



Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 35/2025 van 19 mei 2025

Betreft: een voorontwerp van wet *tot herstel van artikel 31bis van de wetten op de Raad van State, gecoördineerd op 12 januari 1973, met betrekking tot de elektronische procesvoering voor de afdeling bestuursrechtspraak van de Raad van State* (CO-A-2025-024)

Trefwoorden: gedifferentieerde bewaartermijn – logs – logging – verbinding – loggegevens – Breyer – Digital Platform for Attorneys (DPA) – term verbinding – specificeren van betrokkenen en correleren met functionele opdracht

Originele versie

Introductie:

Het advies betreft de artikelen 1 tot en met 4 van een voorontwerp van wet tot herstel van artikel 31bis van de wetten op de Raad van State, gecoördineerd op 12 januari 1973, met betrekking tot de elektronische procesvoering voor de afdeling bestuursrechtspraak van de Raad van State.

Het voorontwerp strekt ertoe artikel 31bis van de gecoördineerd wetten op de Raad van State te herstellen m.h.o. de invoering van een rechtsgrond voor het creëren van een elektronisch platform en de samenhangende gegevensverwerkingen die daaruit voortvloeien.

De Autoriteit formuleert in het bijzonder opmerkingen met betrekking tot de maximale bewaartermijn, van de in het Ontwerp diverse opgesomde soorten gegevens. Tevens wordt aandacht vereist voor enkele aspecten onder de minimale gegevensverwerking die enerzijds geringe aanpassingen vereisen en anderzijds fundamenteel in vraag worden gesteld.

Voor de volledige lijst van opmerkingen wordt verwezen naar het [dispositief](#).

De Autorisatie- en Adviesdienst van de Gegevensbeschermingsautoriteit (hierna de "Autoriteit");

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

Gelet op 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 de adviesaanvraag van de heer Bernard Quintin, minister van Veiligheid en Binnenlandse Zaken, belast met Beliris (hierna "de aanvrager"), ontvangen op 24 maart 2025;

Gelet op de aanvullende inhoudelijke toelichtingen, ontvangen op 16 april 2025;

Brengt op 19 mei 2025 het volgende advies uit:

I. VOORWERP VAN DE ADVIESAANVRAAG

1. Op 24 maart 2025 verzocht de aanvrager het advies van de Autoriteit met betrekking tot een voorontwerp van wet tot herstel van artikel 31bis van de wetten op de Raad van State, gecoördineerd op 12 januari 1973 met betrekking tot de elektronische procesvoering voor de afdeling bestuursrechtspraak van de Raad van State (hierna: het Ontwerp).
2. Het Ontwerp beoogt het herstel van artikel 31bis van de gecoördineerde wetten op de Raad van State en biedt een uitdrukkelijke rechtsgrond voor de oprichting en het gebruik van een elektronisch platform die aan de Raad van State de mogelijkheid biedt om beroepen die voor hen worden gebracht elektronisch te beheren en aldus hun opdracht van openbaar belang uit te oefenen die hen bij artikel 160 van de Grondwet is toevertrouwd.
3. De Autoriteit noteert – op basis van bijkomende uitleg van de aanvrager – dat het voornemen bestaat om artikel 85bis van het besluit van de Regent van 23 augustus 1948 tot regeling van de rechtspleging voor de afdeling bestuursrechtspraak van de Raad van State (hierna: Procedurereglement van de Raad van State), dat de werking van de elektronische procedure

regelt, te vervangen. De Autoriteit herinnert eraan dat zij, gelet op artikel 46, §1 van het reglement van interne orde van de Gegevensbeschermingsautoriteit, uitsluitend normatieve ontwerpen onderzoekt die zich in hun finale ontwerpfasen bevinden, d.w.z. nadat ze zijn goedgekeurd door de regering van de betrokken gefedereerde entiteit of door de ministerraad, voor zover een dergelijke goedkeuring vereist is. In het licht hiervan, kan de Autoriteit – hoewel mogelijke toekomstige aanpassingen in aanmerking genomen werden, *i.e.*, definities, zie *infra*. – zich in de beoordeling van het onderliggend advies, niet inhoudelijk uitspreken over het nieuwe ontwerp van koninklijk besluit tot wijziging van de elektronische procesvoering voor de afdeling bestuursrechtspraak van de Raad van State, waarvan tot op heden nog geen adviesaanvraag van geweest is.

II. ONDERZOEK TEN GRONDE

a. Rechtsgrond

4. *Herhaling van de principes*: 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.¹ De lezer wordt verwezen naar de toepassing van deze principes zoals hierna beschreven.
5. Een 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 (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,

¹ Artikel 6, lid 1, van de AVG: "*De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan: (...)*

c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust; (...)

e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen; (...)."

omvat de wettelijke bepaling, overeenkomstig het legaliteits- en het voorzienbaarheidsprincipe, terzake tevens volgende (aanvullende) essentiële elementen:²

- de (categorieën van) verwerkte persoonsgegevens die ter zake dienend en niet overmatig zijn;
- de categorieën van betrokkenen wiens persoonsgegevens worden verwerkt;
- de (categorieën van) bestemmingen 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.

