Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 68/2026 van 9 april 2026

Betreft: Advies m.b.t. tot een voorontwerp van wet tot aanvulling van de wetten op de Raad van State, gecoördineerd op 12 januari 1973, met bepalingen over klokkenluiders (CO-A-2026-008).

Trefwoorden: maximale bewaartermijn – gezamenlijke verwerkingsverantwoordelijke – bestuursdocumenten – Raad van State klokkenluiders – intern meldingskanaal

Originele versie

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 mevrouw Annelies Verlinden, minister van Justitie (hierna "de aanvrager"), ontvangen op 13 januari 2026;

Brengt de Autorisatie- en Adviesdienst van de Gegevensbeschermingsautoriteit (hierna "de Autoriteit") op 9 april 2026 het volgende advies uit:

I. VOORWERP EN CONTEXT VAN DE ADVIESAANVRAAG

1. Op 13 januari 2026 verzocht de aanvrager het advies van de Autoriteit met betrekking tot een voorontwerp van wet tot aanvulling van de wetten op de Raad van State, gecoördineerd op 12 januari 1973, met bepalingen over klokkenluiders (hierna: Ontwerp).

2. Het Ontwerp betreft de gedeeltelijke omzetting van Richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het Unierecht melden (hierna: de richtlijn) met betrekking tot de leden van het administratief personeel, de personen bedoeld in de artikelen 102bis en 102ter en de ambtsdragers van de Raad van State.[1] Dit vertaalt zich met de invoeging van een nieuw hoofdstuk IX "Bescherming van klokkenluiders" in titel VII ("Inrichting van de Raad van State") van de wetten op de Raad van State, gecoördineerd op 12 januari 1973, waarin de artikelen 115/1 tot 115/11 vervat zijn.

3. Onderhavig Ontwerp vult de eerdere omzettingen van de richtlijn aan, m.n. de wet van 28 november 2022 betreffende de bescherming van melders van inbreuken op het Unie- of nationale recht vastgesteld binnen een juridische entiteit in de private sector, en de wet van 8 december 2022 betreffende de meldingskanalen en de bescherming van de melders van integriteitsschendingen in de federale overheidsinstanties en bij de geïntegreerde politie.

4. In acht genomen dat de wet van 8 december 2022 niet van toepassing is op het personeel van de rechterlijke orde, wordt een voorontwerp van wet voorbereid met als opschrift "*Wetsontwerp betreffende de meldingskanalen en de bescherming van de melders van integriteitsschendingen in de organen van de rechterlijke macht, bedoeld in deel II, boek I, van het Gerechtelijk Wetboek, in het Instituut voor gerechtelijke opleiding en in de Adviesraad van de magistratuur, met uitzondering van de Hoge Raad voor de Justitie*" dat betrekking heeft op rechters, leden van het openbaar ministerie, griffiers, personeelsleden van griffies en parketten, alsook op stagiairs en eveneens het voorwerp uitmaakt van een adviesaanvraag bij de Autoriteit.

5. In afwijking van het voorgaande geldt voor de Raad van State het onderhavig Ontwerp als lex specialis ten opzichte van de in rdnr. 4 vermelde norm, zodat die norm van toepassing blijft behoudens voor zover het Ontwerp uitdrukkelijk in een afwijkende regeling voorziet.[2]

[1] Artikel 115/1 van het Ontwerp.

[2] Memorie van Toelichting, 1.

II. ONDERZOEK TEN GRONDE

II.1 Rechtsgrond

6. *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.[3] De lezer wordt verwezen naar de toepassing van deze principes zoals hierna beschreven.

7. 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).

8. Daarnaast dient de formele norm, overeenkomstig het legaliteits- en het voorzienbaarheidsprincipe, tevens volgende (aanvullende) essentiële elementen te omvatten:[4]

   - de (categorieën van) verwerkte persoonsgegevens die ter zake 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.

---

[3] 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; (....)."

[4] Zie DEGRAVE, E., *"L'egouvernement et la protection de la vie privée – Légalité, transparance 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).

