



Autorité de protection des données  
Gegevensbeschermingsautoriteit

**Avis n° 10/2024 du 9 février 2024**

**Objet : Avis concernant un avant-projet d'arrêté royal *modifiant l'arrêté royal du 11 juillet 2003 fixant les conditions d'agrément et le fonctionnement du Bureau belge et du Fonds commun de garantie* (CO-A-2023-526)**

**Mots-clés : moyen d'authentification fort - plaque d'immatriculation - marque d'immatriculation - système en temps réel - consultation en ligne - code QR - certificat international d'assurance numérique et/ou papier - statut d'assurance - consultation du registre visé à l'article 19 *bis*-6 de la loi RC auto - une réponse binaire peut constituer une donnée à caractère personnel - fichiers de journalisation**

**Traduction<sup>1</sup>**

Le Centre de Connaissances de l'Autorité de protection des données (ci-après "l'Autorité"),  
Présent.e.s : Mesdames Juline Deschuyteneer, Cédrine Morlière et Griet Verhenneman et Messieurs  
Yves-Alexandre de Montjoye, Bart Preneel et Gert Vermeulen ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier  
les articles 23 et 26 (ci-après "la LCA") ;

Vu 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* (Règlement général sur la protection des données, ci-après "le RGPD") ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après "la LTD") ;

---

<sup>1</sup> Pour la version originale validée collégialement, cf. la version néerlandaise du texte qui est disponible sur la version NL de la rubrique « avis » du site web de l'Autorité

Vu la demande d'avis de Monsieur Pierre-Yves Dermagne, Vice-Premier ministre et ministre de l'Économie et du Travail (ci-après "le demandeur"), reçue le 13/11/2023 ;

Émet, le 9 février 2024, l'avis suivant :

## **I. OBJET DE LA DEMANDE D'AVIS**

1. Le 13 novembre 2023, le demandeur a sollicité l'avis de l'Autorité concernant un avant-projet d'arrêté royal *modifiant l'arrêté royal du 11 juillet 2003 fixant les conditions d'agrément et le fonctionnement du Bureau belge et du Fonds commun de garantie* (ci-après "l'avant-projet").
2. L'avant-projet s'inscrit dans le cadre d'une tendance générale à la digitalisation et à la simplification administrative, avec la possibilité de dispenser l'assureur en responsabilité pour les véhicules automoteurs de la délivrance de la carte internationale d'assurance automobile (la carte verte), moyennant le respect de certaines conditions.
3. Plus concrètement, l'avant-projet vise l'exécution des articles 19 *bis*-1 à 19 *bis*-3, 19 *bis*-6 et 19 *bis*-8 de la loi du 21 novembre 1989 *relative à l'assurance obligatoire de la responsabilité en matière de véhicules automoteurs* (ci-après "la loi RC auto" ou loi de base), dans le but de créer un registre en temps réel qui fournira les informations relatives au statut d'assurance tel que connu par le Fonds commun de garantie, et ce au moyen d'une réponse binaire ("assuré" ou "inconnu").
4. Dans ce contexte, l'avant-projet spécifie : *i) la forme et le contenu de la demande d'information tels que stipulés à l'article 19bis-8, § 1<sup>er</sup>, alinéa 3 de la loi RC auto ; ii) les modalités relatives à l'accès au registre de l'article 19bis-6, telles que prévues à l'article 19bis-8, § 2, alinéa 2 de la loi RC auto et iii) la forme et le contenu de la demande d'obtention de l'information tels qu'indiqués à l'article 19bis-8, § 3, alinéa 2 de la loi RC auto.*
5. Il est rappelé que dans son avis n° 29/2022 *concernant un projet de loi portant dispositions diverses en matière d'Économie*, l'Autorité s'est déjà prononcée sur les modifications apportées aux dispositions susmentionnées de la loi de base, reprises au point 3. L'Autorité estime dès lors pertinent de renvoyer aux recommandations formulées dans cet avis. L'Autorité note ensuite que de nouvelles dispositions du *projet d'arrêté royal modifiant l'arrêté royal du 13 février 1991 portant mise en vigueur et exécution de la loi du 21 novembre 1989 relative à l'assurance obligatoire de la responsabilité en matière de véhicules automoteurs* (ci-après le "projet") donnent suite aux recommandations de l'avis n° 29/2022 et seront dès lors, s'il y a lieu, concernées par l'évaluation.

## II. RÉSUMÉ SUCCINCT ET OBSERVATIONS

6. La norme soumise pour avis vise à exécuter plusieurs dispositions de la loi RC auto sur lesquelles l'Autorité s'est déjà prononcée, comme cela a été expliqué ci-dessus. L'objectif visant à instaurer un système électronique en plus du système papier actuel, avec une consultation en temps réel de la situation d'assurance d'un véhicule automoteur ou de la détention ou non de données prouvant l'existence du contrat d'assurance, accompagné de la possibilité pour chaque citoyen de consulter le système, a été qualifié dans l'avis antérieur de risque pour les droits et libertés d'une personne concernée. Sur la base de ces éléments, l'Autorité a recommandé d'utiliser pour chaque consultation électronique une authentification forte. Malgré ces recommandations antérieures, la norme exécutive insiste toujours sur l'utilisation d'une systématique déconseillée précédemment. Par conséquent, l'Autorité estime qu'il est nécessaire de souligner à nouveau les dangers liés à ce nouveau système.
7. Concrètement, l'Autorité a déjà indiqué dans son avis antérieur qu'un contrôle était nécessaire par le biais de mesures techniques et organisationnelles car la possibilité, pour chaque citoyen, de consulter le système pouvait faire apparaître des risques pour les droits et libertés des personnes concernées. L'Autorité renvoyait à cet égard à une utilisation détournée d'un système contraire à sa finalité, par exemple, une publication ultérieure de données consultées en vue de nuire.
8. C'est en effet ce système librement accessible qui suscite de l'inquiétude car bien que la loi désigne qui peut le consulter, dans la pratique, il est ouvert à chacun. Un accès illimité, pour lequel aucune donnée des personnes qui ont procédé à une consultation n'est conservée, présente plusieurs dangers. Il suffit de penser à des situations où des entreprises vont potentiellement conserver des listes avec un statut d'assurance et ensuite les vendre ou les utiliser pour n'importe quelle finalité, ou des situations où, en représailles, on va contrôler ou harceler des voisins, des collègues ou d'autres personnes en cas de désaccord, ou encore des situations où il n'y a pas de limite aux consultations. Cocher que la consultation a lieu dans un intérêt légitime ou que les informations communiquées ne seront pas utilisées à des fins qui ne sont pas liées aux motifs invoqués dans la demande est loin de constituer une garantie de protection adéquate. Cela s'applique d'autant plus que le législateur n'entend conserver aucune identification de la personne qui effectue la consultation et que la prise de connaissance requise en devient dès lors insignifiante.
9. C'est dans cette optique que l'avis antérieur recommandait d'utiliser un moyen d'authentification fort. Vu que le législateur ne propose aucun système alternatif, rendant superflu un tel moyen d'authentification fort, le présent avis souligne toujours l'importance de l'utilisation recommandée antérieurement d'un moyen d'authentification fort.