6. *Concrete toepassing:* de verwerking van persoonsgegevens waartoe het voor advies voorliggende Ontwerp aanleiding geeft, berust op artikel 6(1)(e) AVG.³ In overweging genomen dat het Ontwerp de verwerking van persoonsgegevens met zich meebrengt die: *i) betrekking heeft op speciale categorieën van persoonsgegevens (gevoelige gegevens) in de zin van de artikelen 9 en/of 10 van de AVG en/of hoogst persoonlijke gegevens; ii) plaats vindt voor toezichts- of controledoeleinden⁴; iii) waarbij de gegevens meegedeeld of toegankelijk gemaakt worden voor derden⁵; iv) voorziet in het gebruik van het rijksregisternummer*, is de Autoriteit van oordeel, dat het, **in casu, om een belangrijke inmenging gaat.**

7. Hierna gaat de Autoriteit na in hoeverre het Ontwerp aan deze voorwaarden beantwoordt.

b. Doeleinden

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

9. In dit verband stipuleert ontworpen artikel 31bis, §1, lid 1: "*De Raad van State creëert en beheert een elektronisch platform dat hij ter beschikking stelt van de partijen voor het instellen en het beheren van de geschillenprocedures die voor hem worden gebracht.*" Gelezen in samenhang met artikel 85bis van het Procedurereglement van de Raad van State, vallen hier verschillende handelingen onder. Hieromtrent lichtte de aanvrager verder toe dat:

² Zie DEGRAVE, E., "*L'égouvernement et la protection de la vie privée – Légalité, transparence et contrôle*", Collection du CRIDS, Larcier, Brussel, 2014, p. 161 e.v. (zie o.m.: EHRM, arrest *Rotaru c. Roumania*, 4 mei 2000); Zie ook enkele arresten van het Grondwettelijk Hof: Arrest nr. 44/2015 van 23 april 2015 (p. 63), Arrest nr. 108/2017 van 5 oktober 2017 (p. 17) en Arrest nr. 29/2018 van 15 maart 2018 (p. 26).

³ Artikel 6(1)(e) AVG: "*de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.*"

⁴ Loggegevens.

⁵ Rekening houdend met de bepalingen uit het ontwerp van koninklijk besluit tot wijziging van de elektronische procesvoering voor de afdeling bestuursrechtspraak van de Raad van State dat zowel nog aan het advies van de Autoriteit moet onderworpen worden als gestemd moet worden.

« Comme indiqué à l'article 31*bis*, alinéa 3, l'introduction et la gestion des procédures contentieuses portées devant le Conseil d'État implique le dépôt, par les parties au litige, de différents actes de procédure accompagnés, le cas échéant, de pièces qui y sont annexées.

Ces actes de procédure varient en fonction des procédures et du déroulement de celles-ci et il est donc complexe d'en dresser une liste complète. Ces actes sont toutefois mentionnés dans les lois coordonnées sur le Conseil d'État ainsi que dans les divers arrêtés royaux qui déterminent les procédures applicables devant le Conseil d'État (principalement : le règlement général de procédure, l'arrêté royal du 19 novembre 2024 déterminant la procédure en référé [...], ainsi que l'arrêté royal du 30 novembre 2006 déterminant la procédure en cassation devant le Conseil d'État).

À titre d'exemple nous pouvons toutefois détailler les actes de procédure déposés par les parties à l'occasion d'une procédure en annulation « classique » (sans incidents de procédure et sans mise en œuvre d'une procédure abrégée) :

- 1) La partie requérante dépose une requête en annulation.
- 2) La partie adverse prend connaissance de la requête en annulation, dépose le dossier administratif lié à l'acte attaqué ainsi qu'un mémoire en réponse.
- 3) La partie requérante prend connaissance du mémoire en réponse et dépose un mémoire en réplique.
- 4) L'auditeur désigné dépose un rapport sur le recours en annulation.
- 5) La partie à laquelle le rapport de l'auditeur donne tort prend connaissance de celui-ci et dépose une demande de poursuite de la procédure ainsi qu'un dernier mémoire.
- 6) La partie à laquelle le rapport de l'auditeur donne raison prend connaissance du rapport de l'auditeur et du dernier mémoire de l'autre partie au litige. Elle dépose à son tour un dernier mémoire.

Si une partie, autre que la partie requérante ou la partie adverse, souhaite intervenir en cours de procédure, elle doit le faire au moyen d'une requête en intervention. Si l'intervention est accueillie, la partie intervenante déposera également un dernier mémoire.

D'autres actes de procédure peuvent être communiqués par les parties. Il s'agit par exemple d'un désistement d'instance, d'un retrait de l'acte administratif attaqué, ou encore de notes de plaidoirie déposées à l'audience.

Ces différents actes de procédure peuvent être accompagnés de pièces annexées par les parties. Contrairement aux actes de procédure, qui sont limitativement énumérés et définis par les lois coordonnées et ses arrêtés d'exécutions mentionnés ci-dessus, la nature des pièces annexées n'est pas définie. Celles-ci varient donc d'une affaire à l'autre en fonction, notamment, de la nature du litige soumis au Conseil d'État.

Ces différents actes et pièces déposés par les parties forment – avec les avis, communications et convocations déposés par le Conseil d'État à l'intention des parties – le dossier électronique de l'affaire tel que défini à l'article 85*bis*, § 2, 2°, nouveau du règlement général de procédure. »

10. Concreet onderstelt de Autoriteit dat het beoogde elektrische platform zal dienen voor kennisgevingen, mededelingen, en neerleggingen (van verzoekschriften, conclusies, memories en stukken, alsook de daarbij begeleidende brieven). Het dossier op het elektronisch platform zal – zoals beschreven door de aanvrager – bestaan uit de door de partijen ingediende voormelde

elementen en de adviezen, communicatie en oproepingen van de Raad van State aan de partijen toe.⁶ De Autoriteit neemt hier akte van.

