Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 10/2024 van 9 februari 2024

Betreft: Advies m.b.t. voorontwerp van koninklijk besluit tot *wijziging van het koninklijk besluit van 11 juli 2003 houdende de vaststelling van de toelatingsvoorwaarden en de werking van het Belgisch Bureau en het Gemeenschappelijk Waarborgfonds* (CO-A-2023-526)
Sleutelwoorden: sterke authenticatiemiddel – kentekenplaat – nummerplaat – real time systeem – online raadpleging – QR-code – digitale en of papieren internationale verzekeringsbewijs – verzekeringsstatus – raadpleging register bedoeld in artikel artikel 19bis-6 WAM – binair antwoord kan een persoonlijk gegeven uitmaken - logs
Originele versie

Het Kenniscentrum van de Gegevensbeschermingsautoriteit (hierna: de Autoriteit), aanwezig: mevrouw Juline Deschuyteneer, mevrouw Cédrine Morlière en mevrouw Griet Verhenneman en de heren Yves-Alexandre de Montjoye, Bart Preneel en Gert Vermeulen;

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit,* inzonderheid op artikelen 23 en 26 (hierna: WOG);

Gelet op de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (hierna: AVG);

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna: WVG);

Gelet op het verzoek om advies van De heer Yves Dermagne, vice-eersteminister en minister van Economie en Werk, (hierna aanvrager) ontvangen op 13/11/2023;

brengt op 9 februari 2024 het volgend advies uit:

I. VOORWERP VAN DE ADVIESAANVRAAG

1. Op 13 november 2023 verzocht de aanvrager het advies van de Autoriteit met betrekking tot een voorontwerp van koninklijk besluit *tot wijziging van het koninklijk besluit van 11 juli 2003 houdende de vaststelling van de toelatingsvoorwaarden en de werking van het Belgisch Bureau en het Gemeenschappelijk Waarborgfonds* (hierna: het voorontwerp).

2. Het voorontwerp kadert binnen een algemeen streven naar digitalisering en administratieve vereenvoudiging, met de mogelijkheid om de aansprakelijkheidsverzekeraar voor motorrijtuigen vrij te stellen van de afgifte van de internationale motorrijtuigenverzekeringskaart (de groene kaart), mits aan bepaalde voorwaarden wordt voldaan.

3. Meer concreet beoogt het voorontwerp de uitvoering van de artikelen 19bis-1 tot 19bis-3, 19bis-6 en 19bis-8 van de *wet van 21 november 1989 betreffende de verplichte aansprakelijkheidsverzekering inzake motorrijtuigen* (hierna: WAM), met als doel een register in real time te creëren dewelke informatie over de verzekeringsstatus zal geven zoals gekend door het Gemeenschappelijke Waarborgfonds en dit door middel van een binair antwoord ("verzekerd" of "onbekend").

4. Binnen deze context specifieert het voorontwerp: *i) de vorm en inhoud van het verzoek om inlichtingen bepalen zoals gestipuleerd in artikel 19bis-8, §1, lid 3 WAM; ii) de modaliteiten met betrekking tot de toegang tot het register uit artikel 19bis-6, zoals voorzien in artikel 19bis-8, §2, lid 2 WAM en iii) de vorm en de inhoud van de aanvraag tot het bekomen van de informatie zoals aangegeven in artikel 19bis-8, §3, lid 2 WAM*.

5. Er wordt aan herinnerd dat de Autoriteit zich, in advies nr. 29/2022, betreffende *het wetsontwerp houdende diverse bepalingen inzake economie*, reeds heeft uitgesproken over de wijzigingen die ingevoerd zijn in de voormelde bepalingen van de basiswet, weergegeven in punt 3. De Autoriteit, acht het bijgevolg relevant, om terug te koppelen naar de aanbevelingen die daarin werden voorzien. De Autoriteit noteert voorts dat nieuwe bepalingen van het *ontwerp van koninklijk besluit tot wijziging van het koninklijk besluit van 13 februari 1991 houdende de inwerkingtreding en uitvoering van de wet van 21 november 1989 betreffende de verplichte aansprakelijkheidsverzekering inzake motorrijtuigen* (hierna: ontwerp), opvolging geven aan de aanbevelingen van advies nr. 29/2022 en derhalve, waar toepasselijk, betrokken zullen worden in de beoordeling.

II. KORTE SAMENVATTING EN OBSERVATIES

6. De aan advies onderwerpen norm, beoogt uitvoering te geven aan enkele bepalingen van de WAM, waar zoals eerder toegelicht, de Autoriteit zich reeds over uitgesproken heeft. Het oogmerk om naast het huidige papieren systeem, een elektronisch systeem op poten te zetten, met een real time raadpleging over de verzekeringssituatie van een motorrijtuig of over het al dan niet in bezit zijn van gegevens tot bewijs van het bestaan van de verzekeringsovereenkomst, die gepaard gaat met de mogelijkheid voor elke burger om het systeem te raadplegen, werd in eerder advies aangeduid als een risico voor de rechten en vrijheden van een betrokkene. Op grond hiervan adviseerde de Autoriteit om, voor elke elektronische raadpleging, gebruik te maken van een sterke authenticatie. Ondanks deze eerdere aanbevelingen wordt in de uitvoerende norm nog steeds aangedrongen op eerder afgeraden systematiek. Bijgevolg meent de Autoriteit, dat het noodzakelijk is om de gevaren verbonden aan dit nieuw systeem opnieuw te benadrukken.

7. Concreet gaf de Autoriteit in eerder advies al aan dat een controle door technische en organisatorische maatregelen noodzakelijk was omdat er met de mogelijkheid voor elke burger om het systeem te raadplegen, risico's voor de rechten en vrijheden van de betrokkenen konden ontstaan. De Autoriteit verwees terzake naar een misbruik van een systeem in strijd met het doel ervan, bijvoorbeeld latere publicatie van geraadpleegde gegevens met de bedoeling schade toe te brengen.