9. *Concrete toepassing:* de verwerking van persoonsgegevens waartoe het voor advies voorliggende Ontwerp aanleiding geeft, berust op artikel 6(1)(c) AVG.[5] 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) de verwerking betrekking heeft op kwetsbare personen; iii) plaats vindt voor toezichts- of controledoeleinden; iv) waarbij de gegevens meegedeeld of toegankelijk gemaakt worden voor derden; v) kan leiden tot een beslissing met negatieve gevolgen voor de betrokkenen,* is de Autoriteit van oordeel dat het, *in casu*, om een belangrijke inmenging gaat, waardoor de – reeds bestaande – verplichting om de essentiële elementen vast te leggen des te zwaarder doorweegt.

10. De Autoriteit zal hieronder nagaan of en in welke mate het thans voor advies voorliggend voorontwerp van wet strookt met de gegevensbeschermingsprincipes zoals deze voortvloeien uit de AVG en de WVG, in het bijzonder.

II.2 Artikelsgewijze bespreking

11. Na analyse van het geheel van de documenten stelt de Autoriteit vast dat het Ontwerp bepalingen bevat die betrekking hebben op allerhande aspecten die niet noodzakelijk verband houden met de regeling van de verwerking van persoonsgegevens. De Autoriteit beperkt hiernavolgende bespreking dan ook tot de in dat verband pertinente bepalingen.

ARTIKEL 115/3

12. Ontworpen artikel 115/3, regelt de samenstelling van het interne meldingskanaal, namelijk vier leden waarvan twee afkomstig van de Raad of het Coördinatiebureau en de twee van het Auditoraat, waarbij de taalpariteit wordt gewaarborgd door de aanwezigheid van twee Nederlandstalige en twee Franstalige leden. Daarnaast worden nog andere voorwaarden vastgesteld, waaronder de benoemingsvoorwaarden, bepaalde uitsluitingsgronden, een voorafgaand advies, een hernieuwbare mandaatduur van 6 jaar en de aanwijzing van plaatsvervangende leden.

ARTIKEL 115/4

13. Ontworpen artikel 115/4 voorziet in de keuzemogelijkheid voor de melder m.b.t. de persoon die belast wordt met de opvolging van en de terugkoppeling over diens melding. Bij gebreke aan een dergelijke keuze bepalen de leden van het interne meldingskanaal dit onderling.

[5] 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*."

ARTIKEL 115/5

14. Ontworpen artikel 115/5, bepaald dat het interne meldingskanaal, zie *infra*, aangewezen wordt als verwerkingsverantwoordelijke voor de persoonsgegevens die verwerkt worden i.h.k.v. de interne meldingen die het ontvangt. De Autoriteit neemt hier akte van, maar wijst er niettemin op dat er potentieel ook situaties van gezamenlijke verwerkingsverantwoordelijkheid zullen zijn, bijvoorbeeld bij doorzending van meldingen naar het Comité zoals bedoeld in artikel 6, 3° van de in rdnr. 4 vermelde norm.

ARTIKEL 115/6

15. Ontworpen artikel 115/6, dat artikel 16 van de richtlijn omzet, maakt van de geheimhoudingsplicht een essentiële ex-antemaatregel om represailles te voorkomen. Een dergelijke maatregel is tevens gerechtvaardigd in het licht van het recht op de eerbiediging van het privéleven en het recht op gegevensbescherming. De geheimhouding van de identiteit betreft niet enkel die van de melder, maar ook die van derden die met de melder in verband gebracht kunnen worden, de facilitator en de personen die meegewerkt hebben aan het onderzoek.[6]

16. De identiteit van de melder en van de overige betrokkenen mag in geen geval zonder hun vrije en uitdrukkelijke toestemming[7] worden bekendgemaakt aan anderen dan de gemachtigde personeelsleden die bevoegd zijn voor de ontvangst of de opvolging van de meldingen. Dit geldt ook voor alle andere informatie waaruit de identiteit van de melder of van de overige betrokkenen direct of indirect kan worden afgeleid. De Memorie van toelichting voegt daaraan toe dat in hun hoedanigheid van verwerkingsverantwoordelijken, het interne meldingskanaal ertoe gehouden is om passende technische en organisatorische maatregelen te treffen zodanig dat een passende beveiliging van de persoonsgegevens te waarborgen, zo wordt o.m. verwezen naar een strikt toegangscontrolebeleid waarbij er beperkingen zijn van wie toegang heeft tot de gegevens, het gebruik van betrouwbare authenticatie en het loggen van de toegangen.[8]