11. Daarnaast wordt in de Memorie van Toelichting verduidelijkt dat er: "[...] [m]et die gegevensverwerking [...] **geen andere doeleinden** [worden] **nagestreefd** dan het geval is met een beroep dat via de "papieren" procedure wordt ingesteld en behandeld. De Raad van State **verwerkt die gegevens uitsluitend met het oog op het beheer van de beroepen, de vrijwaring van de belangen van de partijen en de voorzienbaarheid en eenheid van zijn rechtspraak.**"⁷
12. Het geheel in acht genomen, is de Autoriteit de mening toegedaan dat de doeleinden welbepaald, uitdrukkelijk omschreven en gerechtvaardigd zijn.

c. Minimale gegevensverwerking/ Proportionaliteit

13. 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').
14. In dit verband volgt uit ontworpen artikel 31bis, §1 lid 4 dat de persoonsgegevens betreffende de gebruikers⁸ van het elektronisch platform beperkt zijn tot:
 - het rijksregisternummer;
 - de naam en voornamen;
 - het e-mailadres;
 - het telefoonnummer.
15. Met betrekking tot het rijksregisternummer vestigt de Autoriteit de aandacht van de aanvrager op het feit dat het rijksregisternummer alleen mag worden gebruikt/verwerkt onder de voorwaarden als bepaald in artikel 8 van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de

⁶ Inclusief processtukken en betekeningen krachtens huidig toepasselijk artikel 85bis, §13 van het Procedurereglement van de Raad van State.

⁷ Memorie van Toelichting, ontworpen artikel 31bis, §1, lid 4.

⁸ Op vraag van de Autoriteit werd gespecificeerd dat – met uitzondering van toekomstige geringe verandering – de term 'gebruikers' overeenstemt met de huidige definitie in artikel 85bis, §2, 1° van het Procedurereglement van de Raad van State, m.n. "[v]oor toepassing van dit besluit, verstaat men onder : 1° gebruiker : iedere persoon die tussenkomt in een elektronische procesvoering."

Antwoord aanvrager : « Le terme « utilisateurs » utilisé dans l'article 31bis du projet correspond bien à la définition d'« utilisateur » donnée par l'article 85bis, § 2, 1° du règlement général de procédure.

Cette définition est très légèrement modifiée dans le nouvel article 85bis, § 2, 1°, du règlement général de procédure afin de prendre en compte le nouveau système de gestion des utilisateurs au sein duquel les notions de « titulaire d'enregistrement », de « gestionnaire de dossier », et de « délégué » sont supprimées. »

natuurlijke personen.⁹ **Het verdient de aanbeveling om de rechtsgrond, nl. artikel 8 van voormelde wet, expliciet te vermelden in het Ontwerp.** De Autoriteit herinnert er ook in het algemeen aan dat unieke identificatienummers een bijzondere bescherming genieten. Artikel 87 AVG voorziet dat de lidstaten die een nationaal identificatienummer vaststellen, er moeten over waken dat dit alleen wordt gebruikt met passende waarborgen voor de rechten en vrijheden van de betrokkene. Zo vestigde de Commissie voor de bescherming van de persoonlijke levenssfeer, de rechtsvoorganger van de Autoriteit, reeds eerder¹⁰ de aandacht op in acht name van volgende waarborgen terzake:

- het gebruik van een algemeen identificatienummer moet worden beperkt tot de gevallen waarin dit strikt noodzakelijk is aangezien dit gebruik risico's impliceert inzake koppeling van bestanden;
- de doeleinden moeten duidelijk en expliciet worden gepreciseerd zodat men de beoogde soorten verwerkingen kan vermoeden/voorzien;
- de bewaartermijn en de eventuele mededelingen aan derden moeten eveneens worden omkaderd;
- technische en organisatorische maatregelen moeten het beveiligd gebruik passend omkaderen; en
- de niet-naleving van de bepalingen die het gebruik omkaderen moeten worden gesanctioneerd aan de hand van effectieve, proportionele en ontradende sancties.

16. Voorts is er sprake van "[d]e persoonsgegevens die vervat zijn in de processtukken en stukken die een elektronisch dossier vormen [...]" – waarbij er mogelijk ook verwerkingen kunnen zijn van bijzondere categorieën van persoonsgegevens, vermeld in de artikelen 9.1 (gegevens betreffende religieuze of levensbeschouwelijke overtuigingen, gezondheid,...) en 10 (gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten) van de AVG – hetgeen op het eerste gezicht niet noodzakelijk een belemmering vormt.

17. In de toepasselijke context, met name in het kader van de rechtsbevoegdheid van de Raad van State, is het aannemelijk dat dergelijke processtukken en documenten, gelet op hun aard en functie, verschillende soorten persoonsgegevens, onder meer bijzondere categorieën van persoonsgegevens, zullen bevatten. De aanwezigheid van deze gegevens vloeit voort uit de

⁹ "De machtiging om het rijksregisternummer te gebruiken, wordt door de minister bevoegd voor Binnenlandse Zaken toegekend aan de overheden, instellingen en personen, bedoeld in artikel 5, § 1, wanneer dit gebruik noodzakelijk is voor de uitvoering van taken van algemeen belang.

