du traitement sont :

- a) La Direction pour l'Immatriculation des Véhicules (DIV), faisant partie de la Direction générale Mobilité et Sécurité routière du Service public fédéral Mobilité et Transports (n° d'entreprise 0308357852), dont le siège est situé City Atrium, rue du Progrès 56 à 1210 Bruxelles (Saint-Josse-ten-Noode) et représentée par Madame Martine INDOT, Directeur général Transport routier et Sécurité routière.
La DIV agit comme responsable du traitement en tant, notamment, qu'administration publique qui collecte et communique des données de son répertoire matricule des véhicules.
- b) INASTI (n° d'entreprise **BE 0208.044.709**), dont le siège est établi à Quai de Willebroeck 35, 1000 Bruxelles, représentée par Madame Anne Vanderstappen, Administrateur général), agissant au nom de INASTI.
INASTI agit comme responsable du traitement, reçoit des données de la DIV et qui les traite au sens des termes de la présente convention.

DIV et INASTI agissent par conséquence en qualité de responsables du traitement en tant qu'organismes qui déterminent les finalités et les moyens du traitement des données à caractère personnel (article 4 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016)

3. FOURNISSEUR ET DESTINATAIRE DES DONNÉES

Le fournisseur des données est la Direction générale Transport routier et Sécurité routière, mieux identifiée au point 2.a ci-avant et le destinataire des données est INASTI, mieux identifié(e) au point 2.b ci-avant et désigné(e) ci-après en cette qualité de « destinataire ».

4. OBJECTIF(S) AVALISÉ(S) PAR LE COMITÉ DE SECURITÉ DE L'INFORMATION

Sous réserve des conditions éventuelles mentionnées dans l'autorisation du CSI, la INASTI ne peut utiliser les données du répertoire de la BCV que pour les finalités telle qu'autorisée par le CSI dans le chapitre B.3 de sa décision N° 19/007 :

Tout autre objectif n'ayant pas reçu l'agrément formel du CSI ne pourra être légitimement utilisé.

5. DONNÉES COMMUNIQUÉES ET MODALITÉS D'EXÉCUTION

Voir, en annexe, l'autorisation N° 19/007, datée du 5 mars 2019, provenant du CSI. Les données sont communiquées via l'application Dolsis de la Banque Carrefour de la Sécurité Sociale.

6. LA SOUS-TRAITANCE

- a) Lorsque le traitement est confié à un sous-traitant, par exemple un service ICT, le responsable du traitement ou, le cas échéant, son représentant en Belgique, doit :
 - 1 ° choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements;
 - 2 ° veiller au respect de ces mesures notamment par la stipulation de mentions contractuelles;
 - 3 ° fixer dans le contrat la responsabilité du sous-traitant à l'égard du responsable du traitement;
 - 4 ° convenir avec le sous-traitant que celui-ci n'agit que sur la seule instruction du responsable du traitement et est tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu en application des dispositions du point c ci-après;
 - 5 ° consigner par écrit ou sur un support électronique les éléments du contrat visés aux 3 ° et 4 ° relatifs à la protection des données et les exigences portant sur les mesures visées aux dispositions du point c ci-après.
- b) Si le destinataire choisit un sous-traitant, un contrat de sous-traitance doit donc être conclu entre eux et une copie de ce document sera transmise au fournisseur (la DIV) ; ce contrat fera partie intégrante de la présente convention.
Le sous-traitant choisit par le destinataire respectera en tous points les termes du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.
- c) Toute personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi, d'un décret ou d'une ordonnance.
- d) En l'absence d'instructions de la part du responsable du traitement et en dehors d'une obligation imposée par ou en vertu d'une loi, d'un décret ou d'une ordonnance, le sous-traitant s'abstiendra de traiter des données à caractère personnel et ne prendra aucune initiative en la matière.
- e) Toute modification substantielle apportée par le destinataire aux mesures de sécurité technique et d'organisation relatives aux traitements doit être signalée au fournisseur (la DIV), comme, par exemple et non exhaustivement, un changement de matériel informatique ou un changement de sous-traitant.

7. RESTRICTIONS ÉVENTUELLES

En vertu du RGPD, les personnes concernées disposent d'un certain nombre de droits en ce qui concerne leurs données à caractère personnel.