8. Het is met name dit vrij toegankelijk systeem, die ofschoon in de wet aangeduid wordt wie het kan raadplegen, maar in praktijk open staat voor iedereen, die aanleiding voor bezorgdheid geeft. Een onbeperkte toegang, waarbij geen gegevens bijgehouden worden van de raadplegers, brengt verschillende gevaren met zich mee. Denk maar aan situaties waarbij bedrijven potentieel lijsten gaan bijhouden over een verzekeringsstatus en deze nadien verkopen of gebruiken voor enigerlei doeleinde of situaties waarbij men in retributie buren, collega's, anderen waar onenigheid heerst, gaat controleren of pesten of nog situaties waarbij geen limieten zijn op de raadplegingen. Het aanvinken dat de raadpleging met gerechtvaardigd belang gebeurt of dat de verstrekte informatie niet gebruikt zal worden voor doeleinden die geen verband houden met de in de aanvraag aangehaalde redenen, is verre van een adequate beschermingswaarborg. Dit geldt te meer, daar de wetgever niet van inziens is om enige identificatie van de raadpleger bij te houden en de vereiste kennisname bijgevolg onbeduidend wordt.

9. Het is vanuit deze invalshoek, dat eerder advies de aanbeveling gaf om een sterke authenticatiemiddel te gebruiken. In aanmerking genomen dat de wetgever geen alternatief systeem voorstelt, die dergelijk sterk authenticatiemiddel overbodig maakt, bouwt onderhevig advies voort op het eerder aanbevolen gebruik van een sterk authenticatiemiddel.

10. De Autoriteit is er zich van bewust dat de invoering van een sterke authenticatiemethode, niet evident is in de actuele technologische context. Doch wordt onderstreept dat, de eIDAS-verordening, voor de Europese burgers, reeds vandaag, maar ook zeker naar de toekomst toe, een geschikt instrument is dat in aanmerking genomen moet worden. Daarnaast blijft ongeacht de aanbeveling om een sterke authenticatiemiddel te hanteren, de real time raadpleging, in de situatie van derdelanders een neteligere kwestie, o.m. hogere roaming kosten. Bovendien, wijst de Autoriteit erop dat het beoogde real time raadpleging systeem nog andere zwakheden vertoont. Zo wordt geen rekening gehouden met situaties waar geen internet bereik zou zijn of de batterij van een smartphone plat zou zijn of zelfs situaties waar de betrokkene geen smartphone zou hebben.

11. Daarnaast wordt ook een kanttekening gemaakt bij de periode die na het wettelijk vermoeden van geldig verzekerd voertuig volgt. De Autoriteit stelt vast dat er na die periode, geen wettelijk vermoeden geldt als verzekerd voertuig. In een potentieel scenario waar het platform blootgesteld wordt aan een systeemfalen, zal de verzekeringsnemer alsnog in een situatie zitten, waarbij geen bewijs van verzekering afgeleverd kan worden.

12. Kortom, het is precies die keuze van de wetgever, voor een systeem dat dergelijke risico's met zich meebrengt, in het voor advies voorgelegd ontwerp, dat ertoe strekt om aan te dringen op het gebruik van een sterk authenticatiemiddel. Met andere woorden, de keuze van de wetgever voor een ander systeem, zou mogelijks tot een ander oordeel of advies kunnen leiden, waarbij niet noodzakelijk een sterk authenticatiemiddel vereist zou worden. In dat verband merkt de Autoriteit op dat de meest adequate oplossing zowel voor het beoogd doel van de wetgever, als de bescherming van de rechten en vrijheden van de betrokkene en die bovendien ook een oplossing zou bieden voor de aangehaalde zwakheden, het gebruik van een QR-code is, naast de huidige papieren internationale verzekeringsbewijs.

13. In een kader waar de systematiek van een QR-code ingevoerd zou worden (**hetgeen een aanpassing van het wettelijk kader vereist**), bezorgen verzekeraars, aan de verzekerde, een digitaal document met een uniek nummer VZ staat, zowel in QR-code als een combinatie van letters en cijfers, dat bij het voertuig van de verzekerde hoort. Dit zou het mogelijk maken om ter plaatse bij het ongeval de verzekeringsstatus na te gaan als de andere partij online toegang heeft. Als er geen internet verbinding is, kan de VZ gekopieerd worden (met een camera of manueel) en achteraf online, de status nagaan. Het verschil met het huidige voorstel is dat de verificatie niet op basis van publiek beschikbare informatie (het identificatieteken - kentekenplaat of het VIN nummer) gebeurt. Dit vermindert sterk het risico dat iemand van een buur of collega de verzekeringsstatus opvraagt en heeft tot gevolg dat sterke authenticatie niet meer essentieel is.

Niettemin moet er nog altijd wel beveiliging toegevoegd om te beletten dat iemand voor een groot aantal (willekeurige) VZ nummers de verzekeringsstatus kan opvragen (*opvragen email adres, rate limiting per IP adres, captcha*). Rekening houdend met de technologische vooruitgang en het daarmee samenhangend rijzend regelgevend kader, is de Autoriteit van oordeel dat het een meerwaarde blijft om de mogelijkheid open te laten dat men zich authenticeert op basis van eiDAS, zodat dit in de toekomst wel verplicht gemaakt kan worden.

14. Er wordt voorts ook aanbevolen dat de verzekeraar, de verzekerde steeds inlicht van de praktische risico's, zoals aangekaart in punten 8 t.e.m. 11 die gepaard gaan met de overstap van een papieren internationale verzekeringsbewijs naar een digitaal systeem.

III. ONDERZOEK TEN GRONDE

a. Voorafgaande opmerkingen

15. Alvorens verder in te gaan op de bespreking van het voorontwerp, wenst de Autoriteit de aandacht te vestigen op enkele punten die in advies nr. 29/2022 reeds aangekaart werden, maar in onderhevig advies niet opgenomen zijn geweest.