10. L'Autorité comprend que l'instauration d'une méthode d'authentification forte n'est pas évidente dans le contexte technologique actuel. Il est toutefois souligné que le règlement eIDAS (Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 *sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE*) constitue pour les citoyens européens, déjà actuellement mais certainement aussi pour l'avenir, un instrument approprié qui doit être pris en considération. En outre, indépendamment de la recommandation d'utiliser un moyen d'authentification fort, la consultation en temps réel, dans la situation d'habitants de pays tiers, reste une question plus épineuse, avec notamment des frais d'itinérance plus élevés. Par ailleurs, l'Autorité souligne que le système de consultation en temps réel envisagé présente encore d'autres faiblesses. Ainsi, il n'est pas tenu compte de situations dans lesquelles il n'y aurait aucun réseau Internet ou la batterie d'un smartphone serait à plat, ou même de situations dans lesquelles la personne concernée n'aurait pas de smartphone.
11. De plus, une remarque est aussi formulée sur la période qui suit la présomption légale d'un véhicule valablement assuré. L'Autorité constate qu'au terme de cette période, aucune présomption légale ne s'applique en tant que véhicule assuré. Dans un potentiel scénario où la plate-forme est exposée à une défaillance du système, le preneur d'assurance se trouvera encore dans une situation où aucune preuve d'assurance ne peut être délivrée.
12. En bref, c'est précisément ce choix du législateur pour un système qui engendre de tels risques, dans l'avant-projet soumis pour avis, qui incite à insister sur l'utilisation d'un moyen d'authentification fort. En d'autres termes, le choix du législateur pour un autre système pourrait éventuellement conduire à un autre jugement ou avis, dans lequel un moyen d'authentification fort ne serait pas nécessairement requis. À cet égard, l'Autorité fait remarquer que la solution la plus adéquate, tant pour la finalité poursuivie par le législateur que pour la protection des droits et libertés de la personne concernée, qui offrirait en outre aussi une solution aux faiblesses relevées, est l'utilisation d'un code QR en plus du certificat international d'assurance actuel sous format papier.
13. Dans un cadre où la systématique d'un code QR serait instaurée (**ce qui requiert une adaptation du cadre légal**), les assureurs fourniraient à l'assuré un document digital avec un numéro unique d'assurance, tant sous la forme de code QR que sous la forme d'une combinaison de lettres et de chiffres, associé au véhicule de l'assuré. Cela permettrait de vérifier sur place le statut d'assurance en cas d'accident si l'autre partie a accès en ligne. S'il n'y a pas de connexion Internet, le numéro unique d'assurance peut être copié (au moyen d'un appareil photo ou manuellement) et le statut peut être vérifié par la suite en ligne. La différence avec la proposition actuelle est que la vérification n'a pas lieu sur la base d'informations disponibles publiquement

(la marque d'identification - la marque d'immatriculation ou le VIN (numéro d'identification du véhicule ou 'vehicle identification number' : "*code alphanumérique attribué au véhicule par son constructeur, afin d'assurer l'identification adéquate de ce véhicule*)). Cela réduit fortement le risque qu'un voisin ou un collègue réclame le statut d'assurance et cela a pour conséquence qu'une authentification forte n'est plus essentielle. Il faut néanmoins encore toujours ajouter une sécurisation afin d'empêcher qu'une personne puisse réclamer le statut d'assurance pour un grand nombre de numéros uniques d'assurance (aléatoires) (*réclamer l'adresse e-mail, le rate limiting par adresse IP, un captcha*). Compte tenu des progrès technologiques et du cadre réglementaire qui se développe à leur sujet, l'Autorité estime que laisser ouverte la possibilité de s'authentifier sur la base d'eIDAS reste une plus-value, de manière à ce que cela puisse être rendu obligatoire à l'avenir.

14. En outre, il est également recommandé que l'assureur informe toujours l'assuré des risques pratiques, tels qu'évoqués aux points 8 à 11 inclus qui vont de pair avec le passage d'un certificat international d'assurance papier à un système digital.

### **III. EXAMEN QUANT AU FOND**

#### **a. Remarques préalables**

15. Avant de procéder à la discussion de l'avant-projet, l'Autorité souhaite attirer l'attention sur quelques points déjà soulevés dans l'avis n° 29/2022 mais qui n'ont pas été repris dans le présent avis.

