



Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 142/2022 van 19 juli 2022

Betreft: Advies m.b.t. een voorontwerp van wet *betreffende de meldingskanalen en de bescherming van de melders van integriteitsschendingen in de federale overheidsinstanties en bij de geïntegreerde politie (CO-A-2022-134)*

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

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 Mevrouw Petra De Sutter, Minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post (hierna: de aanvrager), ontvangen op 13/05/2022;

brengt op 19 juli 2022 het volgend advies uit:

I. VOORWERP VAN DE ADVIESAANVRAAG

1. Op 13/05/2022 verzocht de aanvrager het advies van de Autoriteit met betrekking tot de artikelen 38 – 58 van het voorontwerp van wet *betreffende de meldingskanalen en de bescherming van de melders van integriteitsschendingen in de federale overheidsinstanties en bij de geïntegreerde politie* (hierna: het ontwerp).
2. Het ontwerp betreft de omzetting van de 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 federale overheidsinstanties voor wat betreft de verplichting van de federale overheid. Overeenkomstig het subsidiariteitsbeginsel vormt de richtlijn een aanvulling op de Europese sectorale regelingen die reeds meldingssystemen in de beroepssfeer bevatten, teneinde de minimumbeschermingsnormen naar boven toe te harmoniseren. Daarnaast worden in het licht van het evenredigheidsbeginsel ook gemeenschappelijke minimumnormen voor bescherming vastgesteld in bepaalde gebieden van het Europees beleid waar er behoefte is aan krachtigere handhaving; waar de niet-melding van misstanden door klokkenluiders de handhaving in het gedrang brengt en waar de inbreuken tot ernstige schade voor het algemeen belang kunnen leiden. De onder het meldingssysteem vallende beleidsdomeinen worden opgesomd in artikel 2, eerste lid, van de richtlijn. Niet elke inbreuk binnen deze gebieden valt evenwel binnen het toepassingsgebied van de richtlijn; het is tevens vereist dat de desbetreffende inbreuk afbreuk doet aan een 'handeling van de Unie'. Desalniettemin laat de richtlijn aan de lidstaten de mogelijkheid om de bescherming uit hoofde van het nationale recht uit te breiden tot gebieden of handelingen die niet *a priori* door de richtlijn worden gevat.
3. Binnen deze context geeft het ontwerp aldus aanleiding tot een verwerking van persoonsgegevens van zowel de melders als elke andere betrokkene en/of derde die in de melding worden vermeld, hetzij – bij een interne melding – door de betrokken federale overheidsinstantie en/of de geïntegreerde politie, hetzij – bij een externe melding – door de federale ombudsman, het Comité P of Comité I, hetzij door het Federaal Instituut voor de bescherming en de bevordering van de Rechten van de Mens (hierna: FIRM) bij een openbaarmaking.
4. Tot slot wijst de Autoriteit in dit kader op haar advies nr. 69/2022 dat betrekking heeft op een voorontwerp van wet *betreffende de bescherming van melders van inbreuken op het Unie- of nationale recht vastgesteld binnen een juridische entiteit in de private sector*¹.

¹ Te raadplegen via: <https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-69-2022.pdf>.

Voormeld voorontwerp van wet betreft de omzetting van de richtlijn ten aanzien van natuurlijke personen die in een werk gerelateerde context (in de private sector) kennis krijgen van informatie over inbreuken.

II. VOORAFGAANDE OPMERKING

5. 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 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. Het ontwerp heeft zonder meer een belangrijke inmenging in de rechten en vrijheden van de betrokkenen tot gevolg; niet alleen voor de melder maar tevens voor de in de melding geïdentificeerde personen (diegenen die ervan worden beschuldigd een inbreuk te hebben gepleegd). Deze personen riskeren immers zware sancties, en in het geval van onjuiste meldingen kan dit nefaste gevolgen hebben voor hun reputatie en/ of verdere carrière. Het zal aldus noodzakelijk zijn, waar mogelijk, om de wezenlijke elementen van de verwerking vast te stellen in het ontwerp.
7. Hierna volgt een artikelsgewijze bespreking van de bepalingen die betrekking hebben op de verwerking van persoonsgegevens, en deze die noodzakelijk zijn om de

gegevensverwerkingscontext te kunnen begrijpen. In dit kader benadrukt de Autoriteit dat dit advies louter betrekking heeft op de verwerkingen van persoonsgegevens die binnen het toepassingsgebied van de AVG vallen; elke verwerking die desgevallend gevat wordt door Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad* valt buiten de adviesbevoegdheid van de Autoriteit.