16. Terzake stelt het voorwoord van het voorontwerp het volgende:

> "*Overwegende dat zelfs als er een sterk authenticatiemiddel zou worden ingevoerd, het moeilijk is om het bewaren van de gegevens in verband met deze raadpleging te rechtvaardigen zonder de privacy te schenden, zodat alle sporen van verbinding zouden moeten worden gewist;*
>
> *Overwegende dat als het niet mogelijk is om de raadpleging met sterke authenticatie bij te houden, het geen toegevoegde waarde heeft om sterke authenticatiemaatregelen te implementeren om het risico op misbruik van het systeem, dat in strijd is met het doel ervan, te minimaliseren;"*

17. De Autoriteit is van inziens dat voormelde stellingen **niet overeenstemmen met de aanbeveling om gebruik te maken van een krachtig authenticatiemiddel**, **voor elke toegang en raadpleging** van het register bedoeld in artikel 19bis-6 WAM.[1] Uit de stellingname kan worden afgeleid dat de aanvrager van het voorontwerp, een sterke authenticatie disproportioneel acht, t.a.v. de informatie die door de aanvrager (ontvanger) ontvangen wordt,

[1] Merk op dat de aanbeveling van een sterke authenticatie gebaseerd is op de ratio uit punten 9 t.e.m. 12. De Autoriteit onderstreept dat gelet op de huidige technologische stand van zaken en in aanmerking genomen van het geheel aan tekortkomingen, de meest adequate systematiek het gebruik van een QR-code is, zoals toegelicht in punten 12 t.e.m. 13, hetgeen een aanpassing van het wettelijk kader vereist.

n.b., het 'binair antwoord' dat ontvangen wordt over de verzekeringsstatus. Doch wijst de Autoriteit erop dat om een binair antwoord over de verzekeringsstatus te kunnen voorzien er toegang tot het register noodzakelijk is. Hierdoor, wordt, hoewel het antwoord zich beperkt tot 'verzekerd' of 'onbekend', onrechtstreeks informatie verschaft over het register. Bovendien is deze informatie steeds gelinkt aan een kentekenplaat of chassisnummer. Bijgevolg kan de communicatie van een binair antwoord over de verzekeringsstatus niet los worden gekoppeld van een persoonlijk gegeven. Hetgeen nogmaals bevestigd is geweest in een recent arrest door het Hof Van Justitie.[2]

18. Voorgaand in acht genomen, zijn volgende stellingen van de aanvrager, in het voorontwerp, klaarblijkelijk onterecht:[3]

> "*[…] het gebruik van een kenteken of chassisnummer een verwerking van persoonsgegevens vormt wanneer het kenteken het mogelijk maakt een natuurlijke*

---

[2] HvJ 9 november 2023, nr. C-319/22, ECLI:EU:C:2023:837, paras 44-50: " 44 In eerste instantie moet, ter beantwoording van deze vraag, worden onderzocht of het VIN onder het begrip „persoonsgegeven" valt in de zin van artikel 4, punt 1, AVG, dat dit begrip definieert als „alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon".

45 **Deze definitie is van toepassing wanneer die informatie wegens haar inhoud, doel of gevolg gelieerd is aan een bepaalde natuurlijke persoon** [arrest van 8 december 2022, Inspektor v Inspektorata kam Visshia sadeben savet (Doel van de verwerking van persoonsgegevens – Strafrechtelijk onderzoek), C-180/21, EU:C:2022:967, punt 70]. Om te **bepalen of een natuurlijke persoon direct of indirect identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is, in de zin van artikel 4, punt 7, AVG, dan wel door enige andere persoon kunnen worden ingezet om deze persoon te identificeren, zonder dat vereist is dat alle informatie aan de hand waarvan de betrokken persoon kan worden geïdentificeerd, bij een en dezelfde entiteit berust** (zie in die zin arrest van 19 oktober 2016, Breyer, C-582/14, EU:C:2016:779, punten 42 en 43).

46 Zoals de advocaat-generaal in de punten 34 en 39 van zijn conclusie heeft opgemerkt, verkrijgt een gegeven als het VIN – dat in artikel 2, punt 2, van verordening nr. 19/2011 wordt gedefinieerd als de alfanumerieke code die door de fabrikant aan een voertuig wordt toegekend om de adequate identificatie van elk voertuig mogelijk te maken en daardoor als zodanig geen „persoonlijk" karakter heeft – **een dergelijk karakter voor degenen die redelijkerwijs over de middelen beschikken om het aan een bepaalde persoon te liëren.**

47 Uit punt II.5 van bijlage I bij richtlijn 1999/37 **volgt dat het VIN moet worden vermeld op het kentekenbewijs** van een voertuig, evenals de naam en het adres van de houder van dat kentekenbewijs. Bovendien kan een natuurlijke persoon op grond van punt II.5 en punt II.6 van die bijlage in dat kentekenbewijs worden **aangeduid als eigenaar van het voertuig of als een persoon die in een andere juridische hoedanigheid dan die van eigenaar over het voertuig kan beschikken**.

48 **Gelet daarop vormt het VIN een persoonsgegeven in de zin van artikel 4, punt 1, AVG van de natuurlijke persoon die op hetzelfde kentekenbewijs is vermeld, voor zover degene die er toegang toe heeft over de middelen kan beschikken om het redelijkerwijs in te zetten voor de identificatie van de eigenaar van het voertuig of van een persoon die in een andere juridische hoedanigheid dan die van eigenaar over het betrokken voertuig kan beschikken.**

49 Zoals de advocaat-generaal in de punten 34 en 41 van zijn conclusie heeft opgemerkt, **vormt het VIN, wanneer de onafhankelijke marktdeelnemers redelijkerwijs kunnen beschikken over middelen waarmee een VIN kan worden gekoppeld aan een geïdentificeerde of identificeerbare natuurlijke persoon**, hetgeen de verwijzende rechter dient te verifiëren, **voor deze marktdeelnemers een persoonsgegeven in de zin van artikel 4, punt 1, AVG,** en is het VIN dit ook indirect voor de autofabrikanten die het ter beschikking stellen, ook al is het VIN op zich voor laatstgenoemden geen persoonsgegeven en is het dat niet met name wanneer het voertuig waaraan dit VIN is toegekend niet aan een natuurlijke persoon toebehoort.

50 Indien uit de in het vorige punt van het onderhavige arrest vermelde verificatie blijkt dat een VIN moet worden beschouwd als een persoonsgegeven, dan **valt het krachtens artikel 2, lid 1, AVG binnen de werkingssfeer van de AVG en moet het dus in overeenstemming met deze verordening worden verwerkt**."

* 'voertuigidentificatienummer' (VIN): "*de alfanumerieke code die door de fabrikant aan een voertuig wordt toegekend om de adequate identificatie van elk voertuig mogelijk te maken*."

[3] Zie in dat verband ook arrest Breyer, C-582/14, EU:C:2016:779, punten 42 en 43, aangaande de identificeerbaarheid van een persoon.

persoon te identificeren, wat niet het geval is wanneer de site een antwoord genereert over de verzekeringsstatus, aangezien er geen persoonsgegevens worden doorgegeven aangezien de eigenaar, de verzekeringnemer of de verzekeraar niet kunnen worden geïdentificeerd;"

"[…] de toegang tot de informatie over de vraag of het in artikel 19bis-6 van voornoemde wet van 21 november bedoelde register al dan niet informatie bevat over de verzekeringsstatus van het motorvoertuig, bijgevolg geen inbreuk vormt op de rechten van de betrokkenen, aangezien geen persoonsgegevens worden meegedeeld;"

19. Bovendien moet, zoals later toegelicht, evengoed van ontvangers van de verzekeringsstatus persoonlijke gegevens worden bewaard.

