Service public fédéral
Mobilité et Transports
Transport routier et Sécurité routière

CONVENTION DE COMMUNICATION DE DONNÉES
entre
le Service Général du Renseignement et de la Sécurité (SGRS)
et
la Banque Carrefour des Véhicules (BCV)

1. CADRE ET OBJET DE LA CONVENTION

La présente convention fixe les règles de la communication de données extraites du fichier de la DIV au SGRS à l'appui de l'autorisation n° 12/2015 du Comité Sectoriel pour l'Autorité Fédérale (CSAF) institué au sein de la Commission de la Protection de la Vie Privée (CPVP) et portant sur la surveillance des flux électroniques des données.

2. LES RESPONSABLES DU TRAITEMENT

Au sens de la loi du 8 décembre 1992 relative à la protection de la vie 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) Le Service Général du Renseignement et de la Sécurité (SGRS), faisant partie du Ministère de la Défense, (n° d'entreprise 0308357555), dont le siège est situé, rue d'Evere 1 à 1140 Bruxelles (EVERE) et représenté par Lieutenant-général Eddy TESTELMANS, Chef du Service Général du Renseignement et de la Sécurité.
SGRS agit comme responsable du traitement en tant, notamment, qu'administration publique qui reçoit des données de la DIV et qui les traite au sens des termes de la présente convention.

DIV et SGRS 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 1er, § 4 de la loi du 8 décembre 1992 relative à la protection de la vie privée).

3. FOURNISSEUR ET DESTINATAIRE DES DONNÉES

Le fournisseur des données est la DIV, mieux identifiée au point 2.a ci-avant et le destinataire des données est SGRS, mieux identifié au point 2.b ci-avant et désigné ci-après en cette qualité de « destinataire ».

4. OBJECTIF(S) AVALISÉ(S) PAR LE COMITÉ SECTORIEL POUR L'AUTORITÉ FÉDÉRALE (CSAF)

Sous réserve des conditions éventuelles mentionnées dans l'autorisation du CSAF, les objectifs du destinataire permis par le CSAF pour l'utilisation des données de la DIV sont les suivants :
L'exécution des missions du SGRS reprises dans l' article 11 de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Tout autre objectif n'ayant pas reçu l'agrément formel du Comité Sectoriel pour l'Autorité Fédérale ne pourra être légitimement utilisé.

5. DONNÉES COMMUNIQUÉES ET MODALITÉS D'EXÉCUTION

Voir, en annexe, l'autorisation FO n°12/2015, datée du 23 avril 2015, provenant du CSAF institué au sein de la CPVP. Les données sont communiquées via un Web Services.

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 de la loi du 8 décembre 1992 relative à la protection de la vie privée.

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. BASES NORMATIVES

a) Pour la DIV :
- Loi du 16 mars 1968 relative à la Police de la Circulation routière.
- 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.

c) Pour le destinataire :
- La loi organique des services du renseignement et de sécurité du 30 novembre 1998
- Arrêté royal du 8 juillet 1999 autorisant l'accès du Service Général du Renseignement et de Sécurité des Forces armées au Registre National des personnes physiques.
- Arrêté royal du 27 octobre 2000 autorisant l'accès du Service Général du Renseignement et de Sécurité des Forces armées à utiliser le numéro d'identification du Registre National des personnes physiques

8. 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.

b) Une demande qui fixe le cadre et l'objet d'un traitement de données à caractère personnel doit être préalablement adressée au Comité Sectoriel pour l'Autorité Fédérale (CSAF). Celui-ci, avant d'octroyer son autorisation, vérifie si la communication de données envisagée est conforme aux dispositions légales et réglementaires. A cette condition seulement, la DIV pourra conclure une convention avec le demandeur visant à la communication de données. L'autorisation du Comité Sectoriel pour l'Autorité Fédérale ainsi que ses conditions éventuelles feront partie intégrante de la convention projetée sous forme d'une annexe écrite.

La DIV se réserve le droit de requérir confirmation de cette autorisation directement auprès dudit comité sectoriel avant toute mise en œuvre de la convention sollicitée.

Cette disposition constitue une condition sine qua non à la conclusion d'une convention de communication de données à caractère personnel entre le fournisseur qu'est la DIV et un destinataire potentiel.

9. 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.