17. Wat het gebruik van een betrouwbare authenticatie betreft, verdient het de aanbeveling om te opteren voor een eIDAS-gebaseerde login van minstens het niveau 'substantieel' en bij voorkeur 'hoog'. In de praktijk komt dat neer op BOSA CSAM/FAS voor het inloggen (met eID, MyGov.be app of Itsme). Daarnaast dienen ook andere technische en organisatorische maatregelen overwogen te worden, zoals pseudonimisering of anonimisering van meldingen waar mogelijk, encryptie van gegevens, zowel bij opslag als bij verzending, gescheiden opslag van identiteitsgegevens en inhoud van meldingen, duidelijke bewaartermijnen en automatische verwijdering van gegevens, regelmatige beveiligingsaudits en tests van meldsystemen, opleiding en vertrouwelijkheidsverplichtingen voor

[6] Artikel 115/6, Memorie van Toelichting, 3.

[7] Artikel 4(11) AVG.

[8] Artikel 115/6, Memorie van Toelichting, 3.

personeelsleden die meldingen behandelen, incident response procedures bij datalekken. Tenslotte dient wat de opvolging van de beveiliging betreft, tijdig te worden toegezien op het verhelpen van softwarebeveiligingsproblemen, en hierbij in het bijzonder aandacht hebben voor eventuele gekende beveiligingsproblemen die door fabrikanten/ ontwikkelaars en het Centrum voor Cybersecurity België (CCB)[9] gemeld worden.

18. Het Ontwerp voorziet wel dat waar mogelijk een geanonimiseerde versie van het bestuursdocument kan worden bezorgd, en enkel en alleen wanneer er uit de context op geen enkele mogelijke manier enige persoonsgegevens, dan wel gegevens met betrekking tot identiteit kunnen worden afgeleid. **De aanvrager wordt verzocht bijkomende duiding te verschaffen over de ratio voor de invoering van deze mogelijkheid. In het bijzonder dient verduidelijkt te worden of dit ter bescherming is van de rechten van verdediging, welke reeds door het tweede paragraaf van ontworpen artikel 115/6 worden gewaarborgd, dan wel of het om transparantie in het kader van openbaarheid van bestuur gaat.** Ofschoon dit bijdraagt tot een hogere graad van transparantie, dient de aanvrager met de invoering van een dergelijke toepassing rekening te houden met het risico voor heridentificatie. Het kan het immers mogelijk zijn dat de loutere uiteenzetting van de context of van de feiten van de integriteitschending reeds toelaten de identiteit van de melder af te leiden, bijvoorbeeld op basis van elementen zoals de hiërarchische relatie, de locatie, etc.

19. In afwijking evenwel van het bovenstaande mogen de identiteit van de melder (en de derden) en enige andere informatie waaruit de identiteit van die personen kan worden afgeleid, "*uitsluitend worden bekendgemaakt indien het gaat om een noodzakelijke en evenredige verplichting krachtens bijzondere wetgeving in het kader van onderzoek door nationale autoriteiten of gerechtelijke procedures, mede ter waarborging van de rechten van verdediging van de betrokkene*." In dat geval moeten de betrokken personen daarvan in kennis worden gesteld, tenzij die informatie de gerelateerde onderzoeken of gerechtelijke procedures in het gedrang zou brengen. De Autoriteit is van oordeel dat de vereiste om over een **uitdrukkelijke, noodzakelijke en evenredige** verplichting krachtens het Unie- of nationale recht te beschikken voldoende waarborgen biedt met betrekking tot de bescherming van persoonsgegevens. Een dergelijke norm impliceert immers de facto de aanwezigheid van een gerechtvaardigd doeleinde voor het onthullen van de identiteit van de melder of de betrokkenen. Dit neemt uiteraard niet weg dat elke norm die een uitzonderingsgrond in het leven roept (en aldus een belangrijke inmenging in de rechten en vrijheden van de betrokkenen tot gevolg heeft), overeenkomstig artikel 36(4), AVG, gelezen in samenhang met artikel 57(1)(c), en overweging 96 van diezelfde verordening, eerst ter advies moet worden voorgelegd aan de Autoriteit.