De machtiging om het rijksregisternummer te gebruiken houdt de verplichting in dit rijksregisternummer eveneens te gebruiken in de contacten met het Rijksregister van de natuurlijke personen.

Er is geen machtiging vereist om het rijksregisternummer te gebruiken wanneer dit gebruik uitdrukkelijk voorzien is door of krachtens een wet, een decreet of een ordonnantie".

¹⁰ Zie advies nr. 19/2018 van 29 februari 2018 betreffende een voorontwerp van wet houdende diverse bepalingen "Binnenlandse Zaken".

noodzaak om de feiten en belangen van partijen correct en volledig te kunnen beoordelen, en is noodzakelijk voor de uitvoering van de opdracht van algemeen belang waarmee de Raad van State als administratief rechtscollege is belast, krachtens artikel 160 van de Grondwet en artikelen 7 tot 17 van de gecoördineerde wetten op de Raad van State. Voor zover de verwerking van deze persoonsgegevens beperkt blijft tot de daarmee samenhangende doeleinden, de uit het Ontwerp voortvloeiende gegevensverwerking eveneens beperkt blijft tot de vooropgestelde doeleinden, en ten minste gepaste waarborgen zoals vertrouwelijkheid en toegangsbeperking worden geïmplementeerd, kunnen de daarmee gepaard gaande risico's adequaat worden ondervangen.

18. Tevens blijkt uit de Memorie van Toelichting bij het ontworpen artikel 31bis, §1, lid 5 dat, wat betreft de categorieën van persoonsgegevens, er ook loggegevens van gebruikers hun activiteiten – *verbinding, precies tijdstip van indiening, precies tijdstip van kennisneming van een ingediend stuk, enz*¹¹ – verwerkt zullen worden. *In casu*, zullen rijksregisternummer, de naam en de voornamen opgehaald worden wanneer de gebruiker zich via het CSAM-systeem van de FOD BOSA authentificeert. In aanmerking genomen dat de in punt 14 vermelde persoonsgegevens gecombineerd zijn met de loggegevens – die zoals blijkt uit punt 20 beiden zichtbaar zullen zijn – en deze combinatie tot identificeerbaarheid van gebruikers kan leiden, kan niet anders dan besloten worden dat de loggegevens als persoonsgegevens beschouwd moeten worden, in lijn met de gangbare rechtspraak van het Hof van Justitie.¹²
19. De aanvrager bevestigde in dat verband dat er geen andere gegevens dan de in het Ontwerp en de Memorie van Toelichting opgesomde gegevens verwerkt zullen worden: « *[o]ui, aucune autre donnée à caractère personnel que celles mentionnées dans l'article 31bis et dans l'exposé des motifs ne sera traitée.* » Bijgevolg kan ondersteld worden dat er onder de term "enz." geen andere elementen inbegrepen zullen zijn. Hetgeen enkel nog een vraagstuk openlaat m.b.t. de term '*verbinding*'. In die mate dat er hiermee iets ander bedoeld wordt dan een '*IP adres*', lijkt het aangeraden om dit minstens in de Memorie van Toelichting te verduidelijken en de noodzaak ervan te motiveren.
20. Tenslotte volgt krachtens ontworpen artikel 31bis, §1, lid 6 dat in het kader van hun functies, de toegang tot de persoonsgegevens open is voor ambtsdragers en medewerkers van de Raad van State. In dat verband verduidelijkt de aanvrager het volgende wat betreft:
 - a) **de persoonsgegevens van gebruikers van het elektronisch platform;** « *[e]n interne au Conseil d'Etat, les magistrats, greffiers et collaborateurs du greffe notamment auront accès aux données des utilisateurs mais il s'agit ici de données*

¹¹ Vet door de Autoriteit toegevoegd.

¹² Zie in dat verband HvJ 19 oktober 2016, nr. C-582/14, *Breyer*, EU:C:2016:779.

dites « utiles », c'est-à-dire nom, prénom, e-mail et téléphone. Le numéro national ne sera pas visible.

Il faut aussi noter que certaines de ces données telles que les noms et prénoms, adresse courriel et numéro de téléphone peuvent également apparaître sur les actes de procédure déposés par les utilisateurs (par exemple les noms, prénoms, adresse courriel et numéro de téléphone de l'avocat, que celui-ci fait apparaître en en-tête d'un acte de procédure). »¹³

- b) **de loggegevens;** « *[l']intention est, en effet, d'y donner accès en interne afin que les magistrats, les greffiers et le greffe puissent déterminer ce qui s'est passé sur la plate-forme dans un dossier X à un moment M. Mais ce sont des données « fonctionnelles », c'est-à-dire nécessaires au traitement du dossier sous un angle procédural. »¹⁴*
- c) **de processtukken:** « *[l']ensemble des titulaires de fonction ont accès aux pièces de procédure. Il en va de même pour les membres du personnel administratif de la section du contentieux administratif qui sont impliqués dans la fonction juridictionnelle du Conseil d'État et auquel il est donné accès à Proadmin+ (le personnel administratif du greffe, des chambres et de l'auditorat). Il ne s'agit donc pas de l'ensemble du personnel administratif. »¹⁵*