10. POINTS DE CONTACT

a) Pour le destinataire : ci-ccirm@qet.be
b) Pour la DIV : help.div@mobilit.fgov.be
c) Pour ICT: parking.div@mobilit.fgov.be

11. UTILISATION ET SÉCURISATION DES DONNÉES

a) Le destinataire a l'obligation de prendre toutes précautions nécessaires afin de garantir la sécurité des données reçues et en est responsable en application des dispositions de la présente convention. Le destinataire a le choix de s'adjoindre un conseiller en sécurité de l'information, responsable de l'exécution de la politique de sécurité du destinataire, soit en son sein, soit auprès d'un tiers spécialisé nommément désigné vu que cette personne sera normalement le premier contact en cas de problèmes. Ce conseiller en sécurité peut aussi être choisi au niveau sectoriel pour plusieurs destinataires.

b) Par la signature de la présente convention, le destinataire s'est assuré que les réseaux auxquels sont connectés les équipements impliqués dans le traitement des données à caractère personnel garantissent la confidentialité et l'intégrité de celles-ci.

c) Toute autre utilisation des données reçues que celle(s) prévue(s) à la présente convention est strictement interdite et conduit à l'annulation pure et simple de la présente convention en application du point 13 de celle-ci (clause de nullité – sanction).

d) 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 se réserve le droit de mener des audits et des enquêtes par sondages, au besoin auprès des personnes concernées par le traitement de leurs données à caractère personnel mais aussi auprès du destinataire,
afin de contrôler si ce dernier respecte ses engagements vis-à-vis de la présente convention, toute en respectant la discrétion nécessaire à l'exécutions des missions du SGRS.

e) Le destinataire des données, en cette qualité, s'engage à accorder à tout moment, un droit de regard à la DIV, à la CPVP et au CSAF ainsi qu'à leurs représentants désignés sur tous les documents considérés comme pertinents pour ces services, et à répondre à toutes leurs questions dans le respect de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. Le cas échéant, ces personnes peuvent effectuer une visite ou une consultation sur place, annoncée à l'avance ou non, afin de contrôler le respect des conditions stipulées dans la présente convention dans le chef du destinataire ou de son sous-traitant éventuel.

f) La DIV et le destinataire, en tant que responsables du traitement, et leurs sous-traitants éventuels, prennent les mesures techniques et organisationnelles nécessaires pour protéger les données à caractère personnel contre la destruction accidentelle ou non-autorisée, contre la perte accidentelle ainsi que la modification, l'accès et tout autre traitement non-autorisé de données à caractère personnel.
Le niveau de protection doit être proportionné à l'état de la technique en la matière, aux frais qu'il engendre, à la nature des données et aux risques potentiels.

g) Le destinataire ou son sous-traitant éventuel ont l'obligation d'établir un plan de sécurité et de répertorier toute question ou réclamation reçue relative à la sécurité des données à caractère personnel ; de même, tout incident éventuel doit être répertorié.
En cas d'incidents sérieux ou répétitifs quant à la sécurité des données à caractère personnel (violation) dans le chef du destinataire ou de son sous-traitant éventuel, ceux-ci doivent être communiqués au fournisseur (la DIV). Ce dernier estime s'il y a lieu d'avertir les autorités judiciaires compétentes, en tenant compte des dispositions pénales prévues aux articles 37 à 43 de la loi du

8 décembre 1992 relative à la protection de la vie privée. La notification faite aux autorités judiciaires par le fournisseur de données décrira les conséquences de la violation et les mesures proposées ou prises pour y remédier.

12. 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 13 de la présente convention (clause de nullité – sanction).

13. CLAUSE DE NULLITÉ - SANCTION

Si les dispositions de la loi du 8 décembre 1992 relative à la protection de la vie privée ou si les dispositions de la présente convention ne sont manifestement pas respectées, la DIV, en tant que fournisseur, se réserve le droit d'interrompre, sur le champ et suite aux contrôles qu'elle aura effectués conformément aux points 11.d et 11.e de cette convention, la communication de données au destinataire et lui en notifie les raisons par courrier postal recommandé ou par courrier électronique avec accusé de réception.

De par cette notification, la convention conclue entre le destinataire et la DIV devient nulle et non avenue.

Tous les différends qui trouvent leur origine dans la présente convention et qui ne peuvent être résolus aux termes de celle-ci sont du ressort des tribunaux de Bruxelles.