16. En la matière, le préambule de l'avant-projet précise ce qui suit :

*"Considérant que même si l'on mettait en place un moyen d'authentification fort, la conservation des données liées à cette consultation serait difficilement justifiable sans porter atteinte à la vie privée de telle sorte que toute trace de connexion devrait être effacée ;*

*Considérant que si l'on ne peut conserver la trace de la consultation avec authentification forte, il n'existe aucune plus-value à la mise en œuvre de mesure d'authentification forte dans le but de minimiser le risque d'une utilisation détournée du système contraire à sa finalité ;"*

17. L'Autorité estime que les affirmations susmentionnées **ne concordent pas avec la recommandation d'utiliser un moyen d'authentification fort, pour chaque accès et**

**consultation** du registre visé à l'article 19*bis*-6 de la loi RC auto<sup>2</sup>. On peut déduire de la prise de position que l'auteur de l'avant-projet estime qu'une authentification forte est disproportionnée par rapport aux informations reçues par le 'demandeur' (destinataire), *N.B.* la 'réponse binaire' reçue sur le statut d'assurance. L'Autorité souligne toutefois que pour pouvoir prévoir une réponse binaire sur le statut d'assurance, un accès au registre est nécessaire. Ainsi, bien que la réponse se limite à 'assuré' ou 'inconnu', des informations sont indirectement transmises sur le registre. En outre, ces informations sont toujours liées à une marque d'immatriculation ou à un numéro de châssis. Par conséquent, la communication d'une réponse binaire sur le statut d'assurance ne peut pas être dissociée d'une donnée à caractère personnel, ce qui a à nouveau été confirmé dans un récent arrêt de la Cour de justice<sup>3</sup>.

18. Compte tenu de ce qui précède, les affirmations suivantes du demandeur dans l'avant-projet sont manifestement infondées :<sup>4</sup>

<sup>2</sup> Il est à noter que la recommandation d'une authentification forte se base sur la justification des points 9 à 12 inclus. L'Autorité souligne qu'en l'état actuel de la technologie et compte tenu de toutes les lacunes, la systématique la plus adéquate est l'utilisation d'un code QR, comme expliqué aux points 12 à 13 inclus, ce qui requiert une adaptation du cadre légal.

<sup>3</sup> CJUE, 9 novembre 2023, n° C-319/22, ECLI:EU:2023:837, paragraphes 44-50 : "*44 Afin de répondre à cette question, il y a lieu d'examiner, dans un premier temps, si le VIN relève de la notion de "donnée à caractère personnel", au sens de l'article 4, point 1, du RGPD, qui définit cette notion comme "toute information se rapportant à une personne physique identifiée ou identifiable".*

*45 Cette définition est applicable lorsque, en raison de leur contenu, de leur finalité et de leur effet, les informations en cause sont liées à une personne physique déterminée [arrêt du 8 décembre 2022, Inspektor v Inspektorata kam Visshia sadeben savet (Finalités du traitement de données à caractère personnel – Enquête pénale), C-180/21, EU:C:2022:967, point 70]. Pour déterminer si une personne physique est identifiable, directement ou indirectement, il convient de prendre en considération l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre soit par le responsable du traitement, au sens de l'article 4, point 7, du RGPD, soit par autrui, pour identifier cette personne, sans pour autant exiger que toutes les informations permettant d'identifier ladite personne se trouvent entre les mains d'une seule entité (voir, en ce sens, arrêt du 19 octobre 2016, Breyer, C-582/14, EU:C:2016:779, points 42 et 43).*

*46 Ainsi que M. l'avocat général l'a relevé aux points 34 et 39 de ses conclusions, une donnée telle que le VIN – qui est défini par l'article 2, point 2, du règlement n° 19/2011 comme un code alphanumérique attribué au véhicule par son constructeur, afin d'assurer l'identification adéquate de ce véhicule et qui, en tant que tel, est dépourvu de caractère "personnel" – acquiert ce caractère à l'égard de quiconque dispose raisonnablement de moyens permettant de l'associer à une personne déterminée.*

*47 Or, il résulte de l'annexe I, point II.5, de la directive 1999/37 que le VIN doit figurer dans le certificat d'immatriculation d'un véhicule, tout comme le nom et l'adresse du titulaire de ce certificat. En outre, en vertu des points II.5 et II.6 de cette annexe, une personne physique peut être désignée dans ledit certificat comme propriétaire du véhicule ou comme une personne pouvant disposer du véhicule à un titre juridique autre que celui de propriétaire.*

*48 Dans ces conditions, le VIN constitue une donnée à caractère personnel, au sens de l'article 4, point 1, du RGPD, de la personne physique mentionnée dans le même certificat, dans la mesure où celui qui y a accès pourrait disposer de moyens lui permettant de l'utiliser pour identifier le propriétaire du véhicule auquel il se rapporte ou la personne pouvant disposer de ce véhicule à un titre juridique autre que celui de propriétaire.*

*49 Ainsi que M. l'avocat général l'a fait observer aux points 34 et 41 de ses conclusions, lorsque les opérateurs indépendants peuvent raisonnablement disposer des moyens leur permettant de rattacher un VIN à une personne physique identifiée ou identifiable, ce qu'il appartient à la juridiction de renvoi de vérifier, ce VIN constitue pour eux une donnée à caractère personnel, au sens de l'article 4, point 1, du RGPD, ainsi que, indirectement, pour les constructeurs automobiles qui le mettent à disposition, même si le VIN n'est pas, en soi, pour ces derniers une donnée à caractère personnel et ne l'est pas, en particulier, lorsque le véhicule auquel ce VIN a été attribué n'appartient pas à une personne physique.*

*50 S'il résulte de la vérification indiquée au point précédent du présent arrêt qu'un VIN doit être considéré comme une donnée à caractère personnel, il relève du champ d'application du RGPD, en vertu de l'article 2, paragraphe 1, de celui-ci, et doit donc faire l'objet d'un traitement conforme à ce règlement."*

<sup>4</sup> Voir également à cet égard l'arrêt Breyer, C-582/14, EU:C:2016:779, points 42 et 43, concernant le caractère identifiable d'une personne.