20. Voorts wenst de Autoriteit in te gaan op de overweging van het voorontwerp die het volgende stelt:

"*Overwegende dat een sterke authenticatiemethode bovendien de toegang tot de informatie zou verhinderen voor bepaalde personen die er een gerechtvaardigd belang bij hebben de verzekeringsstatus te kennen, zoals personen met de buitenlandse nationaliteit;*"

21. Terzake merkt de Autoriteit op dat op Europees niveau de eIDAS-verordening, die sinds 2016 van toepassing is, een elektronische identificatie faciliteert.[4] De aanvrager beschikt desgevallend over een ruime keuzemarge tussen de verschillende betrouwbaarheidsniveaus (laag, substantieel en/of hoog). Bovendien zijn er een aantal technische praktijken[5], overeenkomstig eerder geleverd advies 98/2022, die als behoorlijke en goede praktijken gekenmerkt worden, denk bijvoorbeeld aan het gebruik van een *captcha*, *rate limiting* en de toepassing van oplossingen die bijvoorbeeld het technisch *in bulk downloaden* verbieden. In het licht hiervan werpt de Autoriteit op dat een buitenlandse nationaliteit geen obstakel is voor het gebruik van een sterke authenticatiemethode.

22. Het geheel in acht genomen, blijft de Autoriteit bij haar standpunt, dat een sterke authenticatie noodzakelijk is, ook voor ontvangers van de informatie betreffende de verzekeringsstatus van een motorrijtuig. Aldus acht de Autoriteit, in tegenstelling tot de aanvrager, dat een sterk authenticatiemiddel geoorloofd en proportioneel is en wordt zo de aanname ontkracht dat een

[4] Artikel 3(1) eIDAS verordening: "*het proces van het gebruiken van persoonsidentificatiegegevens in elektronische vorm die op unieke wijze een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, aanduiden*."

[5] De Autoriteit wijst er echter op dat het beperken van de toegang tot personen binnen de EU uiterst gemakkelijk te omzeilen zal zijn, bijvoorbeeld door gebruik te maken van een VPN.

sterk authenticatiemiddel 'niet mogelijk' of 'geen toegevoegde waarde heeft'. In het licht hiervan **dringt de Autoriteit erop aan om in het voorontwerp een sterke authenticatie te voorzien voor elke raadpleging van het register, inclusief voor de ontvangers van een binair antwoord over de verzekeringsstatus van een motorrijtuig.**[6]

b. Rechtsgrond

- Algemene principes

23. Elke verwerking van persoonsgegevens moet een rechtsgrond of een rechtmatigheidsgrond hebben, zoals bepaald in artikel 6, lid 1, van de AVG. Gegevensverwerkingen die bij een normatieve maatregel zijn ingevoerd, zijn bijna altijd gebaseerd op artikel 6, lid 1, punt c) of e), van de AVG.

24. Elke norm die de verwerking van persoonsgegevens regelt (en die van nature een inmenging vormt in het recht op bescherming van persoonsgegevens) moet niet alleen noodzakelijk en evenredig zijn, maar ook voldoen aan de eisen van voorspelbaarheid en nauwkeurigheid, zodat de betrokkenen, over wie gegevens worden verwerkt, een duidelijk beeld krijgen van de verwerking van hun gegevens. Krachtens artikel 6.3 van de AVG, gelezen in samenhang met artikel 22 van de Grondwet en artikel 8 van het EVRM, moet dergelijke wettelijke norm de essentiële elementen van de met de overheidsinmenging gepaard gaande verwerkingen beschrijven. Het gaat hierbij minstens om:
    - het (de) precieze en concrete doeleinde(n) van de gegevensverwerkingen;
    - de aanduiding van de verwerkingsverantwoordelijke(n) (tenzij dit duidelijk is).

    Voor zover de met de overheidsinmenging gepaard gaande verwerkingen van persoonsgegevens een belangrijke inmenging in de rechten en vrijheden van de betrokkenen vertegenwoordigen, omvat de wettelijke bepaling terzake tevens volgende (aanvullende) essentiële elementen:
    - de (categorieën van) verwerkte persoonsgegevens die terzake dienend en niet overmatig zijn;
    - de categorieën van betrokkenen wiens persoonsgegevens worden verwerkt;
    - de (categorieën van) bestemmelingen van de persoonsgegevens, evenals de omstandigheden waarin en de redenen waarom de gegevens worden verstrekt;
    - de maximale bewaartermijn van de geregistreerde persoonsgegevens.
    - de eventuele beperking van de verplichtingen en/of rechten vermeld in de artikelen 5, 12 tot 22 en 34 AVG

- Toepassing van deze principes

[6] Zie voetnoot 1.

25. Terzake is de Autoriteit van oordeel dat gelet op doeleinden van de verwerking en de te verwerken categorieën van persoonsgegevens er sprake is van een belangrijke inmenging in de rechten en vrijheden van de betrokkenen. Het betreft immers *in se* een verwerking op grote schaal die (minstens in secundaire orde) plaatsvindt voor toezichts- of controledoeleinden en die (weliswaar onder bepaalde voorwaarden) ruim toegankelijk zijn voor derden. Dit impliceert dat alle essentiële elementen vastgesteld moeten worden in een formele wettelijke norm, en dat enkel verdere (technische) details en modaliteiten door uitvoeringsbepalingen kunnen worden uitgewerkt, mits daartoe een voldoende nauwkeurige delegatie aan de Koning voorhanden is.

26. Zoals hierboven reeds toegelicht betreft het ter advies voorgelegde voorontwerp **de tenuitvoerlegging** van de artikelen 19bis-1 tot 19bis-3, 19bis-6 en 19bis-8 WAM waarover de Autoriteit zich reeds heeft uitgesproken. Waar relevant (en noodzakelijk) zal de Autoriteit met betrekking tot wezenlijke elementen van de verwerking aldus terugkoppelen naar de bepalingen uit de basiswet, het voormelde advies nr. 29/2022 en het ontwerp. Er weze aan herinnerd dat onderhevig advies geen nieuwe beoordeling vormt omtrent de bepalingen uit de WAM.

c. Doeleinden

27. Volgens artikel 5.1.b) AVG kan de verwerking van persoonsgegevens enkel uitgevoerd worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.