14. 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 :

- L'autorisation du Comité Sectoriel pour l'Autorité Fédérale au sujet de la présente convention.

15. PROTECTION DE LA VIE PRIVÉE

Le traitement des données ainsi recueillies s'effectuera conformément à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et à ses arrêtés d'application, modifiée par la loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Le destinataire s'engage à n'utiliser les données reçues de la DIV que pour la(les) finalité(s) et à la(aux) condition(s) décrite(s) dans l'autorisation du CSAF.

16.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.

c) 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 ».

17. 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 différends sur l'interprétation de cette convention, avantage sera toujours accordé à la résolution du CSAF.

Fait à Bruxelles, le 10/2/17 en deux exemplaires, chaque partie reconnaissant avoir reçu un exemplaire.

Pour le SGRS,

Eddy TESTELMANS
Lieutenant-général
Chef du Service Général du
Renseignement et de la Sécurité

Pour la DIV,

Martine INDOT
Directeur général du Transport routier et
Sécurité routière

Comité sectoriel pour l'Autorité Fédérale

Délibération AF n° 12/2015 du 23 avril 2015

Objet: demande d'autorisation du Service général du Renseignement et de la Sécurité (SGR) afin de recevoir de manière électronique des données à caractère personnel de la Direction pour l'Immatriculation des Véhicules ("DIV") dans le cadre des missions définies à l'article 11 de la loi du 30 novembre 1998 (AF-MA-2015-023)

Le Comité sectoriel pour l'Autorité Fédérale (ci-après "le Comité") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après LVP), en particulier les articles 31*bis* et 36*bis* ;

Vu l'arrêté royal du 17 décembre 2003 *fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la Commission de la protection de la vie privée*, en particulier l'article 18 ;

Vu la demande du Service général du Renseignement et de la Sécurité (ci-après le demandeur), reçue le 19/02/2015 ;

Vu les informations complémentaires reçues le 11/03/2015 ;

Vu la demande d'avis technique et juridique adressée au Service public fédéral Fedict en date du 11/03/2015 ;

Vu le rapport du Président ;

Émet, après délibération, la décision suivante, le 23 avril 2015 ;

I. OBJET DE LA DEMANDE

1. Le demandeur (le SGR) sollicite l'autorisation du Comité de recevoir électroniquement des données à caractère personnel de la DIV afin de faciliter et de garantir l'identification des cibles dans le cadre de ses missions définies par l'article 11 de la loi du 30 novembre 1998[1].

2. L'article 11, § 1er de la loi susmentionnée énumère les missions du demandeur comme suit :
"*1° de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer l'intégrité du territoire national, les plans de défense militaires, le potentiel scientifique et économique en rapport avec les acteurs, tant personnes physiques que personnes morales, qui sont actifs dans les secteurs économiques et industriels liés à la défense et qui figurent sur une liste approuvée par le Comité ministériel du renseignement et de la sécurité, sur proposition du Ministre de la Justice et du Ministre de la Défense, l'accomplissement des missions des Forces armées ou la sécurité des ressortissants belges à l'étranger ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Comité ministériel, et d'en informer sans délai les ministres compétents ainsi que de donner des avis au Gouvernement, à la demande de celui-ci, concernant la définition de sa politique extérieure de défense ;*

2° de veiller au maintien de la sécurité militaire du personnel relevant du Ministre de la Défense nationale, et des installations militaires, armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires et, dans le cadre des cyberattaques de systèmes informatiques et de communications militaires ou de ceux que le Ministre de la Défense nationale gère, de neutraliser l'attaque et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit des conflits armés ;

3° de protéger le secret qui, en vertu des engagements internationaux de la Belgique ou afin d'assurer l'intégrité du territoire national et l'accomplissement des missions des Forces armées, s'attache aux installations militaires, armes, munitions, équipements, aux plans, écrits, documents ou autres objets militaires, aux renseignements et communications militaires, ainsi qu'aux systèmes informatiques et de communications militaires ou ceux que le Ministre de la Défense nationale gère ;

4° d'effectuer les enquêtes de sécurité qui lui sont confiées conformément aux directives du Comité ministériel."

---

[1] *Loi organique des services de renseignement et de sécurité* du 30 novembre 1998, M.B. du 18 décembre 1998.