[9] Zie hiervoor: CCB, *Cyber Threat Research & Intelligence Sharing*, laatst geraadpleegd op 26 maart 2026, langs <https://ccb.belgium.be/nl/cytris>; CCB, *overheid*, laatst geraadpleegd op 26 maart 2026, langs <https://ccb.belgium.be/nl/overheidsdiensten>.

20. De Autoriteit stelt daarnaast vast dat het Ontwerp aangeeft dat "*[d]e verdere verwerking van gegevens dient in het bijzonder in overeenstemming te zijn met artikel 6.1, onder c) en e), van Verordening (EU) 2016/679*." Dat gegevens verwerkt dienen te worden wanneer het noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of wanneer de verwerking noodzakelijk is 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, spreekt voor zich. Het is niettemin onduidelijk wat in deze context exact beoogd wordt door te voorzien in deze uitdrukkelijke specificering.

ARTIKEL 115/7

21. Ontworpen artikel 115/7 legt de concrete en precieze doeleinden vast van de verwerking van persoonsgegevens in het kader van de interne meldingen en de openbaarmakingen, m.n. het nagaan van de juistheid van de melding of de openbaarmaking gedane beweringen en, zo nodig, de gemelde integriteitsschending aanpakken. De Autoriteit neemt hier akte van.

ARTIKEL 115/8

22. Ontworpen artikel 115/8, dat een omzetting is van artikel 18 van de richtlijn, betreft de registratie van meldingen. Daarin wordt bepaald dat juridische entiteiten in de private en de publieke sector en de bevoegde autoriteiten, een register moeten bijhouden van elke ontvangen melding.

23. De bepaling zet drie specifieke hypotheses uiteen afhankelijk van de vorm van de melding, *i.e.*, een mondelinge melding met gespreksopname, een mondelinge melding zonder gespreksopname of een nauwkeurig verslag van het gesprek.

24. De aanvrager moet zich ervan vergewissen dat het ook voor de melder duidelijk is dat het doen van de melding overeenkomt met het geven van toestemming voor de verwerking van alle gegevens die de melder verstrekt. In dit verband wordt de aanvrager op gewezen dat het aan de verwerkingsverantwoordelijke is om, gelet op diens verantwoordelijkheid, aan te tonen dat er niet meer gegevens dan noodzakelijk verwerkt werden.

25. Terzake stelt de Autoriteit vast dat de bepaling in kwestie vermelding maakt van registratie en register. De aanvrager wordt erop gewezen dat de registratie van meldingen (hetgeen een verwerking uitmaakt) enkel rechtmatig is in het licht van de vooropgestelde doeleinden (zie rdnr. 21). Dit wordt in de Memorie van Toelichting geschraagd met de motivering dat "*[d]e implementatie van een meldingssysteem houdt een evenwichtsoefening in waarbij rekening dient te worden gehouden met de belangen van alle protagonisten (de organisatie, de melder en de betrokkene). Het belang van de organisatie vertaalt zich in de interne archiveringsregels inzake behoud en de bewaring van bestuursdocumenten.*"

26. Niettemin blijft onduidelijk wat het doel is van het register, noch welke gegevens erin zullen worden bewaard: wordt enkel de initiële melding geregistreerd, of tevens het volledige verloop van de opvolging; dient het register louter als 'opslagplaats' voor meldingen of is het als het ware het centrale platform binnen de interne en externe meldingskanalen voor de behandeling van meldingen; welke personen hebben toegang tot de inhoud van het register; onder welke voorwaarden kan er een gegevensoverdracht plaatsvinden tussen de registers van de bevoegde autoriteiten; … Deze elementen moeten in het ontwerp worden gepreciseerd. Op basis daarvan kunnen naderhand bijkomende richtlijnen of werkingsmodaliteiten worden vastgesteld.