Concrètement, les personnes concernées disposent des droits suivants (moyennant le respect de conditions et exceptions prévues dans le RGPD) :

- Droit d'accès (art. 15) ;
- Droit de rectification (art. 16) ;
- Droit à l'effacement (art. 17) ;
- Droit à la limitation du traitement (art.18) ;
- Droit d'opposition (art. 21) ;
- Droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques concernant la personne ou l'affectant de manière significative de façon similaire (art. 22) ;

Les Parties s'engagent à remplir les obligations découlant de l'exercice de ces droits par les personnes concernées, conformément à l'article 12 RGPD. Cela signifie que, à condition que la personne concernée prouve son identité et introduise sa demande par un écrit daté, elle pourra obtenir gratuitement, de la part des Parties, la communication des données la concernant ou la rectification des données incomplètes ou incorrectes.

En pratique, moyennant la preuve de l'identité de la personne concernée et sur base d'une demande datée et signée de sa part, celle-ci peut obtenir, sans frais, auprès du destinataire (dont l'adresse est mentionnée au point 2.b de la présente convention) la communication des données la concernant ainsi que la rectification de ces données si celles-ci se révèlent incomplètes, incorrectes ou excessives.

Cette même demande peut être effectuée par courrier électronique à l'adresse suivante : privacy@rsvz-inasti.fgov.be

Le destinataire, en cette qualité, doit fournir à la personne concernée au moins les informations suivantes, sauf si cette dernière en est déjà informée :

- a) Les coordonnées complètes du siège administratif du destinataire et, le cas échéant, le nom et l'adresse de son représentant.
- b) Les finalités du traitement.
- c) L'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement des données à caractère personnel la concernant envisagé à des fins de *direct marketing* ; dans ce cas, la personne concernée doit être informée avant que des données à caractère personnel ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de *direct marketing*.
- d) D'autres informations supplémentaires, notamment :
 - les catégories de données concernées ;
 - les destinataires ou les catégories de destinataires ;
 - l'existence d'un droit d'accès et de rectification des données la concernant ;sauf dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont traitées, ces informations supplémentaires ne sont pas nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.
- e) L'existence du présent protocole d'accord.

8. BASES NORMATIVES

a) Pour la DIV :

- l'article 6 de l'arrêté royal du 20 juillet 2001 relatif à l'immatriculation de véhicules ainsi que son répertoire-matricule créé en vertu de cet arrêté royal.
- Loi du 19 mai 2010 portant création de la Banque-Carrefour des Véhicules.
- Arrêté royal du 8 juillet 2013 portant exécution de la loi du 19 mai 2010 portant création de la Banque-Carrefour des véhicules.

b) Pour le destinataire :

- L'article 23bis, § 2, de l'arrêté royal n° 38 du 27 juillet 1967 organisant le statut social des travailleurs indépendants

9. CONDITIONS DE L'ACCORD

- a) En signant le présent accord, chacune des parties s'engage à respecter les conditions et modalités décrites dans l'accord et dans ses annexes éventuelles, notamment la durée de conservation des données à caractère personnel reçues de la DIV qui ne peut excéder celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement.

10. MODIFICATIONS DE L'ACCORD

Toute modification apportée au texte et au principe du présent accord fera obligatoirement partie intégrante d'un nouvel accord écrit, approuvé et signé par les deux parties.

11. POINTS DE CONTACT

- a) Pour le destinataire : privacy@rsvz-inasti.fgov.be
b) Pour la DIV : vehicledata.exchange@mobilif.fgov.be

12. UTILISATION ET SÉCURISATION DES DONNÉES

En vertu des articles 32 à 34 RGPD, le responsable du traitement et le sous-traitant sont tenus de protéger les données à caractère personnel contre les atteintes à la sécurité qui pourraient entraîner, accidentellement ou illégalement, la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé à ces données à caractère personnel.

La INASTI s'engage à prendre les mesures techniques et organisationnelles appropriées afin de protéger les données à caractère personnel contre tout traitement non autorisé ou illégal, toute perte ou modification des données à caractère personnel, ainsi que pour éviter ou réduire le risque de violations, contre la perte ou le vol accidentels de données, contre des modifications, contre un accès non autorisé ou abusif et toute autre utilisation illégale de données à caractère personnel. En concluant le présent protocole, la INASTI est certaine que les réseaux auxquels sont connectées les installations impliquées dans le traitement des données à caractère personnel garantissent la confidentialité et l'intégrité de ces données.

En cas d'atteinte à la sécurisation, la INASTI s'engage à avertir immédiatement la DGTRSR selon les modalités convenues.

Les Parties s'informent mutuellement des modifications substantielles aux mesures techniques et organisationnelles de sécurité concernant le traitement des données prévu dans le présent protocole.

13. DURÉE ET RÉSILIATION DE LA CONVENTION

- a) La présente convention est conclue pour une durée indéterminée et prend cours à la date de sa signature par les deux parties.
- b) Elle peut être résiliée par une des parties moyennant un préavis de 3 mois sauf dispositions expresses indiquées au point 14 de la présente convention (clause de nullité – sanction).