3. En tant que service de renseignement et de sécurité, le demandeur peut, en vertu de l'article 13 de la loi du 30 novembre 1998 "*(...) rechercher, collecter, recevoir et traiter des informations et des données à caractère personnel qui peuvent être utiles à l'exécution de ses missions et tenir à jour une documentation relative notamment à des événements, à des groupements et à des personnes présentant un intérêt pour l'exécution de ses missions. (...)*".

II. EXAMEN DE LA DEMANDE

A. COMPÉTENCE DU COMITÉ

4. En vertu de l'article 36*bis* de la LVP, "*toute communication électronique de données personnelles par un service public fédéral ou par un organisme public avec personnalité juridique qui relève de l'autorité fédérale, exige une autorisation de principe* du comité sectoriel (compétent)".

5. Il incombe au Comité de vérifier "*que ladite communication, d'une part, est nécessaire à la mise en œuvre des missions confiées, par ou en vertu de la loi, à l'autorité fédérale demanderesse et, d'autre part, que cette communication, en ses divers aspects, est compatible avec l'ensemble des normes en vigueur en matière de protection de la vie privée en ce qui concerne le traitement de données personnelles*" (Doc. Parl. 50, 2001-2002, n° 1940/004).

6. En vertu de l'article 18 de la loi du 19 mai 2010 *portant création de la Banque-Carrefour des véhicules* (ci-après, "loi BCV"), "*l'accès aux autres données de la Banque-Carrefour nécessite une autorisation préalable du comité sectoriel. Avant de donner son autorisation, le comité sectoriel vérifie si cet accès est conforme à la présente loi, à ses arrêtés d'exécution et à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.*
Cette autorisation est accordée par le comité sectoriel :
1° aux autorités publiques belges pour les informations qu'elles sont habilitées à connaître par ou en vertu d'une loi, d'un décret ou d'une ordonnance ;
(...)".

7. La DIV, qui fait partie du Service public fédéral Mobilité et Transport, transmettra des données à caractère personnel par voie électronique au demandeur. Le Comité est par conséquent compétent.

B. QUANT AU FOND

1. PRINCIPE DE FINALITÉ

8. L'article 4, § 1, 2° de la LVP n'autorise le traitement de données à caractère personnel que pour des finalités déterminées, explicites et légitimes et les données ne peuvent en outre pas être traitées ultérieurement de manière incompatible avec ces finalités.

9. Le demandeur explique que les données collectées sont destinées à identifier des cibles faisant l'objet d'enquêtes, conformément aux articles 11 et 13 de la loi du 30 novembre 1998. Les missions d'identification du demandeur doivent être exécutées lors de missions de surveillance, à l'occasion de contrôles de la sécurité militaire et pendant les enquêtes pour l'octroi d'habilitations de sécurité.

10. Le Comité constate que :
    - en ce qui concerne les finalités pour lesquelles la DIV collecte et traite des données à caractère personnel, la loi BCV prévoit que "*La Banque-Carrefour a pour objectif, d'une part, d'assurer la traçabilité des véhicules (...) et, d'autre part, d'identifier à tout moment leur propriétaire, le demandeur et le titulaire de leur immatriculation, ainsi que de retrouver les données concernant leur homologation afin de : (...) 7° faciliter la recherche, la poursuite pénale et l'application des peines des infractions. (...)*"

11. Au regard de ce qui précède, le Comité constate que les finalités poursuivies par le demandeur sont déterminées, explicites et légitimes et rappelle que les données demandées ne peuvent être traitées qu'en vue de réaliser ces finalités.

12. Les traitements de données envisagés sont également admissibles vu l'article 5, c) de la LVP. Le Comité constate en effet que les traitements se basent sur les dispositions légales susmentionnées.