21. Uit de bijkomende toelichting, leidt de Autoriteit af dat er met toegang tot de persoonsgegevens in ontworpen artikel 31bis, §1, lid 6 bedoeld wordt dat binnen de Raad van State, magistraten, griffiers en medewerkers van de griffie toegang zullen hebben tot: *a) persoonsgegevens van gebruikers van het elektronisch platform; b) de loggegevens; c) de processtukken.* De aanvrager lijkt echter aan te geven dat niet alle voormelde personen beslist evenveel toegang hebben tot elk van deze drie onderdelen.¹⁶ Met het oog op de rechtszekerheid verdient het de aanbeveling om minstens in de Memorie van Toelichting verdere duiding te geven over wie precies begrepen wordt onder de termen ambtsdragers en medewerkers van de Raad van State en om een correlatie

¹³ Vertaling: "Binnen de Raad van State hebben met name magistraten, griffiers en medewerkers van de griffie toegang tot de gegevens van gebruikers, maar het gaat hier om zogenaamde 'nuttige' gegevens, d.w.z. naam, voornaam, e-mailadres en telefoonnummer. Het nationale nummer is niet zichtbaar.

Er moet ook worden opgemerkt dat sommige van deze gegevens, zoals namen en voornamen, e-mailadres en telefoonnummer, ook kunnen voorkomen in de door de gebruikers ingediende processtukken (bijvoorbeeld de namen, voornamen, e-mailadres en telefoonnummer van de advocaat, die deze in de koptekst van een processtuk vermeldt).

¹⁴ Vertaling: "Het is namelijk de bedoeling om deze gegevens intern toegankelijk te maken, zodat magistraten, griffiers en de griffie kunnen nagaan wat er op een bepaald moment op het platform is gebeurd in een bepaald dossier. Het gaat echter om "functionele" gegevens, d.w.z. gegevens die nodig zijn voor de procedurele afhandeling van het dossier."

¹⁵ Vertaling: "Alle ambtsdragers hebben toegang tot de processtukken. Hetzelfde geldt voor de administratieve medewerkers van de afdeling administratieve geschillen die betrokken zijn bij de rechtsprekende functie van de Raad van State en die toegang hebben tot Proadmin+ (het administratief personeel van de griffie, de kamers en de auditeur). Het gaat dus niet om het volledige administratief personeel."

¹⁶ **Persoonsgegevens van gebruikers** = magistraten, griffiers en medewerkers van de griffie; **loggegevens** = magistraten, griffiers en de griffie; **processtukken** = ambtsdragers, het administratief personeel van de griffie, de kamers en de auditeur.

te maken tussen hun functionele rol en de gegevens waartoe zij – behoudens wettelijke uitzonderingen – toegang geacht worden te hebben.

22. Wat de gegevens onder a) betreft, zou het om 'nuttige' gegevens gaan zijnde naam, voornaam, e-mail en telefoonnummer. Het rijksregisternummer zou binnen dezelfde cluster vallen, maar zou niet zichtbaar zijn. De beoogde verwerking in overweging genomen is, de Autoriteit, eerder van inziens dat deze als 'noodzakelijk' gekwalificeerd horen te worden. Indien het daarentegen toch om louter 'nuttige' gegevens zou gaan – d.w.z. niet noodzakelijk zijn zodat de verwerkingsdoeleinden bereikt kunnen worden zonder deze gegevens of met geanonimiseerde gegevens – dan spreekt het voor zich dat deze niet verwerkt mogen worden. Er wordt, m.b.t. het rijksregisternummer, in kanttekening opgemerkt dat indien dit de praktische toepassing is, het raadzaam lijkt om dit minstens in de Memorie van Toelichting te verduidelijken. Zonder opheldering, zou men ten onrechte de indruk krijgen dat het rijksregisternummer zichtbaar is voor voormelde personen.
23. Wat de gegevens onder b) betreft, blijkt uit de toelichting van de aanvrager dat de toegang openstaat voor magistraten, griffiers en de griffie. De Autoriteit meent, in de toepasselijke context, dat het effectief noodzakelijk is om te weten wanneer de indiening van stukken en de kennisnemingen plaatsvinden. Niettemin lijkt het, in het licht van de doeleinden, niet essentieel dat de 'verbinding' voor al de voormelde personen toegankelijk zijn. Hierbij wordt aangeraden om eventueel gebruik te maken van machtigingsniveaus zodat de zichtbaarheid van de gegevens beperkt is tot hetgeen werkelijk noodzakelijk is in het licht van het beoogde doeleinden.
24. Met betrekking tot de processtukken staat de Autoriteit positief t.a.v. het oogmerk om de toegang tot de processtukken te beperken. Terzake wordt verwezen naar punten 32 t.e.m. 34, waar dieper ingegaan wordt op mogelijke beschermings- en beveiligingsmaatregelen.
25. Op vraag van de Autoriteit naar de verbinding van het elektronisch platform met andere platformen, gaf de aanvrager dat dit degelijk het geval zou zijn. Zo werd aangegeven dat:
*« La plate-forme électronique décrite dans l'article 31bis, nommée 'eProadmin', est liée à un outil de consultation et de gestion interne dénommé 'Proadmin+'.
La plate-forme eProadmin et l'outil Proadmin+ constituent en réalité les deux volets d'un même outil : eProadmin en est le volet externe (front office), destiné à être utilisé par les utilisateurs tels que définis à l'article 85bis, § 2, 1°, du règlement général de procédure, alors que Proadmin+ est en le volet interne (back office), accessible aux seuls collaborateurs et titulaires de fonction du Conseil d'État.*

Une connexion avec DPA est envisagée afin que les avocats puissent aussi s'identifier par ce canal-là. »¹⁷