28. De doeleinden worden in artikel 19bis-8 WAM uiteengezet. De Autoriteit onderscheidt per paragraaf volgende doeleinde:

- Ten aanzien van de eerste paragraaf volgt dat de verwerking van persoonsgegevens binnen dit kader noodzakelijk is voor de afwikkeling (schadevergoeding) van de bij een ongeval betrokken personen.
- Ten aanzien van de tweede paragraaf volgt de noodzaak van verwerking van persoonsgegevens uit het oogmerk van controle en onderzoek.
- Ten aanzien van het derde paragraaf kunnen drie doeleinden onderscheiden worden die gezamenlijk opgenomen worden in het koepel van bewijsdoeleinde:
    i. vergoeding van geleden schade ontvangen;
    ii. vaststelling van de staat van verzekering; en
    iii. raadpleging van een internationale verzekeringskaart voor motorrijtuigen.

29. Binnen dit kader beoogt het voorontwerp de nadere regels inzake: *i) verzoeken om inlichtingen; ii) de modaliteiten met betrekking tot de toegang tot het register; iii) en de vorm en de inhoud*

van de aanvraag tot het bekomen van de informatie vast te stellen. De Autoriteit neemt hiervan akte.

d. Verwerkingsverantwoordelijke

30. Overeenkomstig artikel 4.7) AVG is de verwerkingsverantwoordelijke elke natuurlijke of rechtspersoon, overheidsinstantie, dienst of ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen. Volledigheidshalve brengt de Autoriteit in herinnering dat de aanduiding van de verwerkingsverantwoordelijke passend moet zijn in het licht van de feitelijke omstandigheden. Zowel de Werkgroep Artikel 29 – voorganger van het Europees Comité voor gegevensbescherming – als de Autoriteit hebben aangedrongen op de noodzaak om deze concepten te benaderen vanuit een feitelijk perspectief. Het is derhalve noodzakelijk de entiteit of entiteiten aan te wijzen die in feite het doel van de verwerking nastreven en de controle erover uitoefenen.

31. Hoewel het voorontwerp zelf geen melding maakt van de verwerkingsverantwoordelijke, geeft deze uitvoering aan de wettelijke bepalingen uit de WAM, waar de verwerkingsverantwoordelijke expliciet vermeld wordt in artikel 16bis-6, §4 WAM. De Autoriteit **neemt er akte** van.

e. Minimale gegevensverwerking/ Proportionaliteit

32. Artikel 5.1.c), AVG bepaalt dat persoonsgegevens toereikend, terzake dienend en beperkt moeten zijn tot wat noodzakelijk is voor de beoogde doeleinden (principe van 'minimale gegevensverwerking').

33. Preliminair acht de Autoriteit het noodzakelijk om verdere duiding te geven rond een ambiguïteit die uit het voorontwerp vloeit, aangaande hetgeen volgens de aanvrager bijgehouden moet worden. Uit de analyse van alle documenten rijst de indruk dat de aanvrager niet de intentie heeft om 'alle gegevens m.b.t. een raadpleging onder artikel 11, van het voorontwerp,' bij te houden. De Autoriteit wijst erop dat aangezien het ook persoonlijke gegevens betreft, deze ergo als dusdanig behandeld moeten worden. In dat verband lijkt het nuttig om de aanvrager eraan te herinneren dat krachtens de bepalingen van de AVG rond passende beveiligingsmaatregelen[7] en het register van verwerkingsactiviteiten[8], de verwerkingsverantwoordelijke, *a fortiori* genoodzaakt

[7] Artikel 32 AVG.

[8] Artikel 30 AVG.

zal zijn om logs bij te houden zodat toepassing gegeven kan worden aan de beginselen van transparantie en accountability. Hieruit volgt redelijkerwijs dat ook de gegevens die onder artikel 11 van het voorontwerp vallen, gelogd zullen moeten worden. Met andere woorden, de gegevens van de ontvangers van informatie of van de verzekeringsstatus, zullen bijgehouden moeten worden door de verwerkingsverantwoordelijke.

34. Tegen deze achtergrond, zal de Autoriteit, gelet op de aard van de norm, *i.e.*, het voorontwerp, voor de toetsing van de essentiële elementen van dit onderdeel teruggrijpen naar artikel 19bis-8 WAM en in het licht hiervan artikel 11, van het voorontwerp, die artikel 14 van het KB van 11 juli 2003 vervangt, beoordelen. Rekening houdend met de onderscheiden doeleinden en de verschillende categorieën van personen, zal de Autoriteit per paragraaf haar beoordeling toelichten.

35. Ten aanzien van de eerste paragraaf, namelijk artikel 19bis-8, §1 WAM:

36. Deze geeft duidelijk en expliciet weer welke categorieën van betrokkenen een verzoek om inlichtingen kunnen instellen. Daarnaast wordt ook duidelijk aangegeven over wie – "*ieder bij het ongeval betrokken motorrijtuig*" – inlichtingen verkregen kunnen worden. In het licht hiervan bevestigt de Autoriteit dat **de categorieën van betrokkenen die beoogd worden duidelijk en nauwkeurig weergeven** worden in de formele wettelijke norm. Wat **de categorieën van persoonsgegevens** betreft, stelt de Autoriteit vast dat de wettelijke formele norm, exhaustief en expliciet aangeeft welke gegevens **verkregen** kunnen worden **betreffende ieder bij het ongeval betrokken** motorrijtuig. Artikel 11, van het voorontwerp, werkt de vorm en inhoud van het verzoek om inlichtingen als volgt uit:

"Art. 11. Artikel 14 van hetzelfde besluit wordt vervangen als volgt:

Art. 14. § 1. Elke aanvraag tot kennisneming van een van de elementen bedoeld bij artikel 19bis-8, § 1, van de wet geschiedt bij eenvoudige zending, gericht aan het Fonds of door ieder elektronisch middel dat door het Fonds ter beschikking van de aanvrager wordt gesteld.