2. PRINCIPE DE PROPORTIONNALITÉ

2.1. *Nature des données*

13. L'article 4, § 1, 3° de la LVP prévoit que les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement.

14. Le demandeur souhaite recevoir les données suivantes du répertoire matricule des véhicules tenu par la DIV :
    - les nom, prénom, date de naissance, numéro de Registre national de la personne au nom de laquelle le véhicule est immatriculé ;
    - l'adresse de la résidence temporaire des personnes visées à l'article 5, § 1er, 1° et 2° de l'arrêté royal du 20 juillet 2001[2] ;
    - le nom, la forme juridique et le numéro de TVA de la personne morale au nom de laquelle le véhicule est immatriculé ;
    - le numéro d'immatriculation (plaque minéralogique) du véhicule ;
    - la date de la première immatriculation du véhicule (en Belgique ou à l'étranger) ;
    - la marque ou, si la marque n'est pas connue, le constructeur du véhicule ;
    - le type, si d'application, la variante et la version du type de véhicule ;
    - la dénomination commerciale du véhicule ;
    - le numéro d'identification (numéro de châssis) du véhicule ;
    - la date de la dernière immatriculation du véhicule ;
    - la cylindrée (en cm^3) du véhicule ;
    - le type de carburant ou le type de source d'énergie du véhicule ;
    - les nom, adresse et, si d'application, numéro de code de la compagnie d'assurance qui couvre les risques de la responsabilité civile du propriétaire ou de l'utilisateur du véhicule ;
    - la couleur de la carrosserie.

---

[2] Arrêté royal du 20 juillet 2001 *relatif à l'immatriculation de véhicules*, M.B. du 8 août 2001.

"*Art. 5. § 1er. Pour les personnes mentionnées ci-après, qui veulent mettre en circulation un véhicule, une immatriculation est requise également, étant toutefois temporaire. Elle peut être soit une immatriculation transit lorsque les personnes mentionnées ci-après ont obtenu l'exemption des droits d'importation et de TVA ou de TVA seulement, soit une immatriculation provisoire dans les autres cas :*

1° les personnes, membres du corps diplomatique ou consulaire en Belgique ou qui y bénéficient des immunités similaires à celles du corps diplomatique, dont le véhicule ne porte pas une marque d'immatriculation comme visée à l'article 20, § 1er, 1° ou 6°, ainsi que les personnes qui sont membres du personnel administratif et technique des missions diplomatiques en Belgique ou qui y résident comme employés consulaires de carrière et les membres du personnel d'une organisation internationale de droit public ayant un siège fixe en Belgique en application d'un accord conclu entre l'organisation concernée et le gouvernement belge ;

2° les organes et les fonctionnaires de l'Union européenne et de l'Organisation pour la sécurité de la navigation aérienne établis en Belgique et désignés par les organisations concernées. (...)"

15. Les données susmentionnées sont nécessaires pour le demandeur à la lumière de la menace possible à l'encontre de l'intégrité du territoire national, des plans de défense militaire, du potentiel économique et scientifique, des missions de l'armée, de la sécurité des ressortissants belges à l'étranger et de la protection du secret.

16. Le demandeur est déjà autorisé à accéder au Registre national (arrêté royal du 8 juillet 1999[3]) et à utiliser le numéro de Registre national (arrêté royal du 27 octobre 2000[4]).

17. En vertu de l'article 5, § 1er de la loi du 5 mai 2014 *garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité et portant simplification et harmonisation des formulaires électroniques et papier*, le Comité est habilité à autoriser l'utilisation du numéro de Registre national. Cet article prévoit en effet que "*Les contrôleurs autorisent l'utilisation du numéro du Registre national chaque fois qu'une décision est prise à propos d'un flux de données personnelles ou d'un traitement de telles données. Cette décision vaut autorisation en exécution de l'article 8 de la loi du 8 août 1983 organisant un registre national des personnes physiques. (...)*"[5].

18. Étant donné que le demandeur dispose déjà d'une autorisation d'accéder aux informations du Registre national et d'utiliser le numéro d'identification de ce Registre, le Comité, lors de son examen, n'a plus qu'à vérifier si l'utilisation du numéro de Registre national est proportionnelle au regard des nouvelles finalités poursuivies par le demandeur (article 4, § 1, 3° de la LVP).