14. SANCTIONS

Toute utilisation des données reçues à des fins autres que celles prévues par le présent protocole est strictement interdite et entraîne, sans exception, l'annulation du présent protocole.

En cas de manquement apparent à la bonne mise en œuvre du présent protocole par la INASTI ou, s'il apparaît que la transmission des données contrevient à toute disposition légale ou réglementaire qui lui est applicable, la DGTRSR peut – sans préjudice de l'application du Titre 6 de la Loi sur la protection des données – sans mise en demeure préalable, suspendre la transmission des données visées au présent protocole ou procéder à sa dissolution intégrale.

Dans une telle situation, la DGTRSR porte à la connaissance de la INASTI par lettre recommandée ou par email avec accusé de réception, les raisons de la suspension ou de la résiliation.

15. ANNEXES

Toute annexe pourra décrire, au besoin et dans le détail, la portée de la collaboration, la durée éventuelle du projet, les conditions à remplir et moyens à mettre en œuvre par chacune des parties.

En annexe de la présente :

- La délibération du Comité de sécurité de l'information

16. PROTECTION DE LA VIE PRIVÉE

Dans le cadre de leurs relations, les Parties s'engagent à respecter, outre la loi de protection des données à caractère personnel, notamment, les dispositions suivantes :

- Le RGPD ;
- 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' (ci-après « loi comité de sécurité de l'information ») ;
- La Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil
- Les avis et recommandations de(s) autorité(s) de contrôle, en particulier l'Autorité chargée de la protection des données, conformément à la loi du 3 décembre 2017 'portant création de l'Autorité de protection des données' (ci-après « loi du 3 décembre 2017 »).

17. TRANSPARENCE

- a) Les parties concernées par la convention ainsi conclue marquent leur accord pour que celle-ci figure intégralement sur le site Internet du SPF Mobilité et Transports, dénommé www.mobilit.fgov.be.
- b) Des exemplaires « papiers » de cette convention sont également disponibles sur simple demande écrite à la DIV ou au destinataire aux adresses postales indiquées aux points 2.a et 2.b de la présente convention ou aux adresses électroniques «help.DIV@mobilit.fgov.be » ou «privacy@rsvz-inasti.fgov.be ».

18. DIFFÉRENCES INTERPRÉTATIVES DE LA PRÉSENTE CONVENTION

Les parties contractantes s'engagent à trouver une solution aux difficultés qui pourraient surgir quant aux différences d'interprétation de la présente convention, de ses annexes et de ses avenants. En cas de situation conflictuelle générée par des différents sur l'interprétation de cette convention, avantage sera toujours accordé à la résolution de l'Autorité de protection des données.

Fait à Bruxelles, le 13 juin 2022 en deux exemplaires, chaque partie reconnaissant avoir reçu un exemplaire.

Pour INASTI,



Anne Vanderstappen
Administrateur général

Pour la DIV,

Martine Indot
(Signature)

Signature numérique de Martine
Indot (Signature)
Date : 2022.06.23 17:55:05 +02'00'

Martine INDOT
Directeur général
Transport routier et Sécurité routière

Remarque :

Le texte en rouge et en bleu claire est à compléter par le destinataire des données et sera ensuite intégré normalement au libellé de la convention

Comité de sécurité de l'information
Chambres Réuniones

FO/19/006

DÉLIBÉRATION N° 19/007 DU 5 MARS 2019 RELATIVE À LA COMMUNICATION DES DONNÉES À CARACTÈRE PERSONNEL PAR LA DIRECTION GÉNÉRALE MOBILITÉ ET SÉCURITÉ ROUTIÈRE DU SERVICE PUBLIC FÉDÉRAL MOBILITÉ ET TRANSPORTS À L'INSTITUT NATIONAL D'ASSURANCES SOCIALES POUR TRAVAILLEURS INDÉPENDANTS PAR LE BIAIS DE L'APPLICATION WEB DOLSIS DANS LE CADRE DE L'IDENTIFICATION DES CONTREVENANTS À LA RÉGLEMENTATION DU STATUT SOCIAL DES TRAVAILLEURS INDÉPENDANTS

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 ;

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

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*, en particulier les articles 95, 97 et 98 ;

Vu la demande de l'Institut National d'Assurances Sociales pour Travailleurs Indépendants ;

Vu le rapport du Service public fédéral Stratégie et Appui ;

Vu le rapport de la Présidente.