III. ARTIKELGEWIJZE BESPREKING VAN HET ONTWERP

ARTIKEL 1

8. Overeenkomstig artikel 5.1.b) AVG kan de verwerking van persoonsgegevens enkel uitgevoerd worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.
9. In artikel 1, §2, tweede lid, van het ontwerp wordt bepaald dat de wet tot doel heeft *“een hoog niveau van bescherming te bieden aan melders van integriteitsschendingen in de federale overheidsinstanties en de geïntegreerde politie.”* Zoals hierboven reeds aangehaald wordt daartoe de richtlijn omgezet in nationaal recht.
10. De Autoriteit merkt op dat, in tegenstelling tot wat volgt uit het adviesaanvraagformulier, het doeleinde van de wet in zijn geheel niet zonder meer overeenstemt met het doeleinde van de door het ontwerp geïntroduceerde verwerking(en) van persoonsgegevens. Het doeleinde van de gegevensverwerking naar aanleiding van een melding moet daarentegen worden afgeleid uit de artikelen 9 – 12², 13 – 22³ en 24⁴; namelijk het ontvangen en opvolgen⁵ van meldingen betreffende inbreuken in de zin van het ontwerp teneinde de juistheid van de in de melding (of openbaarmaking) gedane beweringen na te gaan en de gemelde inbreuk zo nodig aan pakken, onder meer via maatregelen zoals een intern vooronderzoek, een onderzoek, vervolging, een terugvordering van middelen of het beëindigen van de procedure. Indien (en voor zover) de persoon die een melding of openbaarmaking doet de voorwaarden van het ontwerp naleeft, kan hij genieten van de bescherming overeenkomstig hoofdstuk 7 van het ontwerp.

² Procedure ‘interne melding’.

³ Procedure ‘externe melding’.

⁴ Procedure ‘openbaarmaking’.

⁵ De notie ‘opvolging’ wordt in artikel 6, 22°, van het ontwerp als volgt gedefinieerd: *“optreden van de ontvanger van een melding of een bevoegde autoriteit om de juistheid van de in de melding gedane beweringen na te gaan en de gemelde integriteitsschending zo nodig aan te pakken, onder meer via maatregelen zoals een vooronderzoek, een onderzoek, vervolging, een terugvordering van middelen of het beëindigen van de procedure.”*

11. Zoals reeds toegelicht in de punten 5 – 6 van dit advies is het doeleinde van de verwerking een essentieel element. Rekening houdend bovendien met de belangrijke inmenging in de rechten en vrijheden van de betrokkenen en het grote aantal entiteiten door wie gegevens kunnen worden verwerkt in dit kader, is het noodzakelijk om over een duidelijke toetssteen voor de proportionaliteit van de verwerkte gegevens te beschikken. Het kan aldus niet volstaan dat de doeleinden afgeleid moeten worden uit een aantal artikelen van het ontwerp. De concrete en precieze doeleinden van de gegevensverwerking dienen uitdrukkelijk te worden gespecificeerd, bij voorkeur in afdeling 2 van hoofdstuk 6 van het ontwerp, dat betrekking heeft op de verwerking van persoonsgegevens.

ARTIKEL 2 – 4

12. De artikelen 2 – 4 van het ontwerp omschrijven het materieel toepassingsgebied van het ontwerp. Er wordt verduidelijkt dat het ontwerp enkel van toepassing is op de melding van integriteitsschendingen⁶. Ten aanzien van alle overige inbreuken (waaronder bijvoorbeeld pesterijen, ongewenst seksueel gedrag op het werk en allerlei vormen van discriminatie) kan er beroep worden gedaan op de algemene meldingskanalen opgenomen in de wettelijke en reglementaire bepalingen en rechtstreeks toepasbare Europese bepalingen, met inbegrip van de bepalingen die in uitvoering hiervan zijn vastgesteld. De Autoriteit is van oordeel dat de voormelde artikelen geen aanleiding geven tot bijzonder opmerking betreffende de verwerking van persoonsgegevens.

ARTIKEL 5

13. Artikel 5 van het ontwerp stelt het personeel toepassingsgebied van het ontwerp vast. In toepassing van artikel 4, lid 1, van de richtlijn is het ontwerp van wet van toepassing op natuurlijke personen die in een werkgerelateerde context kennis krijgen van informatie over inbreuken. Het ontwerp geldt in de eerste plaats voor personen met de hoedanigheid van (vroegere, huidige of toekomstige) werknemer, waaronder inbegrepen werknemers in een atypische arbeidsverhouding, zoals deeltijdse werknemers, werknemers met een

⁶ Artikel 2, §1, 2^e lid van het ontwerp bepaalt: "*Een integriteitsschending is:*

1° een handeling of het nalaten van een handeling die een bedreiging is voor of een schending is van het algemeen belang, en die:

- a) een inbreuk is op de rechts toepasbare Europese bepalingen, de wetten, de besluiten, de omzendbrieven, de interne regels en de interne procedures die van toepassing zijn op de federale overheidsinstanties en hun personeelsleden; en/ of*
- b) een risico inhoudt voor het leven, de gezondheid of de veiligheid van personen of voor het milieu; en/ of*
- c) getuigt van een ernstige tekortkoming in de professionele verplichtingen of in het beheer van een federale overheidsinstantie;*

2° het welbewust bevelen of adviseren om een integriteitsschending te begaan zoals bedoeld in 1°."

arbeidsovereenkomst voor bepaalde duur en uitzendkrachten, vrijwilligers en bezoldigde of onbezoldigde stagiairs. Daarnaast is het ontwerp eveneens van toepassing op zelfstandigen, aandeelhouders en personen die behoren tot het bestuurlijk, leidinggevend of toezichhoudend orgaan van de federale overheidsinstantie, met inbegrip van niet bij het dagelijks bestuur betrokken leden en eenieder die werkt onder toezicht en leiding van aannemers, onderaannemers en leveranciers. In voorkomend geval wordt het beschermingsregime uitgebreid tot facilitators⁷, derden die verbonden zijn met de melders en die het slachtoffer kunnen worden van represailles in een werkgerelateerde context, zoals collega's of familieleden van de melders en juridische entiteiten die eigendom zijn van de melders, waarvoor de melders werken of waarmee de melders anderszins in een werkgerelateerde context verbonden zijn.

14. De Autoriteit neemt akte van het personeel toepassingsgebied van het ontwerp.

ARTIKEL 7

15. Artikel 7, §1, van het ontwerp omschrijft de voorwaarden waaraan een melder moet voldoen om in aanmerking te komen voor bescherming in de zin van hoofdstuk 7 van het ontwerp. Melders worden beschermd voor zover: *"1° zij gegronde redenen hadden om aan te nemen dat de gemelde informatie over inbreuken op het moment van de melding juist was en dat die informatie binnen het toepassingsgebied van deze wet viel; en 2° zij intern overeenkomstig artikel 9 of extern overeenkomstig artikel 13 een melding hebben gedaan, of een openbaarmaking hebben gedaan overeenkomstig artikel 24.*

Het eerste criterium wordt beoordeeld ten overstaan van een persoon die zich in een vergelijkbare situatie bevindt en over vergelijkbare kennis beschikt.

De melder verliest het voordeel van de bescherming niet op de enkele grond dat de te goeder trouw gedane melding onjuist of ongegrond is bevonden."

16. Het volgt uit de Memorie van toelichting dat de vaststelling van deze voorwaarden het voorwerp uitmaakte van felle discussies op Europees niveau. De inhoud van voormeld artikel, dat een omzetting betreft van artikel 6.1. van de richtlijn, vertaalt de consensus tussen de lidstaten, zonder dat evenwel enige manoeuvreerruimte werd gelaten om bijkomende beschermingsvoorwaarden

⁷ De Memorie van toelichting verduidelijkt ter zake dat: *"De scheidslijn tussen het begrip "facilitator" en dat van "derde" ligt in de concrete bijstand die aan de melder wordt verleend. De facilitator biedt actieve ondersteuning om de acties van de melder te vergemakkelijken. De facilitator kan bijvoorbeeld een collega of naaste zijn die helpt bij de diefstal van achtergehouden gegevens, de verwerking van de gegevens of het zoeken naar een aanspreekpunt dat een onderzoek kan instellen. Het kan ook een werknemers- of vakbondsafgevaardigde of een vertrouwenspersoon integriteit zijn, die de melder informeert over het juridische kader en advies geeft over de te volgen stappen. In die hoedanigheid moeten zij de door het ontwerp van wet vastgestelde bescherming genieten, onverminderd de bescherming die zij genieten in hun hoedanigheid van vertegenwoordigers krachtens andere EU- en nationale voorschriften. Een gewone met de melder verbonden "derde" neemt daarentegen niet actief deel aan de melding. In zijn hoedanigheid van naaste van de melder kan hij evenwel het voorwerp zijn van indirecte represaillemaatregelen."*