19. Le demandeur souhaite se servir du numéro de Registre national comme identifiant de cibles (voir ci-avant au point 9). Le Comité constate qu'en combinaison avec le nom, le

---

[3] Arrêté royal du 8 juillet 1999 *autorisant l'accès du Service général du Renseignement et de Sécurité des Forces armées au Registre national des personnes physiques.*

[4] Arrêté royal du 27 octobre 2000 *autorisant le service général du Renseignement et de la Sécurité des forces armées à utiliser le numéro d'identification du Registre national des personnes physiques.*

[5] L'article 3, 6° de la loi du 5 mai 2014 définit la notion de "contrôleur" comme étant "*l'autorité de droit public visée à l'article 28 de la Directive 95/46/CE du 24 octobre 1995 relative 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 à l'article 8.3 de la Charte des droits fondamentaux de l'Union européenne du 12 décembre 2007, constituée actuellement par la Commission de la protection de la vie privée, instituée par l'article 23 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, ainsi que par les comités sectoriels institués par l'article 31bis de la même loi du 8 décembre 1992, la Commission de Contrôle flamande pour l'échange électronique de données administratives, instituée par l'article 10 du décret du Parlement flamand du 18 juillet 2008 relatif à l'échange électronique de données administratives, la Commission Wallonie-Bruxelles pour le contrôle sur l'échange de données, instituée par l'article 22 de l'Accord de Coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative, et toute autre instance similaire instaurée par loi, décret ou ordonnance.*"

prénom et l'adresse, ce numéro, qui est un numéro unique, permet d'identifier une personne sans la moindre marge d'erreur, évitant ainsi tout à fait la confusion ou les erreurs auxquelles peuvent donner lieu les homonymes ou des fautes d'orthographe dans le nom. Au vu des finalités poursuivies et des conséquences que cela peut engendrer pour la personne concernée, il importe de ne pas commettre la moindre erreur quant à l'identité de celle-ci.

20. À la lumière des finalités définies ci-avant, le Comité conclut que les données que le demandeur souhaite recevoir sont conformes à l'article 4, § 1, 3° de la LVP.

21. De plus, le Comité attire l'attention sur le fait que les données recueillies doivent être considérées comme étant des données judiciaires, telles que définies dans la LVP, si elles sont collectées ou traitées afin d'être utilisées pour porter une affaire devant le tribunal.

22. Il est dès lors rappelé que les bénéficiaires de la présente délibération doivent respecter les conditions particulières relatives à ce type de traitements. Ces conditions sont définies à l'article 25 de l'arrêté royal du 13 février 2001 portant exécution de la LVP. En vertu de cet article, le responsable doit désigner clairement les catégories de personnes ayant accès aux données et leur fonction doit être décrite précisément. La liste des catégories de personnes doit être tenue à la disposition de la Commission de la protection de la vie privée (ci-après la Commission). Le responsable doit en outre veiller à ce que ces personnes désignées soient tenues, par une obligation légale, statutaire ou contractuelle, au respect du caractère confidentiel des données.

2.2. Délai de conservation des données

23. Concernant le délai de conservation des données, le Comité rappelle que les données ne peuvent pas être conservées pendant une durée excédant celle nécessaire à la réalisation de la finalité pour laquelle elles ont été collectées (article 4, § 1, 5° de la LVP).

24. L'article 21 de la loi du 30 novembre 1998 prévoit que "*Les données à caractère personnel traitées dans le cadre de l'application de la présente loi sont conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées, à l'exception de celles présentant un caractère historique, reconnu par les archives de l'État.*"

25. Selon le demandeur, un avant-projet d'arrêté royal portant exécution de l'article 21 de la loi du 30 novembre 1998 prévoit un délai de conservation de 50 ans avec possibilité de prolongation.

26. D'après le demandeur, il sera tenu compte, dans ce cadre, des remarques émises par la Commission dans son avis n° 07/2013 du 20 février 2013[6] concernant cet avant-projet d'arrêté royal. Le Comité en prend acte. Le Comité rappelle à cet égard la remarque et la condition selon lesquelles le délai de 50 ans est un délai de conservation maximal[7].

27. Le Comité constate qu'*in abstracto*, le délai de conservation ne peut en fait pas être défini précisément. Il estime toutefois que dans la pratique, il convient de faire une distinction entre différents modes de conservation dans le temps. Lors de l'exécution d'un contrôle ou d'une mission, les données doivent être disponibles et accessibles normalement aux personnes concernées chargées de l'exécution du contrôle ou de la mission à proprement parler. Dès que ces tâches sont achevées et que les missions effectuées sont archivées électroniquement, il faut opter pour un mode de conservation ne conférant aux données qu'une disponibilité et une accessibilité limitées. Un tel mode de conservation doit permettre de répondre à d'autres finalités éventuelles de cette conservation, comme le respect des dispositions légales en matière de prescription ou l'exécution d'un contrôle administratif (par ex. un contrôle indirect par la Commission en exécution de l'article 13 de la LVP). Dès que la conservation n'est plus utile, les données ne peuvent plus être conservées.