I. OBJET DE LA DEMANDE

1. L'Institut national d'assurances sociales pour travailleurs indépendants (dénommé ci-après « le demandeur » ou « l'INASTI ») souhaite obtenir la communication des données à caractère personnel par la Direction d'Immatriculation des Véhicules (DIV) de la Direction Circulation routière de la Direction générale Mobilité et Sécurité routière du Service public fédéral Mobilité et Transports (dénommée ci-après la « DIV ») aux contrôleurs et inspecteurs sociaux de l'INASTI. Les données à caractère personnel sont destinées à identifier, à l'aide de leur plaque d'immatriculation, les contrevenants à la législation de la sécurité sociale et à

la réglementation européenne, plus spécifiquement dans le cadre de la lutte contre la fraude sociale. Ces données doivent également permettre d'assurer un meilleur suivi des priorités de l'INASTI en matière de fraude sociale.

2. L'arrêté royal du 20 juillet 2001 relatif à l'immatriculation des véhicules stipule précisément que les données du répertoire de la DIV peuvent être traitées pour la recherche et la poursuite pénale des crimes, délits et contraventions.
3. En 2012, quatre services d'inspection ont déjà été autorisés par le Comité sectoriel pour l'Autorité fédérale à accéder à plusieurs données de la DIV en vue de l'exécution de leurs tâches de contrôle et d'inspection. Il s'agissait plus précisément de l'Office national de l'emploi¹, de l'Office national de sécurité sociale², du Service public fédéral Sécurité sociale³ et du Service public fédéral Emploi, Travail et Concertation sociale⁴. En 2017, les autorisations ont été uniformisées⁵.
4. Au cours des dernières années, la collaboration entre les services d'inspection s'est intensifiée dans le cadre de la lutte contre la fraude sociale. Celle-ci s'accompagne souvent d'actions lors desquelles les inspecteurs des différentes inspections collaborent à un contrôle, faisant disparaître une répartition du travail stricte. Une répartition pratique préalable des tâches devient de plus en plus la règle dans un contrôle commun. L'accès aux données de la DIV via l'application web Dolsis permet de mener une approche commune dans la lutte contre la fraude sociale en utilisant des moyens communs.
5. En raison de la réforme et de la redéfinition des services d'inspection sociaux, une nouvelle structure a été mise en place dans le cadre de la lutte contre la fraude sociale et le dumping social au sein de l'INASTI, appelée Direction Concurrence loyale (ECL). Outre les compétences classiques du service d'inspection de l'INASTI (dont le contrôle des abus par des travailleurs indépendants en incapacité de travail), les compétences de la direction ECL portent sur les domaines suivants :
 - la lutte contre les faux statuts (faux indépendants – faux salariés) ainsi que le contrôle de la législation de sécurité sociale applicable à un travailleur indépendant ;
 - la lutte contre les affiliations fictives (les affiliations en tant que travailleur indépendant pour obtenir un droit de séjour et d'autres avantages sociaux) ;
 - la lutte contre le travail non déclaré ;
 - la lutte contre le dumping social.
6. Le service Inspection de la direction ECL effectue toutes sortes d'enquêtes sur demande des services opérationnels, de sa propre initiative, sur demande de l'auditorat du travail ou une autre institution, sur demande d'un autre service d'inspection ou en collaboration avec ce dernier.

¹ Délibération n° 07/2012 du 31 mai 2002.

² Délibération n° 11/2012 du 31 mai 2002.

³ Délibération n° 12/2012 du 31 mai 2002.

⁴ Délibération n° 13/2012 du 31 mai 2002.

⁵ Délibération n° 19/2017 du 29 juin 2017.