26. Volgens de aanvrager zou dit geen uitbreiding van de toegang tot de diverse voormelde persoonsgegevens op het platform met zich meebrengen. De toegang zou beperkt blijven tot enerzijds de gebruikers en anderzijds de ambtsdragers en medewerkers van de Raad van State. De Autoriteit neemt hier akte van en verwijst naar punten 32 t.e.m. 34 voor de aanbevelingen omtrent beschermings- en beveiligingsmaatregelen.
27. Het oogmerk om te voorzien in een verbinding met de Digital Platform for Attorneys (DPA), rijst niettemin een aantal vragen op. In dit verband lijkt het pertinent om te verwijzen naar eerder geleverd advies 78/2018 en in het bijzonder randnummer 29, waarin bemerkt wordt dat:
“De bewaring door de beroepsorganisaties van de gegevens die worden doorgegeven en neergelegd in e-Box en e-Deposit niet legitiem, noch proportioneel in het licht van het doeleinde om een beveiligde toegang tot de e-Box en e-Deposit systemen te verzekeren. Als een actor toegang wenst tot gegevens die voorheen werden doorgegeven volstaat het deze te raadplegen in e-Box en e-Deposit, na zich behoorlijk te hebben geïdentificeerd, indien nodig via zijn beroepsorganisatie.”¹⁸
28. In aanmerking genomen dat toegang tot het elektrisch platform via CSAM dient te verlopen, waarbij authenticatie gelinkt wordt aan ieders rijksregisternummer, en gelet op de informatie op de DPA-website dat vanaf midden 2025 zal kunnen worden ingelogd via eID of itsme, wordt de meerwaarde van een verbinding met het DPA, met het oog op identificatie hier in vraag gesteld. Het zou namelijk volgens de website zo zijn dat *“Het rijksregisternummer of BIS-nummer van de advocaat [...] geregistreerd [moet] zijn bij de balie om met eID of itsme te kunnen inloggen.”¹⁹* Vanuit dit optiek kan ondersteld worden dat deze informatie reeds beschikbaar is bij of verifieerbaar is via de balie en bijgevolg ook het elektrisch platform.
29. Voorts schaaft de Autoriteit zich wedermaal achter eerder geleverde observering, *m.n.*, dat het voor beroepsorganisaties – *in casu* de DPA – volstaat om de nodige gegevens te raadplegen op het elektronisch platform. Bovendien is het zelfs niet zeker dat een dergelijke raadpleging noodzakelijk is, gelet op het feit dat het elektronisch platform meerdere toepassingen zal bevatten die via het DPA tegen betaling aangeboden worden. Meer nog, het in het Ontwerp vastgelegde doeleinden lijken zich daar niet toe te strekken. Het is aan de aanvrager om ervoor te zorgen dat de verwerking van persoonsgegevens op rechtmatige wijze gebeurt, dat de risico's op

¹⁷ Digital Platform for Attorneys (DPA).

¹⁸ Voor de positie van de Autoriteit m.b.t. het DPA wordt verwezen naar advies 78/2018 in zijn geheel.

¹⁹ DPA, laatst geraadpleegd op 09 mei 2025, langs <https://www.dp-a.be/nl/app/toegang>.

gegevensinbreuken geminimaliseerd worden en dat onnodige verbindingen met externe platforms – zeker wanneer gelijkaardige handelingen reeds binnen het eigen systeem kunnen worden uitgevoerd – vermeden worden. In dat opzicht lijkt het elektronisch platform van de Raad van State het meest aangewezen, als elektronisch authentieke bron zijnde.

30. Het geheel in acht genomen, is de Autoriteit van mening dat voor het overgrote deel, de vermelde categorieën van persoonsgegevens, toereikend zijn. Maar om terzake dienend en beperkt te zijn, moet er in eerste instantie verdere duiding gegeven worden over de betrokkenen die toegang krijgen tot de persoonsgegevens. Hierbij lijkt het aangewezen om de Memorie van Toelichting aan te vullen met de bijkomende uitleg van de aanvrager, rekening houdend met de aanbevelingen uit punten 21 t.e.m. 24. In tweede instantie, moet worden nagegaan of het werkelijk essentieel is dat de verbinding zichtbaar is voor alle actoren. In derde instantie, wordt aanbevolen om verdere duiding te voorzien voor bepaalde termen. Tenslotte, wordt de noodzaak voor een verbinding met het DPA, in het licht van de beoogde doelstellingen in vraag gesteld.

d. Authenticatie en beschikbaarheid

31. Voorts wordt in het ontworpen artikel 31bis, §3 vermeld dat de werkwijze van het elektronisch platform, inclusief de registratieprocedure, de methodes voor de authenticatie van de gebruikers, het formaat en de ondertekening van de documenten, de nadere regels inzake het gebruik en de beveiliging vastgelegd worden in een koninklijk besluit na overleg in de ministerraad.
32. De Autoriteit staat positief tegenover het voornemen om beschermings- en beveiligingsmaatregelen vast te leggen. Terzake verdient het de aanbeveling om met autorisatiemaatregelen te werken, zodat toegang tot het platform, in het bijzonder dossierinhoud, en het uitvoeren van operaties of acties afhankelijk gemaakt wordt van bevoegdheden die gekoppeld wordt aan ieders identiteit.
33. Tevens wordt aanbevolen om logs bij te houden van de mandaathouders en medewerkers van de Raad van State hun activiteiten op het platform.²⁰ Gelet op de gevoelige context, wordt afgeraden om te opteren voor een lagere beschermingsgraad dan de tweefactorauthenticatie. In dat opzicht staat de Autorisatie positief tegenover het gebruik van CSAM als identificatiemiddel, zoals uit de Memorie van Toelichting blijkt.