*"[...] l'utilisation d'un numéro de plaque ou d'un numéro de châssis est un traitement de données à caractère personnel lorsque ce numéro de plaque permet d'identifier une personne physique, ce qui n'est pas le cas lorsque le site génère une réponse concernant le statut d'assurance car il ne transfère pas un élément de données à caractère personnel puisque le propriétaire, le preneur d'assurance, l'assureur ne sont pas identifiables ;"*

*"[...] l'accès à l'information selon laquelle le registre de l'article 19bis-6 de la loi du 21 novembre précitée contient ou non une information quant à la situation d'assurance du véhicule automoteur ne viole donc pas les droits des personnes concernées en tant qu'il ne communique aucune donnée personnelle ;"*

19. En outre, il faut également conserver des données à caractère personnel des destinataires du statut d'assurance, comme expliqué ultérieurement.

20. L'Autorité souhaite ensuite réagir au considérant de l'avant-projet qui précise ce qui suit :

*"Considérant, en outre, qu'un moyen d'authentification fort empêcherait l'accès à l'information à certaines personnes présentant un intérêt légitime à connaître la situation d'assurance comme les personnes de nationalité étrangère ;"*

21. En la matière, l'Autorité fait remarquer qu'au niveau européen, le règlement eIDAS, d'application depuis 2016, facilite une identification électronique<sup>5</sup>. Le demandeur dispose le cas échéant d'un large choix entre les différents niveaux de fiabilité (faible, substantiel et/ou élevé). En outre, il existe plusieurs pratiques techniques<sup>6</sup>, conformément à l'avis n° 98/2022 émis antérieurement, qui sont qualifiées de bonnes pratiques loyales, pensons par exemple à l'utilisation d'un *captcha*, *rate limiting* et à l'application de solutions qui interdisent par exemple le téléchargement massif (*in bulk downloaden*) technique. À la lumière de ces éléments, l'Autorité objecte qu'une nationalité étrangère ne constitue pas un obstacle à l'utilisation d'une méthode d'authentification forte.

22. Tout bien considéré, l'Autorité reste sur sa position selon laquelle une authentification forte est nécessaire, aussi pour les destinataires des informations relatives au statut d'assurance d'un véhicule automoteur. Contrairement au demandeur, l'Autorité estime donc qu'un moyen d'authentification fort est autorisé et proportionnel et cela infirme la supposition selon laquelle un moyen d'authentification fort 'n'est pas possible' ou 'n'a aucune valeur ajoutée'. À la lumière de

---

<sup>5</sup> Article 3(1) du règlement eIDAS : "le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale."

<sup>6</sup> L'Autorité souligne toutefois que la limitation de l'accès aux personnes au sein de l'UE sera extrêmement facile à contourner, par exemple en utilisant un VPN.

ces considérations, **l'Autorité insiste pour que l'avant-projet prévoie une authentification forte pour chaque consultation du registre, y compris pour les destinataires d'une réponse binaire sur le statut d'assurance d'un véhicule automoteur**<sup>7</sup>.

## **b. Base juridique**

### ➤ Principes généraux

23. Chaque traitement de données à caractère personnel doit avoir une base juridique ou de licéité, comme le prévoit l'article 6, paragraphe 1 du RGPD. Les traitements de données qui sont instaurés par une mesure normative sont presque toujours basés sur l'article 6.1, point c) ou e) du RGPD.

24. En plus de devoir être nécessaire et proportionnée, toute norme régissant le traitement de données à caractère personnel (et constituant par nature une ingérence dans le droit à la protection des données à caractère personnel) doit répondre aux exigences de prévisibilité et de précision afin que les personnes concernées au sujet desquelles des données sont traitées aient une idée claire du traitement de leurs données. En vertu de l'article 6.3 du RGPD, lu en combinaison avec les articles 22 de la *Constitution* et 8 de la CEDH, une telle norme doit décrire les éléments essentiels des traitements allant de pair avec l'ingérence de l'autorité publique. Dans ce cadre, il s'agit au moins :

- de la (des) finalité(s) précise(s) et concrète(s) des traitements de données ;
- de la désignation du (des) responsable(s) du traitement (à moins que cela soit clair).

Si les traitements de données à caractère personnel allant de pair avec l'ingérence de l'autorité publique représentent une ingérence importante dans les droits et libertés des personnes concernées, la disposition légale doit également comprendre les éléments essentiels (complémentaires) suivants :

- les (catégories de) données à caractère personnel traitées qui sont pertinentes et non excessives ;
- les catégories de personnes concernées dont les données à caractère personnel seront traitées ;
- les (catégories de) destinataires des données à caractère personnel ainsi que les conditions dans lesquelles ils reçoivent les données et les motifs y afférents ;
- le délai de conservation maximal des données à caractère personnel enregistrées ;
- l'éventuelle limitation des obligations et/ou droits mentionné(e)s aux articles 5, 12 à 22 et 34 du RGPD.

---

<sup>7</sup> Voir la note de bas de page n° 2.

➤ Application de ces principes

25. À cet égard, l'Autorité estime qu'au vu des finalités du traitement et des catégories de données à caractère personnel à traiter, il est question d'une ingérence importante dans les droits et libertés des personnes concernées. Il s'agit en effet en soi d'un traitement à grande échelle qui a lieu (au moins à titre secondaire) à des fins de surveillance ou de contrôle et qui (certes sous certaines conditions) est largement accessible à des tiers. Cela implique que tous les éléments essentiels doivent être définis dans une norme légale formelle et que seul(e)s des détails et modalités (techniques) ultérieur(e)s peuvent être élaboré(e)s au moyen de dispositions d'exécution, à condition qu'il existe à cet effet une délégation au Roi suffisamment précise.
26. Comme cela a déjà été expliqué ci-dessus, l'avant-projet soumis pour avis concerne **l'exécution** des articles 19*bis*-1 à 19*bis*-3, 19*bis*-6 et 19*bis*-8 de la loi RC auto au sujet desquels l'Autorité s'est déjà prononcée. Dans la mesure où cela est pertinent (et nécessaire), l'Autorité renverra donc à l'avis susmentionné n° 29/2022 et au projet en ce qui concerne les éléments essentiels du traitement. Il est rappelé que le présent avis ne constitue pas une nouvelle évaluation des dispositions de la loi RC auto.