7. L'INASTI a déjà été autorisé par le Comité sectoriel de la sécurité sociale et de la santé à accéder via l'application web Dolsis, en vue de l'exécution de ses tâches de contrôle et d'inspection, aux données à caractère personnel des banques de données suivantes : les registres de la Banque-Carrefour, la banque de données à caractère personnel DIMONA et le fichier de personnel des employeurs inscrits auprès de l'Office national de sécurité sociale (ONSS) et de l'Office national de sécurité sociale des administrations provinciales et locales (ONSSAPL), la banque de données à caractère personnel DmfA de l'ONSS et de l'ONSSAPL, le répertoire des employeurs de l'ONSS et de l'ONSSAPL, le cadastre LIMOSA (« *Landoverschrijdend Informatiesysteem ten behoeve van MigratieOnderzoek bij de Sociale Administratie - Système d'information transfrontalier en vue de la recherche en matière de migration auprès de l'administration sociale* ») et l'application GOTOT (« *GrensOverschrijdende Tewerkstelling – Occupation Transfrontalière* »), le fichier des déclarations de travail, la banque de données « enregistrement des présences » (Check in At Work) et la banque de données des attestations multifonctionnelles⁶.
6. L'application web Dolsis a été spécifiquement développée pour ouvrir les sources authentiques aux services de contrôle et d'inspection des communautés, des régions et de l'autorité fédérale. Les modalités de l'application Dolsis ont été fixées dans la recommandation n° 12/01 du 8 mai 2012 du Comité sectoriel de la sécurité sociale et de la santé.
7. Concrètement, l'INASTI souhaite accéder aux données à caractère personnel suivantes de la DIV : plaque d'immatriculation ; prénom, nom de famille, date de naissance, adresse, numéro de registre national et numéro d'entreprise du titulaire du véhicule ; dénomination officielle de l'entreprise ; marque du véhicule ; nom du constructeur automobile ; type, variante, exécution, dénomination commerciale, numéro de châssis, modèle, catégorie, type de carburant, émissions de CO₂, masse de chargement maximale autorisée, masse en ordre de marche, masse de référence, masse maximale autorisée, date de la première immatriculation, durée de validité de l'immatriculation provisoire, date d'immatriculation, date de radiation, statut de l'immatriculation, nombre de places assises et nombre de places debout du véhicule.

II. EXAMEN DE LA DEMANDE

A. RECEVABILITÉ ET COMPÉTENCE DU COMITÉ

8. En vertu de l'article 35/1, § 1, 3^e alinéa de la loi du 15 août 2012 *relative à la création et à l'organisation d'un intégrateur de services fédéral*, la communication de données à caractère personnel par les services publics et les institutions publiques de l'autorité fédérale à des institutions de sécurité sociale visées à l'article 2, alinéa premier, 2^o, a), de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, requiert une délibération préalable des chambres réunies du comité de sécurité de l'information si les responsables du traitement de l'institution communiquant les données, de l'institution destinataire et de la Banque-carrefour de la sécurité sociale, en exécution de l'article 20 de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, ne parviennent pas à un accord

⁶ Délibération CSSSS n° 13/020 du 5 mars 2013, modifiée le 7 juin 2016 et le 3 juillet 2018.

sur la communication ou si au moins un de ces responsables demande une délibération et en a informé les autres responsables du traitement.

9. Le Comité souligne que l'article 20 de loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, (ci-après « LTD ») n'entre en vigueur que le 1^{er} avril 2019. Il ne peut dès lors pas encore être satisfait à la condition telle que prévue à l'article 35/1 précité de la loi du 15 août 2012. La communication visée des données par la Direction générale Mobilité et Sécurité routière du Service public fédéral Mobilité et Transports requiert dès lors une délibération sur la base de l'article 35/1 de la loi précitée du 15 août 2012.
10. En vertu de l'article 35/1, § 2, de la loi du 15 août 2012 *relative à la création et à l'organisation d'un intégrateur de services fédéral* et en vertu de l'article 15, § 3, de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, la chambre autorité fédérale et la chambre sécurité sociale et santé respectivement peuvent également fournir, pour autant qu'elles doivent fournir une délibération pour une communication des données à caractère personnel, une délibération pour l'utilisation du numéro d'identification du Registre national des personnes physiques par les institutions concernées si cela est nécessaire dans le cadre de la communication visée.
11. Compte tenu de ce qui précède, le Comité est donc compétent pour s'exprimer par rapport à la communication de données à caractère personnel par la Direction générale Mobilité et Sécurité routière du Service public fédéral Mobilité et Transports au demandeur et à l'utilisation du numéro de Registre national.

B. QUANT AU FOND

B.1. RESPONSABILITÉ

12. Conformément à l'article 5, § 2, du Règlement général sur la protection des données⁷ (ci-après dénommé « RGPD »), il incombe tant à la Direction générale Mobilité et Sécurité routière du Service public fédéral Mobilité et Transports qu'à l'INASTI, en tant que responsables du traitement, de veiller au respect des principes du RGPD et d'être en mesure de le démontrer.
13. Le Comité indique qu'en exécution de l'article 30 du RGPD, tant le demandeur que la Direction générale Mobilité et Sécurité routière du Service public fédéral Mobilité et Transports doivent tenir un registre des activités de traitement effectuées sous leur responsabilité conformément aux conditions prévues audit article.

B.2. LICÉITÉ

14. Conformément à l'article 5, § 1^{er}, a), du RGPD, les données à caractère personnel doivent être traitées de manière licite au regard de la personne concernée. Cela implique que tant le traitement initial (par la Direction générale Mobilité et Sécurité routière du Service public fédéral Mobilité et Transports) que le traitement ultérieur (communication à l'INASTI et utilisation des données par celui-ci) doivent être basés sur l'un des fondements de licéité mentionnés à l'article 6 du RGPD.