De aanvraag tot kennisneming** van een van de elementen bedoeld bij artikel 19bis-8, § 1, van de wet**, bevat de naam en het adres van de aanvrager, de datum van de aanvraag en het ongeval, het land van het ongeval en de nummerplaat van het bij de aanvraag betrokken motorrijtuigen.

De datum van de zending of de systeemdatum is rechtsgeldig.

Het Fonds moet de gevraagde inlichtingen zo spoedig mogelijk meedelen door middel van een gewone zending of om het even welk elektronisch communicatiemiddel. […]"

37. In het licht van de context waarin een verzoek om inlichtingen kan worden gedaan, acht de Autoriteit het aanvaardbaar dat de te verwerken persoonsgegevens van de verzoeker[9] pas in een uitvoeringsbesluit worden vastgesteld.

38. Onverminderd de reeds aangekaarte aanbeveling om gebruik te maken van 'een sterk authenticatiemiddel[10] en de bemerking uit punt 33, is de Autoriteit van mening dat de eerste paragraaf – artikel 19bis-8, §1 WAM en het eerste paragraaf van artikel 11, van het voorontwerp – geen aanleiding geeft tot bijzondere opmerkingen betreffende de proportionaliteit van de onderliggende gegevensverwerkingen.

39. Ten aanzien van de tweede paragraaf, stelt de Autoriteit vast dat de formele wettelijke norm – m.n. artikel 19bis-8, §2 WAM – een onderscheid maakt tussen twee scenario's die nauwkeurig, expliciet en duidelijk aangeven welke categorieën van betrokkenen onder de toepassing van enigerlei scenario's ressorteren. Het gaat om de controle van verzekeringssituaties van een bepaald voertuig, enerzijds, en om het uitvoeren van preventie, controle- en onderzoeksmissies, anderzijds.

40. Het verschil betreft de toegang tot het aantal gegevens. In de eerste situatie gaat het niet verder dan aangeven of het voertuig 'verzekerd' is of de verzekeringsstatus 'onbekend' is. In de tweede situatie, wordt naargelang de wettelijke opdrachten toegang verleend tot de relevante gegevens uit het register van artikel 19bis-6 WAM. In dat verband verwijst de Autoriteit naar advies nr. 29/2022, waarbij met het oog op de bescherming van de rechten en vrijheden van de betrokkenen, de aandacht op de technische en organisatorische maatregelen werd gevestigd.[11] In navolging hiervan voorziet artikel 11, van het voorontwerp, de modaliteiten m.b.t. de toegang, zoals hiernavolgend weergeven:

"[…] § 2. Het Fonds verleent de personen bedoel in artikel 19bis-8, § 2, van de wet een ***beveiligde toegang met een sterke authenticatie*** *tot het register bedoeld in artikel 19bis-6 van de wet. De autoriteiten implementeren een informaticasysteem met beveiligde toegang dat door het Fonds ter beschikking wordt gesteld.*

Deze integratie volgt ***sterke beveiligingsregels, namelijk versleuteling, IPwhitelisting en het gebruik van een token.***

[9] Of **ontvanger** van informatiegegevens.

[10] Zie voetnoot 1.

[11] Zie advies nr. 29/2022, randnr. 32.

De identiteit van de leden die het register raadplegen, wordt door elke autoriteit geregistreerd.

De toegang van de personen bedoeld in artikel 19bis-8, § 2, is beperkt tot de doeleinden en de leden bedoeld in artikel 19bis-8, § 2, voor het uitvoeren van hun opdracht. De autoriteiten waken erover dat hun leden die toegang hebben tot het register, die verplichting naleven. Ze organiseren de ***controle op het gebruik van de gegevens, de nodige logboeken en audits.***

Een bijgewerkte lijst van personen die toegang hebben tot het register, met vermelding van hun hoedanigheid, wordt opgesteld door elke autoriteit en ter beschikking gesteld van de Gegevensbeschermingsautoriteit.

De toegang bedoeld in artikel 19bis-8, § 2, eerste lid, laat een raadpleging toe in real time, permanent en op afstand.

Wat betreft de informatie bedoeld in artikel 19bis-8, § 2, derde lid, moet het Fonds de gevraagde gegevens zo spoedig mogelijk meedelen door middel van een gewone zending of om het even welk elektronisch communicatiemiddel. […]"

41. Vooreerst wijst de Autoriteit erop dat "*het gebruik van een token*," in praktijk heel veel technologieën kan afdekken en daarom als een vage term beschouwd wordt door technici. Vroeger betekende dit een extern hardware device (https://en.wikipedia.org/wiki/Security_token). Nu kan dit echter niet alleen in software geïmplementeerd worden op een smartphone, maar ook een JSON Web token zijn, wat eigenlijk een voorstelling is in een bitstring van een security claim. In het licht hiervan vraagt de Autoriteit om de term "token" te vermijden in het ontwerp.

42. De volgende technische en organisatorische maatregelen worden vastgesteld: *i) beveiligde toegang met een sterke authenticatie; ii) beveiligingsregels – versleuteling; IPwhitelisting en het gebruik van een token*[12]*; iii) registratie van identiteit bij raadpleging van het register; iv) controle op het gebruik van gegevens; v) logboeken; vi) audits; vii) bijgewerkte lijst van personen die toegang hebben tot het register*.

43. In aanmerking genomen dat een controle van de verzekeringssituatie geen rechtstreeks toegang verschaft tot de gegevens van het register uit artikel 19bis-6 WAM, maar beperkt is tot de

[12] De Autoriteit verwijst naar randnr. 32 van onderhevig advies, m.b.t. het vermijden van het gebruik van de term 'token'.

verzekeringsstatus zijnde 'verzekerd' of 'onbekend', vermoedt de Autoriteit dat de opgesomde technische en organisatorische maatregelen niet beoogd zijn voor de eerste situatie. In het licht van eerder besproken punten 15-22 betreffende de sterke authenticatie, vraagt de Autoriteit om de nodige aanpassingen in te voeren, zodat ook voor de ontvangers, van een binair antwoord over de verzekeringsstatus van een motorrijtuig, het gebruik van een sterk authenticatiemiddel opgelegd wordt.[13]

44. Wat de tweede situatie betreft, zijnde het uitvoeren van preventie, controle- en onderzoeksmissies, meent de Autoriteit dat door de invoering van voormelde technische en organisatorische maatregelen in het voorontwerp, gehoor wordt gegeven aan de aanbevelingen uit het eerdere advies.[14] De Autoriteit neemt hier akte.