op te leggen. Hoewel een dergelijke *modus operandi* te verdedigen valt in het kader van de harmonisatie van het recht van de lidstaten, dient opgemerkt te worden dat de voormelde voorwaarden minder strikt zijn dan de voorwaarden die voortvloeien uit de rechtspraak van het Europees Hof voor de Rechten van de Mens (EHRM). Meer concreet heeft het criterium van de redelijke overtuiging (dat de informatie correct is) het gehaald van het motivatiecriterium dat wordt gehanteerd door het EHRM ("*een daad wegens persoonlijke grieven of wrok of in het vooruitzicht van een persoonlijk voordeel, met name geldgewin, geen bijzonder hoog beschermingsniveau rechtvaardigt*") daar de Europese wetgever van oordeel is dat "*de motieven van de melders om te melden moeten losstaan van de beslissing of zij bescherming moeten krijgen*"⁸. Daarnaast werd in de richtlijn tevens afgezien van de 'verplichting' voor de melder om steeds de trapsgewijze procedure na te leven (eerst intern, dan extern, en slechts als *ultimum remedium* een openbaarmaking). Overeenkomstig de richtlijn (en het ontwerp) zal de melder – naar eigen goeddunken – "*het meest geschikte kanaal kunnen kiezen naargelang de individuele omstandigheden van het geval*"⁹.

17. Zonder zich ten gronde uit te spreken over de wenselijkheid van de voormelde criteria, betreurt de Autoriteit deze (potentiële) discrepantie tussen het recht van de Europese Unie enerzijds, en de rechtspraak van het EHRM, anderzijds. Aangezien er voor de Belgische wetgever evenwel geen enkele mogelijkheid was om ter zake een afwijkend regime vast te stellen, neemt de Autoriteit er akte van.
18. De paragrafen 2 en 3 van dit artikel zetten leden 2 en 3 van artikel 6 van de richtlijn om en luiden als volgt: "*§2. De interne en externe meldingskanalen waarop deze wet van toepassing is moeten de anonieme meldingen van integriteitsschendingen ontvangen en de opvolging ervan verzekeren. §3. Personen die anoniem informatie over integriteitsschendingen hebben gemeld of openbaar gemaakt, maar later zijn geïdentificeerd en het slachtoffer worden van represailles, komen in aanmerking voor bescherming overeenkomstig hoofdstuk 7, in zover ze beantwoorden aan de voorwaarden onder paragraaf 1.*"
19. Ten aanzien van de mogelijkheid om een anonieme melding te doen is de Autoriteit van oordeel dat een dergelijke melding zoveel mogelijk de uitzondering moet blijven. Niet alleen bemoeilijkt deze werkwijze de communicatie tussen de melder en de bestemming van de melding (dewelke nodig is voor een passende opvolging), bovendien kan dit aanleiding geven tot misbruiken in hoofde van de melders en de daarmee gepaard gaande ongeoorloofde verwerkingen van persoonsgegevens. Hoewel de eindverantwoordelijkheid met betrekking tot de verwerking van persoonsgegevens steeds rust bij de respectieve verwerkingsverantwoordelijken, dient ook de

⁸ Zie overweging 32 van de richtlijn.

⁹ Zie overweging 33 van de richtlijn.

melder de nodige verantwoordelijkheidszin aan de dag te leggen; een melding kan immers belangrijke gevolgen hebben voor de geviseerde personen.

20. In het licht van het proportionaliteitsbeginsel lijkt het aangewezen om, onverminderd bestaande verplichtingen om te voorzien in anonieme melding op grond van het Unierecht, het recht om een anonieme melding te doen te beperken tot de gevallen waar de risico's voor de melder duidelijk opwegen tegen de potentieel nadelige gevolgen voor de in de melding geviseerde personen.

ARTIKELN 9 – 12

21. De voormelde artikelen hebben betrekking op de verplichting voor federale overheidsinstanties, desgevallend na overleg en in samenspraak met de vakorganisaties, om interne meldingskanalen op te zetten voor hun werknemers en de procedures voor interne melding en opvolging vast te stellen.
22. In dit kader wijst de Autoriteit volledigheidshalve op de aanbeveling nr. 01/2006 *betreffende de verenigbaarheid van meldsystemen (klokkenluidersystemen) met de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens*¹⁰ van de Commissie voor de bescherming van de persoonlijke levenssfeer, de rechtsvoorganger van de Autoriteit, waarin werd onderstreept dat elk gebeurlijk overleg met de vakorganisaties of sociale partners moet plaatsvinden met naleving van de wetgeving inzake het collectief arbeidsrecht.
23. Daarnaast neemt de Autoriteit er akte van dat het overeenkomstig artikel 10, §1, 2^e lid van het ontwerp aan de federale overheidsinstanties vrij staat om de interne meldingskanalen ook open te stellen voor andere personen dan werknemers die in contact staan met de betrokken instantie en in het kader van hun werkgerelateerde activiteiten vaststellingen doen betreffende een integriteitsschending. Immers, aangezien er geen verplichting bestaat om een trapsgewijze procedure te volgen (*supra* punt 16), geeft de situatie waarin interne meldingskanalen niet zouden openstaan voor dergelijke personen geen aanleiding tot een uitholling van hun recht op bescherming overeenkomstig het ontwerp.
24. Artikel 10, §2 van het ontwerp bepaalt dat de Federale Audit dienst doet als intern meldingskanaal voor de beleidsorganen en de federale administratieve overheden waarbinnen geen intern meldingskanaal is opgericht. De Autoriteit neemt er akte van.