⁷ 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.

15. Le traitement initial des données à caractère personnel par la Direction générale Mobilité et Sécurité routière du Service public fédéral Mobilité et Transports est licite étant donné qu'il est nécessaire pour satisfaire à une obligation légale qui incombe au responsable du traitement (art. 6, § 1^{er}, c), du RGPD). Les données qui seront transmises par la Direction générale Mobilité et Sécurité routière du Service public fédéral Mobilité et Transports au demandeur seront initialement collectées et traitées dans le cadre de l'arrêté royal du 20 juillet 2001 relatif à l'immatriculation des véhicules.
16. La communication de données à caractère personnel et le traitement des données à caractère personnel par l'INASTI est licite étant donné que le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement (art. 6, § 1^{er}, e), du RGPD).
17. L'article 23bis, § 2, de l'arrêté royal n° 38 du 27 juillet 1967 *organisant le statut social des travailleurs indépendants* stipule que les inspecteurs et les contrôleurs sociaux de l'Institut national surveillent le respect des obligations découlant de l'application de l'arrêté royal précité et des régimes visés par l'article 18 de cet arrêté. Les compétences légales du service d'inspection de l'INASTI incluent le contrôle des abus par les travailleurs indépendants en incapacité de travail, la lutte contre les faux statuts, contre les affiliations fictives, contre le travail non déclaré et contre le dumping social.

B.3. LIMITATION DES FINALITÉS

18. Conformément à l'article 5, § 1^{er}, b), du RGPD, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.
19. Comme mentionné précédemment, les données ont été initialement collectées par la Direction générale Mobilité et Sécurité routière du Service public fédéral Mobilité et Transports dans le cadre de l'arrêté royal du 20 juillet 2001 relatif à l'immatriculation des véhicules. L'article 6, § 2, 1^o, de l'arrêté royal précité stipule expressément que les données sont traitées dans le répertoire de la DIV pour la recherche et la poursuite pénale des crimes, délits et contraventions.
20. La communication visée des données à caractère personnel au service d'inspection de l'INASTI poursuit les finalités concrètes suivantes, qui sont indiquées en détail dans la demande :
 - une lutte efficace contre les faux indépendants, plus spécifiquement l'application de la loi-programme du 27 décembre 2006 *relative à la nature des relations de travail* ;
 - l'amélioration de l'efficacité de l'organisation et des contrôles
 - le dumping social dans un contexte européen.
21. Le Comité est donc d'avis que les données à caractère personnel en question sont collectées à des fins déterminées, explicites et légitimes. Compte tenu du fait que la finalité du traitement ultérieur s'inscrit dans l'une des finalités légales du répertoire de la DIV (recherche et poursuite pénale des crimes, délits et contraventions) et vu les dispositions du

Code pénal social⁸, le Comité estime que la finalité de collecte initiale n'est pas incompatible avec celle du traitement ultérieur.

B.4. LOYAUTÉ ET TRANSPARENCE

22. Conformément à l'article 5, § 1^{er}, a), du RGPD, les données à caractère personnel doivent être traitées de manière loyale et transparente au regard de la personne concernée. L'article 12 du RGPD oblige le responsable du traitement à prendre des mesures appropriées pour fournir toute information visée aux articles 13 et 14 du RGPD (c'est-à-dire les informations à fournir lorsque les données sont collectées ou non auprès de la personne concernée) ainsi que pour procéder à toute communication au titre des articles 15 à 22 (concernant les droits de la personne concernée) et de l'article 34 (en cas de violation) en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples.
23. Le Comité juge acceptable que l'exception à l'obligation d'information prévue à l'article 14, § 5, c), du RGPD soit invoquée étant donné que l'obtention ou la fourniture de données est expressément prescrite dans le droit de l'Union ou le droit d'un État membre, plus précisément dans la réglementation mentionnée au point 21.