45. Ten aanzien van de derde paragraaf, zijnde artikel 19bis-8, §3 WAM:

46. Acht de Autoriteit dat de categorieën van personen die een aanvraag tot het bekomen van informatie, duidelijk beschreven zijn in de formele wetgevende norm, *i.e.*, artikel 19bis-8, §3, lid 1 WAM. Wat de categorieën van persoonsgegevens betreft, volgt uit voormelde bepaling dat er geen toegang is tot (gegevens van) het register uit artikel 19bis-6 WAM. De verschaffing van informatie aan een aanvrager (ontvanger) is beperkt "*tot het bekomen van de bevestiging dat het Fonds al dan niet in het bezit is van gegevens tot bewijs van het bestaan van de verzekeringsovereenkomst.*"[15] In uitvoering hiervan werd in artikel 11, van het voorontwerp, een delegatie aan de Koning voorzien, ter bepaling van de vorm en inhoud van de aanvraag, zoals hierna weergeven:

> "[…] *§ 3. De informatieaanvraag bedoeld in artikel 19bis-8, § 3, van de wet wordt ingediend door het elektronisch middel dat door het Fonds ter beschikking wordt gesteld.*
>
> *De raadpleging van de verzekeringsstatus op de website wordt beschermd door een validatiecode die garandeert dat deze niet door een computerprogramma wordt geïnitieerd.*
>
> *De aanvrager moet:*
>
> *1° bevestigen dat zijn aanvraag gerechtvaardigd is door ten minste een van de volgende hoedanigheden:*
>
> *a) benadeelde of een persoon die in naam van die persoon optreedt;*
> *b) eigenaar van het voertuig of een persoon die in naam daarvan optreedt;*

[13] Zie voetnoot 1.

[14] Zie hiervoor advies 29/2022, randnr. 32.

[15] In overeenstemming met advies 29/2022, randnr. 24.

c) bestuurder van het voertuig of een persoon die in naam daarvan optreedt;
d) de houder van het voertuig of een persoon die in naam daarvan optreedt;
e) een natuurlijk persoon of rechtspersoon die door de wet, een decreet of een beschikking gemachtigd is om naar het verzekeringsbewijs te vragen, met uitzondering van de personen bedoeld in artikel 19bis- 8, § 2;

2° kennisnemen van het feit dat hij, bij gebrek aan gerechtvaardigd belang, op ongeoorloofde wijze over de informatie beschikt;

3° verklaren dat hij de verstrekte informatie niet zal gebruiken voor doeleinden die geen verband houden met de in zijn aanvraag aangehaalde reden;

4° bevestigen dat hij kennis heeft genomen van de vertrouwelijkheidsverklaring inzake de gegevensbescherming.

De opzoeking gebeurt op basis van het kentekenplaat of het chassisnummer.

De aanvraag preciseert de datum voor dewelke de informatie wordt gevraagd. Deze datum mag niet meer dan zes maanden voorafgaan aan de datum van de aanvraag.

De toegang bedoeld in artikel 19bis-8, § 3, laat een raadpleging toe in real time, permanent en op afstand."

47. Dat de categorieën van personen die een informatieaanvraag kunnen indienen duidelijk blijkt uit de formele wetgevende norm, werd in punt 46 al bevestigd. Hoewel er in eerder advies op gewezen is geweest dat gegevens over identiteit en hoedanigheid verzameld moeten worden, **wordt noch in de formele wetgevende norm, noch in het voorontwerp <u>expliciet</u> aangegeven welke categorieën van persoonsgegevens vereist zijn in dergelijke aanvraag**.[16] Er kan aangenomen worden dat om een hoedanigheid of identiteit aan te tonen, minstens naam, voornaam en idealiter Rijksregisternummer[17] bekend moeten zijn. De Autoriteit vraagt om deze lacune aan te vullen en in de mate van het mogelijke de vereiste informatie te beperken tot hetgeen onder de eerste paragraaf van artikel 11 van het voorontwerp ressorteert. De Autoriteit wijst erop dat hier vanzelfsprekend aan wordt voldaan door gebruik te maken van de aanbevolen sterke authenticatie, zoals eerder toegelicht in punten 15-22.[18]

[16] Zie advies 29/2022, randnr. 30.

[17] De Autoriteit wijst erop dat elk gebruik van het Rijksregister onderworpen is aan de bepalingen uit de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en m.n. artikels 5 en 8, die redelijkerwijs ook vermeld moeten zijn in de beoogde norm.

[18] Zie voetnoot 1.

48. Zoals eerder gesteld in advies nr. 29/2022, betreft hetgeen onder artikel 19bis-8, §3 WAM een nieuwe gegevensverwerking met een algemeen doel die als bewijsvoering gecategoriseerd kan worden. In dat verband stelt de Autoriteit, overeenkomstig eerder advies, vast dat een voertuig enkel aan het verkeer mag deelnemen indien de bestuurder het bewijs van verzekeringsovereenkomst kan afleveren. In eerder advies werd reeds aangekaart dat een vrijstelling van verzekeraars om een internationaal verzekeringsbewijs af te geven een risico kan vormen voor de bewegingsvrijheid van verzekeringsnemers.[19] De Autoriteit observeert dat de uitvoeringsmaatregelen voorzien in het ontwerp, beantwoorden aan de aanbevelingen uit eerder advies en geacht worden voldoende te zijn om het hoofd te bieden aan potentiële risico's voor de rechten en vrijheden van verzekeringsnemers.[20]

f. Bewaartermijn

49. Krachtens artikel 5.1.e) AVG mogen persoonsgegevens niet langer worden bewaard, in een vorm die het mogelijk maakt de betrokkenen te identificeren, dan noodzakelijk voor de verwezenlijking van de doeleinden waarvoor zij worden verwerkt.

50. Voor de bewaartermijn wijst de Autoriteit op het onderscheid van gegevens uit het register, zoals bepaald in artikel 19bis-6, §2 WAM en de gegevens die verwerkt moeten worden krachtens artikel 19bis-8 WAM en het voorontwerp, dat hieraan uitvoering geeft. In het formulier voor de aanvraag van advies van dit voorontwerp, wordt het volgende gesteld:

> " - *voor het register is dit voorzien in de basiswet, art. 19bis-6, §2...*
> *- in het kader van artikel 11 van het voorontwerp van decreet lijkt het ons dat de* ***raadplegingsgegevens***[21] *niet kunnen worden bewaard, zoals uitgelegd in de preambule cf. ook overweging 18 van richtlijn 2021/2118 van het Europees Parlement en de Raad van 24 november 2021 tot wijziging van richtlijn 2009/103/EG. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32021L2118*"[22]

51. Er wordt terecht verwezen naar artikel 19bis-6, §2 WAM, die aangeeft **dat de gegevens uit het register** niet langer dan 7 jaar na het verstrijken van de inschrijving van het voertuig of van de verzekeringsovereenkomst mogen worden bewaard.