²⁰ Het is aan de aanvrager om hiervoor de maximale bewaartermijn vast te leggen, rekening houdend met de noodzakelijkheid van de gegevens in het licht van de beoogde doelstellingen. Deze mag in geen geval langer zijn dan de bewaringstermijn van het onderliggend dossier of zaak. De redenering uit punten 41 t.e.m. 44 geldt hier eveneens naar analogie.

34. Daarnaast lijkt het aangeraden om een hiërarchische toegangsstructuur te implementeren, met verschillende classificatieniveaus – bijvoorbeeld laag, gemiddeld, hoog of vertrouwelijk, geheim, zeer geheim. Derwijze kan er naargelang de operationele en functionele noodzaak rekening houdend met ieders functionele taak, differentiële toegang verleend worden tot gebruikersgegevens, loggegevens, processtukken. Tenslotte moet encryptie geïmplementeerd worden voor de opslag en communicatie voor het verzekeren van de vertrouwelijkheid van de gegevens.

e. Verwerkingsverantwoordelijke(n)

35. De aanduiding van de verwerkingsverantwoordelijke moet overeenstemmen met de rol die deze actor in de praktijk zal opnemen en met de zeggenschap die hij heeft over de doeleinden en de middelen die voor de verwerking zullen worden ingezet. Dit moet in de praktijk voor elke verwerking van persoonsgegevens worden nagegaan.
36. Uit artikel 2 van het Ontwerp, *i.e.*, ontworpen artikel 31bis, volgt dat de Raad van State uitdrukkelijk aangeduid wordt als verwerkingsverantwoordelijke voor de verwerking van gegevens die daaruit voortvloeien.
37. De Autoriteit neemt hier akte van. Er wordt in kanttekening niettemin opgemerkt dat bij de invoering van een verbinding met het DPA, zie *supra*, meerdere verwerkingsverantwoordelijken mogelijk zijn, met alle gevolgen en verplichtingen van dien.²¹

f. Bewaartermijn

38. 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.
39. Terzake wordt in het hersteld artikel 31bis, §1, lid 4 gespecificeerd dat de persoonsgegevens van gebruikers van het elektronisch platform 30 jaar bewaard zullen worden. Deze termijn kan indien nodig, verlengd worden totdat alle rechtsmiddelen in hangende procedure waarmee die gegevens verband houden, uitgeput zijn. Daarnaast wordt in de Memorie van Toelichting verder aangegeven dat ook de loggegevens (vermeld in punt 20) bewaard zullen worden. Wat dat laatste betreft, bevestigde de aanvrager dat ook voor deze gegevens de bewaartermijn op 30 jaar wordt gesteld, met uitzondering van eventuele verlengingen zoals vermeld in het artikel. Op vraag naar de

²¹ Zie in dezelfde lijn advies 78/2018, randnrs. 24-25.

noodzakelijkheid van een bewaartermijn van 30 jaar, die aan verlenging onderworpen kon worden, stipuleerde de aanvrager het volgende:

« Comme cela est indiqué dans le commentaire du paragraphe 1^{er} de l'article 31bis , le délai de conservation de trente ans s'inspire du délai identique fixé par l'article 3, alinéa 2, de l'arrêté royal du 16 juin 2016 portant création de la communication électronique conformément à l'article 32ter du Code judiciaire.

Ce délai est notamment justifié par le fait que la survenance de certains incidents de procédure – par exemple une inscription de faux, qui doit d'abord être tranchée par le juge judiciaire avant que le Conseil d'État puisse poursuivre l'examen du recours – peut retarder la clôture du dossier devant le Conseil d'État. De la même manière, la solution d'un litige pendant devant le Conseil d'État peut être différée lorsqu'elle dépend de l'issue d'une procédure engagée devant les juridictions judiciaires, lesquelles peuvent nécessiter un temps de traitement particulièrement long.

Au vu de ces éléments, il est nécessaire que le Conseil d'État puisse conserver durant trente ans les données liées à l'utilisation de la plate-forme électronique, lesquelles doivent pouvoir être consultées et vérifiées en cas de contestation de la validité de la procédure menée devant le Conseil d'État. »²²

40. In aanmerking genomen dat de aanvrager tevens aangaf dat de 30 jarige maximale bewaartermijn een actieve bewaartermijn betreft, formuleert de Autoriteit de volgende bedenkingen:
41. Het geheel in acht genomen, is het redelijkerwijs noodzakelijk om gegevens te bewaren totdat de hangende rechtsprocedures beëindigd zijn en alle beroepsmogelijkheden uitgeput zijn. Echter wordt deze noodzakelijkheid in vraag gesteld voor dossiers die in een kortere termijn worden afgesloten, *i.e.*, voor het verstrijken van de aangegeven 30 jarige bewaartermijn. In dergelijke gevallen lijkt een ongedifferentieerde opgelegde bewaartermijn van dertig jaar zijn doel voorbij te schieten.
42. In dezelfde lijn heeft het Hof van Justitie meermaals benadrukt dat *"zelfs een oorspronkelijk rechtmatige verwerking van gegevens na verloop van tijd onverenigbaar met verordening 2016/679 kan worden wanneer deze gegevens niet langer noodzakelijk zijn in het licht van*

²² Vertaling: "Zoals aangegeven in de toelichting bij lid 1 van artikel 31bis, is de bewaartermijn van dertig jaar geïnspireerd op de identieke termijn die is vastgesteld in artikel 3, tweede lid, van het koninklijk besluit van 16 juni 2016 houdende de invoering van elektronische communicatie overeenkomstig artikel 32ter van het Gerechtelijk Wetboek.