B.5. MINIMISATION DES DONNÉES

24. Conformément à l'article 5, § 1^{er}, c), 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. Ce principe se reflète au niveau des catégories des données, de la durée et de la périodicité de la communication et des catégories de destinataires.
25. Le demandeur déclare que les données à caractère personnel demandées doivent permettre aux services d'inspection d'identifier uniquement le conducteur et le véhicule.
26. En ce qui concerne la lutte contre les faux indépendants, les inspecteurs et les contrôleurs sociaux peuvent par exemple décider que l'intéressé ne se présente pas en tant qu'entreprise à l'égard des tiers lorsqu'il n'est fait aucun usage d'un lettrage, de logos ou d'un autre élément sur les véhicules. Par conséquent, l'utilisation de véhicules dont il est propriétaire ou locataire, peut être prise en compte dans l'évaluation de la relation de travail. Les inspecteurs et les contrôleurs sociaux doivent dès lors pouvoir établir un lien entre le véhicule et le titulaire de l'immatriculation. Pour les personnes qui effectuent un transport de marchandises pour le compte d'une entreprise ou pour les personnes qui effectuent le transport de personnes qui leur est confié par une entreprise, avec des véhicules dont ils ne sont pas propriétaires, ou dont l'achat est financé ou le financement garanti, s'applique une supposition irréfutable que leurs prestations de travail sont effectuées en tant que travailleur.
27. Le demandeur déclare que les données visées sont par ailleurs nécessaires pour assurer une organisation efficace des contrôles. À l'aide des plaques d'immatriculation, les inspecteurs

⁸ Les articles 23 à 24 du Code pénal social décrivent les compétences des inspecteurs sociaux. Ils peuvent notamment collecter tous les renseignements qu'ils estiment nécessaires pour vérifier si la législation sur laquelle ils exercent une surveillance est respectée. L'article 55 du Code pénal social précise expressément que les autorités sont tenues de fournir aux inspecteurs sociaux, à leur demande, toutes les informations qu'elles jugent utiles. Le livre II du Code pénal social fixe des infractions pénales aux diverses réglementations que les inspecteurs sociaux surveillent. Les traitements des données DIV demandées découlant de la collaboration intensive entre les différents services d'inspection ont une base juridique dans l'article 54 du Code pénal social.

et contrôleurs sociaux peuvent mieux répertorier les entreprises, les travailleurs indépendants et les travailleurs, et procéder plus rapidement à une identification avant d'effectuer un contrôle. L'exécution efficace des contrôles peut à son tour donner de meilleurs résultats dans la lutte contre la fraude sociale. Les données visées sont par ailleurs nécessaires pour rechercher et sanctionner les abus par les travailleurs indépendants en incapacité de travail et le travail non déclaré comme la présence (préalable) de véhicules sur les chantiers peut servir d'indication et d'aide dans l'identification des fraudeurs. Les données contribuent également à l'appréciation de la solvabilité des travailleurs indépendants et des entreprises. Enfin, les données visées sont nécessaires à la lutte contre le dumping social. De cette manière, les inspecteurs et contrôleurs sociaux peuvent contrôler plus rapidement et plus efficacement si les règles de détachement des travailleurs indépendants ont été respectées. Préalablement aux contrôles sur le terrain, le conducteur et le véhicule peuvent ainsi être établis et identifiés.

28. Le Comité constate également qu'il existe une légère disparité entre les données issues du répertoire de la DIV par rapport à celles pour lesquelles le Comité sectoriel de l'autorité fédérale a accordé une autorisation uniformisée à l'égard des quatre services d'inspection (délimitation FO n° 19/2017 du 29 juin 2017) et les données qui sont énumérées dans la présente demande de l'INASTI.
29. En concertation avec le demandeur, l'accès aux données de la DIV est donc aussi limité aux données mentionnées dans la délibération FO n° 19/2017 du 29 juin 2017 : plaque d'immatriculation ; prénom, nom de famille, date de naissance, adresse, numéro de registre national et numéro d'entreprise du titulaire du véhicule ; dénomination officielle de l'entreprise ; marque du véhicule ; numéro de châssis, modèle, catégorie, type de carburant, émissions de CO₂, masse de chargement maximale autorisée, masse maximale autorisée, date d'immatriculation, date de radiation, statut de l'immatriculation, nombre de places assises du véhicule.
30. En ce qui concerne l'utilisation du numéro de registre national, le Comité constate qu'il permet une identification univoque de l'intéressé. Sur la base de la loi susmentionnée du 15 août 2012 *relative à la création et à l'organisation d'un intégrateur de services fédéral*, les services publics sont tenus d'utiliser un numéro de registre national lors de l'échange de données, pour autant qu'ils obtiennent une délibération.
31. Compte tenu de ce qui précède, le Comité estime que l'utilisation du numéro de registre national est justifiée et correspond donc à l'article 5, 1., c), du RGPD.

En ce qui concerne la périodicité de la communication et la durée de l'autorisation

32. Comme les contrôles peuvent être exécutés à n'importe quel moment, le demandeur demande un accès permanent aux données et, vu la mission légale, pour une durée indéterminée. Le Comité juge cette modalité acceptable.