**c. Finalités**

27. Conformément à l'article 5.1.b) du RGPD, le traitement de données à caractère personnel ne peut être effectué que pour des finalités déterminées, explicites et légitimes.
28. Les finalités sont exposées à l'article 19*bis*-8 de la loi RC auto. L'Autorité distingue par paragraphe les finalités suivantes :
- À l'égard du premier paragraphe, le traitement de données à caractère personnel est nécessaire dans ce cadre pour régler les dossiers (indemnisation) des personnes concernées impliquées dans un accident.
  - À l'égard du deuxième paragraphe, le traitement est nécessaire à des fins de contrôle et d'enquête.
  - À l'égard du troisième paragraphe, on peut distinguer trois finalités qui sont reprises conjointement sous le dénominateur de la finalité de preuve :
    - i. obtenir la réparation du dommage subi ;
    - ii. déterminer l'état d'assurance ; et
    - iii. consulter une carte internationale d'assurance automobile.

29. Dans ce cadre, l'avant-projet vise à définir les règles concernant : *i) les demandes de renseignements ; ii) les modalités relatives à l'accès au registre et iii) la forme et le contenu de la demande d'obtention des informations.* L'Autorité en prend acte.

#### **d. Responsable du traitement**

30. Conformément à l'article 4.7) du RGPD, le responsable du traitement est toute personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre. Dans un souci d'exhaustivité, l'Autorité rappelle que la désignation du responsable du traitement doit être adéquate au regard des circonstances factuelles. Tant le Groupe de travail "Article 29" – prédécesseur du Comité européen de la protection des données – que l'Autorité ont insisté sur la nécessité d'aborder ces concepts dans une perspective factuelle. Il est donc nécessaire de désigner la ou les entités qui, dans les faits, poursui(ven)t la finalité du traitement visé et en assure(nt) la maîtrise.
31. Bien que l'avant-projet lui-même ne fasse pas mention du responsable du traitement, il exécute les dispositions légales de la loi RC auto qui mentionne explicitement le responsable du traitement à l'article 19*bis*-6, § 4. L'Autorité **en prend acte.**

#### **e. Minimisation des données/Proportionnalité**

32. L'article 5.1.c) du RGPD prévoit que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités visées (principe de 'minimisation des données').
33. Au préalable, l'Autorité estime nécessaire de fournir des précisions concernant une ambiguïté qui découle de l'avant-projet quant à ce qui doit être conservé selon le demandeur. L'analyse de tous les documents donne l'impression que le demandeur n'a pas l'intention de conserver 'toutes les données relatives à une consultation en vertu de l'article 11 de l'avant-projet'. L'Autorité souligne que vu qu'il s'agit aussi de données à caractère personnel, celles-ci doivent par conséquent être traitées comme telles. À cet égard, il semble utile de rappeler au demandeur qu'en vertu des dispositions du RGPD concernant les mesures de sécurité appropriées<sup>8</sup> et le registre des activités

---

<sup>8</sup> Article 32 du RGPD.

de traitement<sup>9</sup>, le responsable du traitement sera *a fortiori* contraint de conserver les fichiers de journalisation de manière à pouvoir appliquer les principes de transparence et de responsabilité. Il s'ensuit raisonnablement que les données relevant de l'article 11 de l'avant-projet feront également l'objet d'une journalisation. En d'autres termes, les données des destinataires des informations ou du statut d'assurance devront être conservées par le responsable du traitement.

34. Dans ce contexte, vu la nature de la norme, à savoir l'avant-projet, l'Autorité se référera à l'article 19*bis*-8 de la loi RC auto pour contrôler les éléments essentiels de ce volet et à la lumière de ce contrôle, évaluera l'article 11 de l'avant-projet qui remplace l'article 14 de l'arrêté royal du 11 juillet 2003. Compte tenu des différentes finalités et des différentes catégories de personnes, l'Autorité expliquera son évaluation par paragraphe.

35. À l'égard du premier paragraphe, à savoir l'article 19*bis*-8, § 1<sup>er</sup> de la loi RC auto :

36. Celui-ci formule clairement et explicitement quelles catégories de personnes concernées peuvent introduire une demande de renseignements. En outre, il est également indiqué explicitement à quel sujet des renseignements peuvent être obtenus - "*tout véhicule automoteur impliqué dans l'accident*". À la lumière de ces éléments, l'Autorité confirme que les **catégories de personnes concernées qui sont visées sont clairement et précisément indiquées** dans la norme légale formelle. En ce qui concerne **les catégories de données à caractère personnel**, l'Autorité constate que la norme légale formelle indique de manière exhaustive et explicite quelles données peuvent être **obtenues concernant tout véhicule automoteur impliqué dans l'accident**. L'article 11 de l'avant-projet élabore la forme et le contenu de la demande de renseignements comme suit :

*"Art. 11. L'article 14 du même arrêté est remplacé par ce qui suit :*

*Art. 14. § 1<sup>er</sup>. Chaque demande d'information quant à un des éléments visés à l'article 19*bis*-8, § 1<sup>er</sup>, de la loi se fait par simple envoi adressé au Fonds ou par tout moyen électronique qui est mis à la disposition du demandeur par le Fonds.*

***Une demande d'information quant à un des éléments visés à l'article 19*bis*-8, § 1<sup>er</sup>, de la loi, comporte le nom et l'adresse du demandeur, la date de la demande et de l'accident, le pays de l'accident et la marque d'immatriculation du véhicule concerné par cette demande.***

*La date de l'envoi ou la date du système fait foi.*

---

<sup>9</sup> Article 30 du RGPD.

*Le Fonds est tenu, dans les meilleurs délais de communiquer les renseignements demandés par simple envoi ou tout moyen électronique. [...]*".