¹⁰ Te raadplegen via: <https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-1-2006.pdf>.

25. Zoals destijds reeds aangehaald door de Commissie voor de bescherming van de persoonlijke levenssfeer¹¹, zal de melding van een inbreuk nagenoeg altijd aanleiding geven tot een verwerking van persoonsgegevens, hetgeen zonder meer de noodzaak om een verwerkingsverantwoordelijke aan te duiden impliceert. De Autoriteit stelt vast dat de verwerkingsverantwoordelijke niet uitdrukkelijk wordt aangeduid, noch kan zijn identiteit, en dit in tegenstelling tot de 'externe procedure', met zekerheid worden afgeleid uit het ontwerp. De aanduiding van de verwerkingsverantwoordelijke draagt bij tot transparantie en vergemakkelijkt de uitoefening van de rechten van de betrokkenen vastgelegd in de artikelen 12 – 22 AVG. Bovendien moet de aanduiding van de verwerkingsverantwoordelijke in het licht van de feitelijke omstandigheden gepast zijn. Met andere woorden, voor elke verwerking van persoonsgegevens moet worden nagegaan wie feitelijk het doel nastreeft en controle heeft over de verwerking¹².
26. In beginsel zal het steeds de federale overheidsinstantie zelf zijn die optreedt als verwerkingsverantwoordelijke ten aanzien van de gegevens die worden verwerkt in het kader van een interne melding. De werknemers die binnen een bepaalde federale overheidsinstantie belast zijn met de opvolging van meldingen kunnen aldus louter aangemerkt worden als 'personen die handelen onder het gezag van de verwerkingsverantwoordelijke of van de verwerker' in de zin van artikel 29 AVG. Het feit dat de verwerkingsverantwoordelijke niet daadwerkelijk toegang heeft tot de gegevens (dit zou uiteraard de verplichte geheimhouding van de melding in het gedrang brengen) speelt daartoe geen rol¹³. Teneinde elke onduidelijkheid hieromtrent te vermijden, vraagt de Autoriteit om uitdrukkelijk in het ontwerp te specificeren dat wanneer het meldingsbeheer wordt waargenomen door (een) werknemer(s) van de federale overheidsinstantie, de federale overheidsinstantie zelf optreedt als verwerkingsverantwoordelijke.
27. Ook wanneer de federale overheidsinstantie overeenkomstig artikel 10, §1, derde lid, van het ontwerp beroep doet op een derde voor het beheer van het meldingskanaal zal het de federale overheidsinstantie zijn die optreedt als verwerkingsverantwoordelijke (en de derde louter als verwerker).

¹¹ Zie ter zake de voormelde aanbeveling nr. 01/2006.

¹² Zowel de Europees Comité voor gegevensbescherming als de Autoriteit hebben benadrukt dat het concept verwerkingsverantwoordelijke vanuit een feitelijk perspectief moet worden benaderd. Zie in dat kader de richtsnoeren 07/2020 van de EDPB *over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG*. (https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_nl.pdf (let op: deze vertaling werd op heden nog niet officieel goedgekeurd)) en Gegevensbeschermingsautoriteit, *Overzicht van de begrippen verwerkingsverantwoordelijke/verwerker in het licht van de Verordening (EU) nr. 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 (AVG) en enkele specifieke toepassingen voor vrije beroepen zoals advocaten* (https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Begrippen_VW_OA.pdf).

¹³ Dit wordt bevestigd in de richtsnoeren 07/2020 van de EDPB *over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG*.