En ce qui concerne le délai de conservation

33. En ce qui concerne le délai de conservation, le Comité indique que le mode de conservation des données doit être adapté en fonction du besoin évoluant dans le temps. Les données doivent ainsi être conservées dans le cas d'une recherche en cours et active de manière à ce qu'elles soient disponibles et accessibles aux inspecteurs chargés du dossier. Dès que le délai nécessaire à la gestion administrative du dossier est expiré, les données conservées ne doivent plus être disponibles et accessibles que de manière limitée. Une fois que la conservation n'est

plus nécessaire pour réaliser les finalités poursuivies (en ce compris les délais d'appel, la prescription et l'archivage administratif éventuel), les données doivent être détruites.

B.7. INTÉGRITÉ ET CONFIDENTIALITÉ

34. Conformément à l'article 5, § 1^{er}, f), du RGPD, les données à caractère personnel doivent être 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.
35. L'INASTI confirme satisfaire à l'arrêté royal du 12 août 1993 *relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale*. L'INASTI est une institution publique de sécurité sociale qui appartient au réseau primaire de la sécurité sociale. Conformément à l'article 24 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, il a désigné un fonctionnaire à la protection des données, dont l'identité a été communiquée à la Banque-carrefour de la sécurité sociale.
36. L'INASTI confirme que sa politique en matière de sécurité de l'information est conforme aux normes de sécurité minimales de la Banque-carrefour de la sécurité sociale. Le système de gestion ou Information Security Management System est basé sur la norme internationale ISO 27001 pour la sécurité de l'information.
37. Les autorisations qui donnent accès aux informations de la Banque-carrefour sont accordées par les fonctionnaires dirigeants des services internes. Le contrôle et la gestion de ces autorisations sont assurés par le fonctionnaire à la protection des données. Toute consultation des données via la BCSS par les membres du personnel de l'INASTI est enregistrée dans un fichier-journal. Les membres du personnel ont signé un code de conduite et une déclaration de confidentialité. L'INASTI dispose d'une liste actuelle des différentes personnes compétentes qui ont accès ou obtiennent la communication des données visées.
38. Le Comité renvoie enfin à l'évaluation positive de la politique en matière de sécurité de l'information de l'INASTI par le Comité sectoriel de la sécurité sociale et de la santé dans le cadre de la délibération n° 13/020 du 5 mars 2013, modifiée le 7 juin 2016 et le 3 juillet 2018.

Analyse d'impact relative à la protection des données

39. Le Comité souligne que dans certains cas, l'article 35 du RGPD requiert que le responsable du traitement réalise, avant le traitement, une évaluation de l'impact des activités de traitement visées sur le traitement de données à caractère personnel. Le Comité souligne que, conformément à l'article 23 de la loi du 30 juillet 2018 concernant la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, chaque entité fédérale doit exécuter une analyse d'impact relative à la protection des données.

Par ces motifs,

le Comité de sécurité de l'information, chambres réunies, décide :

La communication des données à caractère personnel telle que visée dans la présente délibération est autorisée pour autant qu'il soit satisfait aux mesures fixées dans la présente délibération visant à garantir la protection des données, en particulier les mesures en matière de limitation des finalités, de minimisation des données, de limitation de la conservation et de sécurité de l'information.

La communication autorisée concerne la communication par la Direction générale Mobilité et Sécurité routière du Service public fédéral Mobilité et Transports aux services d'inspection de l'INASTI des données suivantes : plaque d'immatriculation ; prénom, nom de famille, date de naissance, adresse, numéro de registre national et numéro d'entreprise du titulaire du véhicule ; dénomination officielle de l'entreprise ; marque du véhicule ; numéro de châssis, modèle, catégorie, type de carburant, émissions de CO₂, masse de chargement maximale autorisée, masse maximale autorisée, date d'immatriculation, date de radiation, statut de l'immatriculation, nombre de places assises du véhicule.

Le demandeur et la Direction générale Mobilité et Sécurité routière du Service public fédéral Mobilité et Transports sont tenus, le cas échéant, de communiquer au Comité le résultat de l'analyse d'impact relative à la protection des données. Si cette analyse révèle que des mesures supplémentaires doivent être prises, les parties doivent soumettre ensemble et de leur propre initiative une demande de modification de la présente délibération. La communication de données à caractère personnel ne peut, le cas échéant, se faire tant que l'autorisation requise du Comité n'a pas été obtenue.

Mireille Salmon
Présidente Chambre Autorité fédérale

Michel Deneyer
Chambre Sécurité sociale et Santé

<p>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). Le siège de la chambre sécurité sociale du Comité de sécurité de l'information est établi dans les bureaux de la BCSS – Quai de Willebroeck 38 – 1000 Bruxelles (tél. 32-2-747 84 27).</p>
--