37. À la lumière du contexte dans lequel une demande de renseignements peut être effectuée, l'Autorité estime acceptable que les données à caractère personnel du demandeur<sup>10</sup> qui seront traitées ne soient définies que dans un arrêté d'exécution.
38. Sans préjudice de la recommandation déjà abordée préconisant d'utiliser 'un moyen d'authentification fort'<sup>11</sup> et de la remarque au point 33, l'Autorité estime que le premier paragraphe - l'article 19*bis*-8, § 1<sup>er</sup> de la loi RC auto et le premier paragraphe de l'article 11 de l'avant-projet - ne donne lieu à aucune remarque particulière concernant la proportionnalité des traitements de données sous-jacents.
39. À l'égard du deuxième paragraphe, l'Autorité constate que la norme légale formelle - à savoir l'article 19*bis*-8, § 2 de la loi RC auto distingue deux scénarios qui indiquent précisément, explicitement et clairement quelles catégories de personnes concernées relèvent de l'application de l'un ou de l'autre scénario. Il s'agit du contrôle de la situation d'assurance d'un véhicule déterminé d'une part et de l'exercice de missions de prévention, de contrôle et d'enquête d'autre part.
40. La différence a trait à l'accès à plusieurs données. Dans la première situation, cela ne va pas au-delà du fait d'indiquer si le véhicule est 'assuré' ou si le statut d'assurance est 'inconnu'. Dans la deuxième situation, un accès est accordé aux données pertinentes du registre visé à l'article 19*bis*-6 de la loi RC auto, selon les missions légales. À cet égard, l'Autorité renvoie à son avis n° 29/2022 qui attirait l'attention sur les mesures techniques et organisationnelles dans un souci de protection des droits et libertés des personnes concernées<sup>12</sup>. Conformément à cet élément, l'article 11 de l'avant-projet prévoit les modalités relatives à l'accès, telles que formulées ci-après :
- "[...] § 2. Le Fonds met à disposition des personnes visées à l'article 19bis-8, § 2, de la loi un **accès sécurisé, avec authentification forte**, au registre visé à l'article 19bis-6 de la loi. Les autorités mettent en place un système informatique intégrant l'accès sécurisé mis à disposition par le Fonds.*

---

<sup>10</sup> Ou **destinataire** des informations.

<sup>11</sup> Voir la note de bas de page n° 2.

<sup>12</sup> Voir l'avis n° 29/2022, point 32.

*Cette intégration obéit à **des règles de sécurité strictes, à savoir le cryptage, la liste blanche des adresses IP et l'utilisation d'un token.***

***L'identité des membres consultants le registre est enregistrée par chaque autorité.***

*L'accès des personnes visées à l'article 19bis-8, § 2, est limité aux finalités et aux membres visés à l'article 19bis-8, § 2, dans l'exercice de leur mission. Les autorités veillent au respect de cette obligation, par leurs membres ayant accès au registre. Ils organisent le **contrôle de l'utilisation des données, les journaux et les audits nécessaires.***

*Une liste actualisée des personnes ayant accès au registre avec la mention de leur qualité, est établie par chaque autorité et mise à la disposition de l'Autorité de protection des données.*

*L'accès visé à l'article 19bis-8, § 2, alinéa 1<sup>er</sup>, permet une consultation en temps réel, en permanence et à distance.*

*Concernant les informations visées à l'article 19bis-8, § 2, alinéa 3, le Fonds est tenu, de communiquer dans les meilleurs délais les renseignements demandés par simple envoi ou tout moyen électronique. [...]"*

41. Tout d'abord, l'Autorité souligne que dans la pratique, "l'utilisation d'un token" peut cacher de très nombreuses technologies et est dès lors considérée par les techniciens comme une expression vague. Auparavant, ce terme désignait un dispositif matériel externe ([https://en.wikipedia.org/wiki/Security\\_token](https://en.wikipedia.org/wiki/Security_token)). Cependant, à présent, il peut non seulement être implémenté dans un logiciel sur un smartphone mais il peut aussi s'agir d'un JSON Web token, ce qui constitue une représentation dans une chaîne de bits d'une security claim. À la lumière de ces éléments, l'Autorité demande d'éviter le terme "token" dans l'avant-projet.
42. Les mesures techniques et organisationnelles suivantes sont établies : *i) un accès sécurisé, avec authentification forte ; ii) des règles de sécurité strictes - le cryptage, la liste blanche des adresses IP et l'utilisation d'un token<sup>13</sup> ; iii) l'enregistrement de l'identité lors de la consultation du registre ; iv) le contrôle de l'utilisation des données ; v) des journaux ; vi) des audits ; vii) une liste actualisée des personnes ayant accès au registre.*
43. Vu qu'un contrôle de la situation d'assurance ne procure pas un accès direct aux données du registre de l'article 19bis-6 de la loi RC auto mais se limite au statut d'assurance, à savoir 'assuré'

---

<sup>13</sup> L'Autorité renvoie au point 32 de l'avis n° 29/2022 concernant le fait d'éviter l'utilisation du terme 'token'.

ou 'inconnu', l'Autorité présume que les mesures techniques et organisationnelles énumérées n'ont pas été visées pour la première situation. À la lumière des points 15-22 discutés précédemment concernant l'authentification forte, l'Autorité demande que soient apportées les adaptations nécessaires de manière à ce que l'utilisation d'un moyen d'authentification fort soit également imposée pour les destinataires d'une réponse binaire concernant le statut d'assurance d'un véhicule automoteur<sup>14</sup>.

44. En ce qui concerne la deuxième situation, à savoir l'exercice de missions de prévention, de contrôle et d'enquête, l'Autorité estime que l'introduction des mesures techniques et organisationnelles susmentionnées dans l'avant-projet montre qu'il a été tenu compte des recommandations de l'avis antérieur<sup>15</sup>. L'Autorité en prend acte.