28. Het bovenstaande laat uiteraard onverlet de geheimhoudingsplicht in hoofde van de ontvangers van meldingen overeenkomstig artikel 25 van het ontwerp en de sancties waaraan zij zich bij een schending van deze verplichting blootstellen (zie artikel 40 van het ontwerp).
29. Tot slot omschrijft artikel 12 van het ontwerp de modaliteiten van de procedures voor interne melding en opvolging. De concrete elementen van de procedure moeten overeenkomstig artikel 10, §1, 4^e lid, van het ontwerp nader worden uitgewerkt door de federale overheidsinstantie in een reglement of omzendbrief. Eenzelfde verplichting bestaat in hoofde van de Federale Audit wanneer zij dienstdoet als intern meldingskanaal overeenkomstig artikel 10, §2 van het ontwerp¹⁴. Deze reglementen, omzendbrieven of samenwerkingsakkoorden zijn bindend en dienen bekend te worden gemaakt op de respectieve websites van de federale overheidsinstanties, de Federale Audit of het FIRM. Hoewel de elementen van de procedure (zoals die volgen uit artikel 12 van het ontwerp) *an sich* geen aanleiding geven tot bijzondere opmerkingen aangaande de verwerking van persoonsgegevens, vraagt de Autoriteit zich desalniettemin af in hoeverre er effectief sprake kan zijn van 'bindende' regels, gelet op de wijze waarop zij moeten worden vastgesteld. Rekening houdend met de belangrijke inmenging in de rechten en vrijheden van de betrokkenen, is het cruciaal dat de concrete procedureregels inzake de ontvangst en opvolging van een melding voor iedereen dezelfde zijn. Deze reglementen worden dus bij voorkeur vastgesteld in een koninklijk besluit. Volledigheidshalve nog wijst de Autoriteit in dit kader op de richtsnoeren van de Europese Toezichthouder voor gegevensbescherming (EDPS) (*EDPS, Guidelines on processing personal information within a whistleblowing procedure*, december 2019¹⁵) dewelke specifiek betrekking hebben op de verwerking van persoonsgegevens in het kader van 'klokkenluider-procedures'. Hoewel deze richtsnoeren in beginsel gericht zijn tot de instellingen, organen en instanties van de Europese Unie, vormen zij zonder meer een waardevolle bron van inspiratie voor de nationale instanties of autoriteiten.

ARTIKELN 13 – 23

30. Deze artikelen omschrijven de modaliteiten van en de procedures voor de externe meldingskanalen.
31. Het kan worden afgeleid uit de voormelde artikelen dat ofwel de federale ombudsman, het Comité P, of het Comité I optreden als verwerkingsverantwoordelijke ten aanzien van de gegevensverwerkingen in het kader van de externe melding van integriteitsschendingen begaan in respectievelijk de federale overheidsinstanties in het algemeen, het Coördinatieorgaan voor de

¹⁴ Artikel 11, derde lid, van het ontwerp bepaalt daartoe: "De Federale Audit bepaalt in het permanent samenwerkingsverband de elementen als bedoeld in artikel 12 door middel van een reglement. Bij gebreke aan dit reglement wordt het door de Koning bepaald."

¹⁵ Te raadplegen via: https://edps.europa.eu/sites/default/files/publication/19-12-17_whistleblowing_guidelines_en.pdf.

Dreigingsanalyse zoals bedoeld in de wet van 10 juli 2006 *betreffende de analyse van de dreiging* en de Algemene Dienst Inlichting en Veiligheid of de Veiligheid van de Staat. Desalniettemin lijkt het aangewezen om dit uitdrukkelijk vast te stellen in het ontwerp.

32. De aanvrager verduidelijkt in de Memorie van toelichting bij het ontwerp dat de oprichting van de externe meldingskanalen bij de collaterale organen van het Federaal Parlement een waarborg inhoudt voor de in artikel 11, paragraaf 2, lid a) van de richtlijn vereiste criteria van onafhankelijkheid en autonomie van de externe meldingskanalen voor het ontvangen en in behandeling nemen van informatie over inbreuken. De Autoriteit neemt er akte van.
33. Overeenkomstig artikel 14, §2, laatste lid, van het ontwerp dienen de externe meldingskanalen hun verplichtingen inzake beroepsgeheim na te leven bij het geven van feedback in de zin van punt 4° van het eerste lid van paragraaf 2 van datzelfde artikel. Ter zake merkt de Autoriteit op dat de geheimhoudingsverplichting, in lijn met de geest van overweging 77 en artikel 13, paragraaf 3, van de richtlijn, betrekking heeft op de gehele ontvangst- en opvolgingsprocedure. In de mate dat artikel 14, §2, laatste lid, van het ontwerp (verkeerdelijk) de indruk geeft dat dit niet het geval is, lijkt het aangewezen om voormeld artikel als volgt aan te passen: 'bij de uitoefening van hun bevoegdheden overeenkomstig het eerste lid dienen de externe meldingskanalen hun verplichtingen inzake beroepsgeheim na te leven.'
34. Het volgt uit artikel 14, §3, van het ontwerp dat: *"Elke autoriteit die een melding ontvangt, maar niet bevoegd is om de gemelde integriteitsschending te behandelen, moet de melding binnen een redelijke termijn en op veilige wijze doorgeven aan de desgevallend bevoegde autoriteit indien zij deze op grond van de beschikbare informatie kan bepalen, en de melder onverwijld over deze doorgifte informeren.*
Indien de autoriteit die de melding heeft ontvangen er kennis van heeft dat ook andere autoriteiten bevoegd zijn, wordt de informatie van de melding binnen een redelijke termijn en op veilige wijze doorgegeven aan de andere bevoegde autoriteiten."
- Het verdient aanbeveling om in het ontwerp, of desgevallend naderhand bij koninklijk besluit, de verhouding vast te stellen tussen de ontvangende autoriteit en de (overige) bevoegde autoriteit(en). Meer concreet moet in dergelijke gevallen uitgeklaard worden wanneer, en onder welke voorwaarden de onderscheiden autoriteiten optreden als verwerkingsverantwoordelijke, dan wel als verwerker of gezamenlijke verwerkingsverantwoordelijke¹⁶.
35. Artikel 15, §2, van het ontwerp bepaalt welke informatie de melding moet bevatten, het betreft:

¹⁶ Indien er sprake is van gezamenlijke verantwoordelijkheid in de zin van artikel 26 AVG verwijst de Autoriteit, voor wat betreft de praktische gevolgen daarvan, naar punt 2 van het tweede deel van de richtsnoeren 07/2020 van de EDPB *over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG*. Zie voetnoot 13.

"1° de naam en de contactgegevens van de melder, tenzij de melder opteert voor de anonieme melding;

2° de datum waarop de melding wordt gedaan;

3° de aard van de arbeidsrelatie tussen de melder en de betrokken federale overheidsinstantie;

4° de naam van de bij de integriteitsschending betrokken federale overheidsinstantie;

5° de beschrijving van de integriteitsschending;

6° de datum waarop of de periode waarin de integriteitsschending heeft plaatsgevonden, plaatsvindt of zeer waarschijnlijk zal plaatsvinden.

De melder voegt alle informatie toe waartoe hij toegang heeft en die kan bijdragen aan het beoordelen van het redelijk vermoeden van de integriteitsschending."

36. In het licht van de opmerkingen die daartoe werden geformuleerd in punt 47 van het advies nr. 69/2022 laat de Autoriteit zich gunstig uit over de aanduiding van de categorieën van persoonsgegevens die (minstens) verwerkt zullen worden in het kader van de opvolging van een melding. Met betrekking tot de gegevens van de in de melding geïdentificeerde personen benadrukt de Autoriteit evenwel dat deze persoonsgegevens zich moeten beperken tot de gegevens die pertinent zijn in het kader van de vermeende inbreuk. Dit doet uiteraard geen afbreuk aan de verplichting in hoofde van de verwerkingsverantwoordelijken om per geval toe te zien op de naleving van het evenredigheidsbeginsel en het beginsel van de minimale gegevensverwerking overeenkomstig artikel 5.1.c) AVG.
37. Voorts volgt het uit de artikelen 18, §1, 3°, en 19, tweede lid, 5°, van het ontwerp dat tevens *"de naam, de taalrol en de contactgegevens van de door het extern meldingskanaal afgevaardigde onderzoekers en, desgevallend, de deskundigen die hen bijstaan bij de uitvoering van het onderzoek"* zullen worden verwerkt. Gelet op de beoogde doeleinden geeft de verwerking van deze persoonsgegevens geen aanleiding tot bijzondere opmerkingen.
38. Desalniettemin is de Autoriteit van oordeel dat een gelijkaardige regelgeving opgenomen moet worden voor wat betreft de interne meldingen (en desgevallend de openbaarmaking), dan wel dat de inhoud van deze bepalingen overgeheveld moet worden naar artikel 26 van het ontwerp (dat betrekking heeft op alle gegevensverwerkingen krachtens het ontwerp).
39. Tot slot bepaalt artikel 23 van het ontwerp, dat artikel 14 van de richtlijn omzet, het volgende: *"De externe meldingskanalen evalueren hun procedures voor de ontvangst en opvolging van meldingen regelmatig, en ten minste om de drie jaar. Bij de evaluatie van deze procedures houden de externe meldingskanalen rekening met hun eigen ervaring en die van andere bevoegde autoriteiten en passen zij hun procedures dienovereenkomstig aan."*

In dat kader stellen de externe meldingskanalen een geanonimiseerd samenvattend verslag op dat ze overmaken aan het Parlement."