Deze termijn is met name gerechtvaardigd door het feit dat bepaalde procedurele incidenten – bijvoorbeeld een valse inschrijving, waarover eerst door de gewone rechter moet worden beslist voordat de Raad van State de behandeling van het beroep kan voortzetten – de afsluiting van het dossier voor de Raad van State kunnen vertragen. Evenzo kan de beslechting van een geschil dat aanhangig is bij de Raad van State worden uitgesteld wanneer deze afhangt van de uitkomst van een procedure voor de gewone rechtbanken, die bijzonder lang kan duren.

Gezien deze elementen is het noodzakelijk dat de Raad van State de gegevens met betrekking tot het gebruik van het elektronisch platform gedurende dertig jaar kan bewaren, zodat deze kunnen worden geraadpleegd en gecontroleerd in geval van betwisting van de geldigheid van de procedure voor de Raad van State."

dergelijke doeleinden [zie in die zin arrest van 24 september 2019, GC e.a. (Verwijdering van links naar gevoelige gegevens), C-136/17, EU:C:2019:773, punt 74] en dat de gegevens moeten worden uitgewist wanneer deze doeleinden zijn bereikt.”²³

43. Er wordt tevens opgemerkt dat een ongedifferentieerde langdurige opslag ook risico's met zich meebrengt t.a.v. de juistheid van de gegevens, die na verloop van tijd mogelijks niet meer up-to-date zijn. Het is aan de aanvrager om aan te tonen waarom een dertig jarige termijn proportioneel en noodzakelijk is, hetgeen, *in casu*, ontbreekt voor afgesloten zaken zonder lopende gevolgen. In het licht hiervan verdient het de aanbeveling om, in eerste instantie, deze bewaartermijn te heroverwegen zodat niet alle gebruikersgegevens en loggegevens, systematisch gedurende dertig jaar bewaard worden, behoudens de wettelijke voorziene verlengingen en, in tweede instantie, de verschillende termijnen in de vorm van maximumtermijnen te formuleren. Zo kunnen er op basis van de status van een dossier (open, gesloten, beroep, enz.) specifieke bewaarbeleidsregels gehanteerd worden. Daarnaast kunnen ook retentie-herinneringen ingevoerd worden om na te gaan of de bewaring nog noodzakelijk is en kan er ook gewerkt worden met toegangsbeperkingen, waarbij de toegang tot gegevens die bewaard worden beperkt wordt tot een gesloten omgeving met toegangsrechten; hetgeen raadpleging, indien noodzakelijk, mogelijk maakt.
44. Wat de persoonsgegevens betreft die vervat zijn in de processtukken en stukken die een elektronisch dossier vormen, stipuleert het ontworpen artikel 31bis, §1, lid 5 dat "*deze bewaard [worden] zolang dat nodig is voor de uitoefening van de opdracht van openbaar belang waarmee de Raad van State als administratief rechtscollege bekleed is.*" Het is in dit verband aan de aanvrager om zich ervan te verzekeren dat de bewaartermijn overeenkomt met hetgeen strikt noodzakelijk is m.h.o het bereiken van de vooropgestelde doeleinden, binnen het kader van de opdracht en missie die aan de Raad van State toevertrouwd zijn.²⁴

OM DEZE REDENEN

de Autoriteit,

is van oordeel dat minstens de volgende wijzigingen geboden zijn in het voorontwerp van wet:

- voorzien in een verwijzing naar artikel 8 van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen (zie randnr. 15);

²³ HvJ 20 oktober 2022, nr. C-77/21, *Digi*, ECLI:EU:C:2022:805, para. 54.

²⁴ Het Grondwettelijk Hof heeft reeds erkend dat "de wetgever de voorwaarden voor het bewaren van persoonsgegevens, alsook de duur van deze bewaring in algemene bepalingen kan vastleggen", arrest nr. 29/2018 van 15 maart 2018, punt B. 23.

- aangeven in de Memorie van Toelichting dat het rijksregisternummer niet zichtbaar zal zijn (randnr.22);
- de termen ambtsdragers en medewerkers van de Raad van State verder specificeren en correleren met functionele rol en de gegevens waar toegang tot is (zie randnr. 21);
- indien de term verbinding op iets anders slaat dan '*IP adres*', wordt aanbevolen dit minstens in de Memorie van Toelichting te verduidelijken (zie randnr. 19);
- gedifferentieerde maximale bewaartermijn voorzien (zie randnrs. 40-43);

wijst op het belang van:

- het vastleggen van in deze context als minimaal beschouwde beschermings- en veiligheidsmaatregelen (zie randnrs. 32 - 34);
- het rechtmatigheidsbeginsel en het beginsel van minimale gegevensverwerking, in het bijzonder met betrekking tot de noodzakelijkheid van een verbinding met het DPA (zie randnrs. 28-30).

Voor de Autorisatie- en Adviesdienst,
(get.) Alexandra Jaspar, Directeur