28. Le Comité conclut que les données en question peuvent être traitées en vue de différents contrôles et enquêtes (voir ci-avant au point 9). La mise en œuvre concrète des directives générales exposées dans les alinéas précédents en matière de délais de conservation peut dès lors être différente dans ces cas.

2.3. Fréquence de l'accès et durée de l'autorisation

29. Le demandeur sollicite un accès permanent aux données demandées.

30. Étant donné que le demandeur doit pouvoir identifier les véhicules et leurs propriétaires tous les jours, le Comité considère qu'une transmission électronique permanente est justifiée à la lumière de l'article 4, § 1, 3° de la LVP.

31. Le demandeur sollicite une transmission électronique pour une durée indéterminée. Le Comité constate que la finalité pour laquelle le demandeur souhaite un accès n'est pas

[6] Voir http://www.privacycommission.be/sites/privacycommission/files/documents/avis_07_2013.pdf.

[7] Voir le point 20 de l'avis susmentionné du 20 février 2013.

limitée dans le temps et que, par conséquent, une autorisation pour une durée indéterminée est appropriée (article 4, § 1, 3° de la LVP).

2.4. Destinataires et/ou tiers auxquels les données sont communiquées

32. Le demandeur précise que les données seront traitées en interne par ses agents tels que définis à l'article 3, 2° de la loi du 30 novembre 1998[8]. Le Comité n'a aucune remarque quant au fait que les personnes susmentionnées aient accès aux données pertinentes pour autant que cet accès intervienne dans les conditions suivantes :

- L'accès (des agents) du demandeur intervient uniquement dans les limites des compétences qui leur sont dévolues par la réglementation, en ce compris les conditions rappelées au point 22 ci-dessus ;
- Le demandeur et ses agents sont tenus par une obligation légale, statutaire ou contractuelle au respect de la confidentialité des données ;
- Les mesures nécessaires sont prises afin que seuls les agents susmentionnés aient accès, et ce uniquement lorsqu'un cas concret le justifie.

3. PRINCIPE DE TRANSPARENCE

33. Le Comité rappelle qu'un traitement de données loyal est un traitement qui se fait de manière transparente. L'obligation d'information au sens de l'article 9, § 2 de la LVP constitue une des pierres d'angle d'un traitement transparent.

34. En l'occurrence, les traitements de données envisagés seront toutefois effectués en application de dispositions prescrites par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

35. En vertu de l'article 3, § 4 de la LVP, le demandeur est en outre dispensé de toute application des articles 9, 10 et 12 de la LVP, sans préjudice de la possibilité d'un accès indirect via la Commission (article 13 de la LVP).

36. Compte tenu des éléments susmentionnés, aucune mesure particulière visant à une plus grande transparence n'est réclamée au demandeur.

---

[8] "*tout membre du personnel statutaire ou contractuel et tout militaire exerçant ses fonctions au sein des services de renseignement et de sécurité visés à l'article 2*".

4. SÉCURITÉ

4.1. Au niveau du demandeur

37. Il ressort des documents transmis par le demandeur que ce dernier dispose d'un conseiller en sécurité de l'information, ainsi que d'un plan de sécurité.

38. Le Comité en prend acte.

4.2. Au niveau de la DIV

39. Il ressort des documents dont dispose le Comité que la DIV dispose d'un conseiller en sécurité de l'information, ainsi que d'un plan de sécurité.

PAR CES MOTIFS,

le Comité

autorise le demandeur à recevoir les données électroniques visées dans la demande d'autorisation, aux conditions fixées dans la présente délibération et aussi longtemps que celles-ci seront respectées ;

décide qu'il se réserve le droit, le cas échéant et à intervalles réguliers (si nécessaire via la Commission), de vérifier la mise en œuvre effective et durable des mesures de sécurité techniques et organisationnelles conformes à l'état de la technique et de nature à couvrir adéquatement les risques en présence pendant toute la durée de l'autorisation. À cet égard, le Comité enjoint le demandeur de lui notifier tout changement pertinent dans la sécurisation des traitements autorisés.

Pour l'Administrateur f.f., abs.

Le Président,

(sé) An Machtens
Chef de section OMR f.f.

(sé) Stefan Verschuere