45. À l'égard du troisième paragraphe, à savoir l'article 19bis-8, § 3<sup>er</sup> de la loi RC auto :

46. L'Autorité estime que les catégories de personnes pouvant introduire une demande d'obtention d'informations ont été clairement définies dans la norme législative formelle, à savoir l'article 19bis-8, § 3, alinéa 1 de la loi RC auto. En ce qui concerne les catégories de données à caractère personnel, il découle de la disposition susmentionnée qu'il n'y a pas d'accès au registre (aux données du registre) de l'article 19bis-6 de la loi RC auto. La communication d'informations à un demandeur (destinataire) est limitée "à la confirmation que le Fonds est ou non en possession de données prouvant l'existence du contrat d'assurance."<sup>16</sup> En exécution de cette disposition, une délégation au Roi est prévue à l'article 11 de l'avant-projet pour déterminer la forme et le contenu de la demande, formulée comme suit :

*"[...] § 3. La demande d'information visée à l'article 19bis-8, § 3, de la loi est introduite par le moyen électronique que le Fonds met à disposition.*

*La consultation du statut d'assurance sur le site web est protégée par un code de validation garantissant qu'elle n'est pas initiée par un programme informatique.*

*Le demandeur doit :*

*1° confirmer que sa demande est justifiée par au moins une qualité suivante :*

- a) une personne lésée, ou une personne qui intervient en son nom ;*
- b) le propriétaire du véhicule ou une personne qui intervient en son nom ;*
- c) le conducteur du véhicule ou une personne qui intervient en son nom ;*

<sup>14</sup> Voir la note de bas de page n° 2.

<sup>15</sup> Voir à cet effet l'avis n° 29/2022, point 32.

<sup>16</sup> Conformément à l'avis n° 29/2022, point 24.

d) le détenteur du véhicule ou une personne qui intervient en son nom ;  
e) une personne physique ou morale qui est habilitée par la loi, un décret ou une ordonnance à solliciter la preuve d'assurance, à l'exclusion des personnes visées à l'article 19bis-8, § 2 ;

2° prendre connaissance du fait qu'en absence d'un d'intérêt légitime [NdT : il convient de lire "en l'absence d'intérêt légitime" ou "en l'absence d'un intérêt légitime"], il dispose de l'information de manière illicite ;

3° déclarer qu'il ne va pas utiliser l'information fournie à des fins sans lien avec la raison invoquée dans sa demande ;

4° confirmer avoir pris connaissance de la déclaration de confidentialité relative à la protection des données.

*La recherche s'effectue sur base de la marque d'immatriculation ou du numéro de châssis.*

*La demande précise la date pour laquelle l'information est demandée. Cette date ne peut être antérieure de plus de six mois à la date de la demande.*

*L'accès visé à l'article 19bis-8, § 3, permet une consultation en temps réel, en permanence et à distance."*

47. Le fait que les catégories de personnes pouvant introduire une demande d'information transparaisse clairement dans la norme législative formelle a déjà été confirmé au point 46. Bien que l'avis antérieur soulignait que des données relatives à l'identité et à la qualité devraient être collectées, **ni la norme législative formelle, ni l'avant-projet n'indiquent explicitement quelles catégories de données à caractère personnel sont requises dans une telle demande**<sup>17</sup>. On peut supposer que pour établir une qualité ou une identité, au moins le nom, le prénom et idéalement le numéro de Registre national<sup>18</sup> doivent être connus. L'Autorité demande que cette lacune soit comblée et, dans la mesure du possible, que les informations requises soient limitées à ce qui relève du premier paragraphe de l'article 11 de l'avant-projet. L'Autorité souligne que cette exigence est forcément satisfaite en utilisant l'authentification forte recommandée, comme cela a été expliqué précédemment aux points 15-22<sup>19</sup>.

---

<sup>17</sup> Voir l'avis n° 29/2022, point 30.

<sup>18</sup> L'Autorité souligne que chaque utilisation du Registre national est soumise aux dispositions de la loi du 8 août 1983 *organisant un registre national des personnes physiques* et spécialement les articles 5 et 8 qui doivent logiquement aussi être mentionnés dans la norme envisagée.

<sup>19</sup> Voir la note de bas de page n° 2.

48. Comme cela a déjà été précisé dans l'avis n° 29/2022, ce qui relève de l'article 19*bis*-8, § 3 de la loi RC auto concerne un nouveau traitement de données ayant une finalité générale qui peut être catégorisée d'administration de la preuve. À cet égard, l'Autorité constate, conformément à son avis antérieur, qu'un véhicule n'est admis à la circulation que si le conducteur peut apporter la preuve d'un contrat d'assurance. L'avis antérieur soulignait déjà qu'une dispense pour les assureurs de délivrer un certificat international d'assurance pouvait constituer un risque pour la liberté de mouvement des preneurs d'assurance<sup>20</sup>. L'Autorité fait remarquer que les mesures d'exécution prévues dans le projet répondent aux recommandations formulées dans l'avis antérieur et sont jugées suffisantes pour faire face aux risques potentiels pour les droits et libertés des preneurs d'assurance<sup>21</sup>.

#### f. Délai de conservation

49. En vertu de l'article 5.1.e) du RGPD, les données à caractère personnel ne peuvent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées.

50. Pour le délai de conservation, l'Autorité souligne la distinction entre les données du registre, telles que définies à l'article 19*bis*-6, § 2 de la loi RC auto, et les données qui doivent être traitées en vertu de l'article 19*bis*-8 de la loi RC auto et de l'avant-projet, qui l'exécute. Le formulaire de demande d'avis relatif au présent avant-projet précise ce qui suit :

*" - pour le registre, c'est prévu par la loi de base art. 19bis-6, §2.*

*- dans le cadre de l'article 11 de l'avant-projet d'arrêté, il nous semble que les **données relatives à la consultation**<sup>22</sup> ne peuvent pas être conservées, comme l'explique le préambule cfr aussi le considérant 18 de la Directive 2021/2118 du Parlement européen et du Conseil du 24 novembre 2021 modifiant la directive 2009/103/CE. <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32021L2118><sup>23</sup>*

51. Il est fait référence à juste titre à l'article 19*bis*-6, § 2 de la loi RC auto qui indique **que les données du registre** ne peuvent pas être conservées au-delà de 7 ans après que l'immatriculation du véhicule ou le contrat d'assurance a pris fin.