27. Tenslotte wordt in de vijfde paragraaf gesteld dat "*[a]lle relevante documenten met betrekking tot een onderzoek in het kader van een melding door een intern meldingskanaal worden gedurende tien jaar bijgehouden worden*."

28. De aanvrager wordt er in dit verband op gewezen dat krachtens artikel 5(1)(e) van de AVG persoonsgegevens niet langer mogen 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. Dit wil zeggen dat, als het doeleinde bereikt is voor het verstrijken van de vooropgestelde bewaartermijn van 10 jaar, deze gegevens verwijderd dienen te worden. Doch om te kunnen bepalen wanneer deze bewaartermijn ingaat, dient een aanvangstermijn te worden voorzien. Zo kan de bewaartermijn ingaan op het ogenblik van de ontvangst van de melding, maar kan zij ook telkens opnieuw beginnen lopen bij nieuwe stappen in de procedure, zoals de opmaak van schriftelijke weergaven of de afsluiting van het onderzoeksrapport.

29. Daarnaast is het van wezenlijk belang om de aanvrager te verwijzen naar de adviespraktijk van de Raad van State waar sprake is van maximale bewaartermijn en niet van een algemeen vaste bewaartermijn.[10] Zo kan geenszins eenzelfde bewaartermijn gelden voor meldingen die wel tot een onderzoek geleid en meldingen die zonder verder gevolg zijn gebleven. Derhalve wordt verzocht het Ontwerp te wijzigen door de term 'gedurende' te schrappen en te vervangen door het begrip 'maximaal' en hierbij ook rekening te houden met diverse scenario's die een verschillende bewaartermijn vereisen.

ARTIKEL 115/9

30. Ontworpen artikel 115/9 verwijst naar het comité als bedoeld in artikel 14 van het in rdnr. 4 vermelde voorontwerp van wet, dat de taak van het extern meldingskanaal toevertrouwd aan een onafhankelijk orgaan, genaamd het Comité, dat samengesteld wordt uit een magistraat van het Grondwettelijk Hof, een magistraat van het Hof van Cassatie en een magistraat van de Raad van State. Deze bepaling regelt voorts de procedure en de samenstelling van het externe meldingskanaal, alsook het kader wat

[10] Adv.RvS 68.936/AV, 7 april 2021 over een voorontwerp dat heeft geleid tot de wet van 14 augustus 2021 betreffende de maatregelen van bestuurlijke politie tijdens een epidemische noodsituatie, Parl.St. Kamer 2020-21, nr. 55-1951/001, 119.

betreft het lid en de plaatsvervangende lid van het Hof bij het Comité. Deze bepaling geeft geen aanleiding tot verdere bemerkingen.

OM DEZE REDENEN,

Is de Autoriteit van oordeel dat:

1. De aanwijzing van de verwerkingsverantwoordelijke aangevuld moet worden zodat er vermelding gemaakt wordt van de gevallen van gezamenlijke verwerkingsverantwoordelijkheid (**rdnrs. 13**);

2. De aanvrager wordt aanbevolen om rekening te houden met de voorgestelde technische en organisatorische maatregelen (**rdnr. 17**);

3. De aanvrager dient de ratio en de toepassingsvoorwaarden van de geanonimiseerde versie van bestuursdocumenten nader te preciseren, met bijzondere aandacht voor het risico op heridentificatie (**rdnr. 18**);

4. De aanvrager dient de draagwijdte van de mogelijkheid tot verder verwerking, zoals beoogd door de verwijzing naar artikel 6(1)(c) en (e) AVG nader te preciseren (**rdnr. 20**);

5. De aanvrager dient te waarborgen dat de melder duidelijk wordt geïnformeerd over de verwerking van de verstrekte gegevens en dat enkel de voor het doeleinde noodzakelijke gegevens verwerkt worden (**rdnr. 24**);

6. Precisering betreffende het register en de registratie aan de orde is (**rdnrs. 22-26**);

7. Het Ontwerp voorzien van een maximale bewaartermijn (**rdnrs.** Error! Reference source not found.**-**Error! Reference source not found.).

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