---

[19] Zie advies 29/2022 randnr. 19.

[20] Zie advies 29/2022, randnrs. 16-25.

[21] Vet toegevoegd door Autoriteit.

[22] Vertaling door Autoriteit.

52. Wat artikel 11, van het voorontwerp, betreft die samengelezen wordt met 19bis-8 WAM komt de Autoriteit tot een afwijkende standpunt dan dit van de aanvrager van het voorontwerp. Uit een contextuele analyse van voorgaande passage, het voorwoord van het voorontwerp[23] en de verwijzing naar de richtlijn[24] concludeert de Autoriteit – zoals eerder toegelicht in punten 17-18 – dat de aanvrager bij de beoordeling over de verwerking van (persoons)gegevens, enkel de verzekeringsstatus van de (on)verzekerde, die een binair antwoord omvat – 'verzekerd' of 'onbepaald' – in aanmerking genomen heeft. Onverlet de aanbeveling op het gebruik van een sterk authenticatiemiddel, hoort bij die beoordeling ook de verwerking van persoonsgegevens van andere partijen – zijnde ontvangers die naar de verzekeringsstatus of informatie uit het register vragen.[25] Het gaat *in casu* om de *gegevens betreffende aanvragen tot kennisneming van een element bedoeld bij artikel 19bis, §1 WAM, de logboeken en registratie van de identiteit van de leden die het register raadplegen, maar ook de gegevens van de informatieaanvragen onder het onderdeel 14,§3 in artikel 11, van het voorontwerp*. De meerwaarde van een bepaling waar dergelijke gegevens worden vereist van de ontvangers en vervolgens onmiddellijk gewist worden, wordt in vraag gesteld. Overigens lijkt de ratio om dergelijke gegevens, in de eerste plaats, te vragen onverenigbaar met het opzet om deze niet te bewaren. Bovendien wordt, zoals toegelicht in punt 33, aangenomen dat de verwerkingsverantwoordelijke minstens logs zal bijhouden. In acht genomen dat het gebruik van een sterk authenticatiemiddel aan de orde is, komt de Autoriteit tot het besluit dat binnen het kader van artikel 11 van het voorontwerp, hoe dan ook gegevens bewaard zullen moeten worden.[26]

53. In het licht hiervan vraagt de Autoriteit om in de basiswet, ook voor deze gegevens een maximum bewaartermijn te voorzien.

---

[23] Het voorontwerp stipuleert o.m. het volgende: "*Overwegende dat het gebruik van een kenteken of chassisnummer een verwerking van persoonsgegevens vormt wanneer het kenteken het mogelijk maakt een natuurlijke persoon te identificeren, **wat niet het geval is wanneer de site een antwoord genereert over de verzekeringsstatus**, aangezien er geen persoonsgegevens worden doorgegeven aangezien de eigenaar, de verzekeringnemer of de verzekeraar niet kunnen worden geïdentificeerd; **Overwegende dat wanneer de specifieke website wordt geraadpleegd en "verzekerd" wordt vermeld**, geen details over het verzekeringscontract zoals verzekeraar, polisnummer of verzekeringsnemer worden meegedeeld om redenen van privacy; **Overwegende dat de mededeling van de verzekeringsstatus, zonder** vermelding van de identiteit van de eigenaar van het voertuig, de verzekeraar of het polisnummer, geen hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen*.".

[24] VW.18 richtlijn nr. 2021/2118, 24 november 2021 tot wijziging van Richtlijn 2009/103/EG betreffende de verzekering tegen de wettelijke aansprakelijkheid waartoe de deelneming aan het verkeer van motorrijtuigen aanleiding kan gevenen de controle op de verzekering tegen deze aansprakelijkheid, *Pb.L.* 02 december 2021, afl 430, 1: "*In overeenstemming met die beginselen mogen de lidstaten de persoonsgegevens **die uitsluitend verwerkt zijn met het doel een verzekeringscontrole** te verrichten, niet langer bewaren dan nodig is om na te gaan of een voertuig geldig verzekerd is. Wanneer blijkt dat een voertuig gedekt is, moeten alle gegevens met betrekking tot die controle worden gewist. Wanneer een controlesysteem niet in staat is vast te stellen of een voertuig verzekerd is, moeten die gegevens slechts worden bewaard gedurende een beperkte periode die maximaal het aantal dagen bedraagt dat nodig is om vast te stellen of er al dan niet sprake is van een geldige verzekeringsdekking. Voor voertuigen waarvan is vastgesteld dat zij niet gedekt zijn door een geldige verzekeringspolis, is het redelijk te eisen dat dergelijke gegevens worden bewaard totdat de administratieve of gerechtelijke procedures zijn voltooid en het voertuig door een geldige verzekeringspolis is gedekt*." (vet toegevoegd door Autoriteit).

De verwijzing die in dit verband gemaakt is geweest betreft enkel de gegevens met betrekking tot een verzekeringscontrole.

[25] Zie hiervoor advies 29/2022, randnr. 15 en randnr. 30.

[26] Zie voetnoot 1.

OM DEZE REDENEN,
de Autoriteit,

is van oordeel dat de volgende wijzigingen aan het voorontwerp zich opdringen:

- hantering van een sterke authenticatiemiddel voor elke (on)rechtstreekse toegang tot het register zoals bedoeld in artikel 19bis-6 WAM (punten 15-22, 43,47);
- vervanging van de term 'token' (punt 41);
- nadere omschrijving van de categorieën van persoonsgegevens, waarbij ervoor moet worden gezorgd dat alleen de categorieën gegevens worden vermeld die strikt noodzakelijk en relevant zijn voor het beoogde doel (punt 52);
- maximale bewaartermijn specifiëren voor persoonsgegevens van de ontvangers van informatie of verzekeringsstatus (punt 52-53).

Voor het Kenniscentrum,
(get.) Cédrine Morlière, Directeur