<sup>20</sup> Voir l'avis n° 29/2022, point 19.

<sup>21</sup> Voir l'avis n° 29/2022, points 16-25.

<sup>22</sup> Mise en gras ajoutée par l'Autorité.

<sup>23</sup> En français dans le texte.

52. En ce qui concerne l'article 11 de l'avant-projet, lu conjointement avec l'article 19*bis*-8 de la loi RC auto, l'Autorité adopte un point de vue divergent de celui du demandeur. Une analyse contextuelle du passage qui précède, le préambule de l'avant-projet<sup>24</sup> et la référence à la directive<sup>25</sup> permettent à l'Autorité de conclure - comme cela a été expliqué précédemment aux points 17-18 - que lors de l'évaluation relative au traitement de données (à caractère personnel), le demandeur a uniquement pris en considération le statut d'assurance de l'assuré (du non-assuré), qui comprend une réponse binaire - 'assuré' ou 'inconnu'. Sans préjudice de la recommandation sur l'utilisation d'un moyen d'authentification fort, le traitement de données à caractère personnel d'autres parties - à savoir les destinataires qui demandent le statut d'assurance ou des informations du registre<sup>26</sup> -, relève également de cette évaluation. Il s'agit en l'occurrence des *données relatives aux demandes d'information quant à un des éléments visés à l'article 19bis-8, § 1<sup>er</sup> de la loi RC auto, des journaux et de l'enregistrement de l'identité des membres qui consultent le registre mais également des données des demandes d'information relevant de l'article 14, § 3 de l'arrêté royal du 11 juillet 2003 tel que modifié par l'article 11 de l'avant-projet*. La plus-value d'une disposition qui prévoit que de telles données seront requises de la part des destinataires, pour être immédiatement effacées ensuite, est remise en question. Par ailleurs, la raison de demander dans un premier temps de telles données semble incompatible avec l'intention de ne pas les conserver. En outre, comme cela est expliqué au point 33, on suppose que le responsable du traitement conservera au moins les fichiers de journalisation. Étant donné que l'utilisation d'un moyen d'authentification fort est prévue, l'Autorité conclut que dans le cadre de l'article 11 de l'avant-projet, des données devront quoi qu'il en soit être conservées<sup>27</sup>.

---

<sup>24</sup> L'avant-projet stipule notamment ce qui suit : "*Considérant que l'utilisation d'un numéro de plaque ou d'un numéro de châssis est un traitement de données à caractère personnel lorsque ce numéro de plaque permet d'identifier une personne physique, ce qui n'est pas le cas lorsque le site génère une réponse concernant le statut d'assurance car il ne transfère pas un élément de données à caractère personnel puisque le propriétaire, le preneur d'assurance, l'assureur ne sont pas identifiables ; Considérant que lorsque le site web spécifique est consulté et que "assuré" est mentionné, aucun détail concernant le contrat d'assurance comme l'assureur, le numéro de la police d'assurance, le preneur d'assurance n'est communiqué pour raison de confidentialité ; Considérant que la communication du statut d'assurance, sans mentionner l'identité du propriétaire du véhicule, de l'assureur, du numéro de police d'assurance, n'entraîne pas un risque élevé pour les droits et libertés des personnes concernées.*"

<sup>25</sup> Considérant 18 de la Directive n° 2021/2118 du 24 novembre 2021 modifiant la directive 2009/103/CE concernant l'assurance de la responsabilité civile résultant de la circulation de véhicules automoteurs et le contrôle de l'obligation d'assurer cette responsabilité, JO du 2 décembre 2021, L 430/1 : "*Conformément auxdits principes, les États membres ne devraient pas conserver les données à caractère personnel traitées exclusivement aux fins d'un contrôle de l'assurance au-delà de la période nécessaire pour vérifier si un véhicule est couvert par une assurance valide. Lorsqu'il est constaté qu'un véhicule est couvert, il convient d'effacer toutes les données relatives à cette vérification. Lorsqu'un système de vérification ne permet pas de déterminer si un véhicule est assuré, il convient de conserver ces données uniquement pendant une période limitée, qui n'excède pas le nombre de jours nécessaire pour établir l'existence d'une couverture par une assurance. Lorsqu'il est constaté qu'un véhicule n'est pas couvert par une police d'assurance valide, il est raisonnable d'imposer la conservation de ces données jusqu'à la fin de la procédure administrative ou judiciaire et la couverture du véhicule par une police d'assurance valide.*" (mise en gras ajoutée par l'Autorité).

La référence faite à cet égard concerne uniquement les données relatives à un contrôle d'assurance.

<sup>26</sup> Voir à cet effet l'avis n° 29/2022, points 15 et 30.

<sup>27</sup> Voir la note de bas de page n° 2.

53. À la lumière de ces éléments, l'Autorité demande que la loi de base prévoie également un délai de conservation maximal pour ces données.

**PAR CES MOTIFS,**

**l'Autorité,**

**estime que les modifications suivantes s'imposent dans l'avant-projet :**

- utiliser un moyen d'authentification fort pour chaque accès (in)direct au registre, tel que visé à l'article 19*bis*-6 de la loi RC auto (points 15-22, 43,47) ;
- remplacer le terme 'token' (point 41) ;
- décrire davantage les catégories de données à caractère personnel, en veillant à ce que seules les catégories de données strictement nécessaires et pertinentes pour la finalité visée soient mentionnées (point 52) ;
- spécifier un délai de conservation maximal pour les données à caractère personnel des destinataires d'informations ou du statut d'assurance (points 52-53).

Pour le Centre de Connaissances,  
(sé.) Cédric Morlière, Directrice