40. Betreffende het geanonimiseerde verslag dat overgemaakt moet worden aan het Federaal Parlement herhaalt de Autoriteit dat de identificatie van een persoon niet enkel slaat op de mogelijkheid om zijn naam en/of adres te achterhalen maar eveneens op de mogelijkheid om hem te identificeren via een proces van individualisering, correlatie of gevolgtrekking. Ter zake dient gewezen te worden op het verschil tussen gepseudonimiseerde gegevens, die in artikel 4.5) AVG worden gedefinieerd als gegevens die *"niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt"* en geanonimiseerde gegevens, die niet langer met redelijke middelen aan een bepaalde persoon kunnen worden toegeschreven, en dat enkel deze laatste geen persoonsgegevens meer vormen en dus overeenkomstig overweging 26 zijn uitgesloten van de werkingssfeer van de AVG¹⁷. Derhalve, rekening houdend met de definitie van persoonsgegevens in artikel 4. 1), van de AVG¹⁸, moet ervoor worden gezorgd dat aan de vereiste hoge normen voor anonimisering wordt voldaan en dat de gegevens niet eenvoudigweg worden gepseudonimiseerd. De verwerking van dergelijke gegevens, zelfs al zijn ze gepseudonimiseerd, moet immers worden gezien als een verwerking van persoonsgegevens als bedoeld in de AVG. Uit het voorgaande volgt dat als er sprake is van pseudonimisering (en niet anonimisering):
- er moet worden verwezen naar de verslagen van het Europees Agentschap voor Cyberbeveiliging betreffende technieken en goede praktijken voor pseudonimisering¹⁹;
 - deze verwerking moet worden omkaderd met alle vereiste waarborgen en moet voldoen aan de heersende beginselen ter zake²⁰.

¹⁷ Voor meer informatie, zie het advies 5/2014 (WP216) *over anonimiseringstechnieken*, 2.2.3, van de Groep 29, de rechtsvoorganger van de EDPB. Te raadplegen via: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_nl.pdf.

¹⁸ Namelijk: *"alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon"*.

¹⁹ ENISA: <https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases> en <https://www.enisa.europa.eu/news/enisa-news/enisa-proposes-best-practices-and-techniques-for-pseudonymisation>.

²⁰ Hetzelfde geldt voor het proportionaliteitsbeginsel dat verwijst naar het specifiekere beginsel van *"minimale gegevensverwerking"* dat inhoudt dat de persoonsgegevens toereikend, ter zake dienend en beperkt moeten zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt, overeenkomstig artikel 5, § 1, c), van de AVG.

ARTIKEL 24

41. Artikel 24, §1, van het ontwerp bepaalt de voorwaarden – naast degene die reeds zijn neergelegd in artikel 7, §1, van het ontwerp – waaraan een persoon die een openbaarmaking doet, moet voldoen om in aanmerking te komen voor bescherming uit hoofde van het ontwerp. Er worden twee gevallen onderscheiden:

“1° in geval van een indirecte openbaarmaking: de persoon deed eerst een interne en externe melding, of meteen een externe melding overeenkomstig de hoofdstukken 3 en 4, maar er zijn naar aanleiding van die melding geen passende maatregelen genomen binnen de in artikel 12, 6°, of artikel 18, paragraaf 1, tweede lid, genoemde termijn; of

2° in geval van een directe openbaarmaking: de persoon heeft gegronde redenen om aan te nemen dat:

a) de integriteitsschending een dreigend of reëel gevaar kan zijn voor het algemeen belang; of

b) er in geval van externe melding een risico op represailles bestaat, of het niet waarschijnlijk is dat de integriteitsschending doeltreffend wordt verholpen, wegens de bijzondere omstandigheden van de zaak, omdat bijvoorbeeld bewijsmateriaal kan worden achtergehouden of vernietigd, of een autoriteit kan samenspannen met de pleger van de integriteitsschending of bij de integriteitsschending betrokken is.

Het eerste lid, 1°, geldt niet wanneer geen feedback wordt verstrekt overeenkomstig artikel 12, tweede lid.”

42. Paragraaf 2 van datzelfde artikel bepaalt dat het openbaarmakingsregime niet van toepassing is, of beter, geen afbreuk doet aan de regelgeving inzake de verwerking van persoonsgegevens voor journalistieke doeleinden overeenkomstig de artikelen 85 AVG en 24 WVG, met name wanneer een persoon op grond van de voormelde bepalingen rechtstreeks informatie aan de pers verstrekt.

43. Tot slot dient in dit kader gewezen te worden op artikel 41, §2, eerste lid, van het ontwerp dat bepaalt: *“Onverminderd andere maatregelen waarin deze wet of andere wettelijke of bestuursrechtelijke bepalingen voorzien, worden melders gestraft overeenkomstig de artikelen 443 tot en met 450 van het Strafwetboek wanneer wordt vastgesteld dat zij opzettelijk valse informatie hebben gemeld **of openbaar hebben gemaakt.**”* Dergelijke personen stellen zich bijgevolg ook bloot aan de sancties neergelegd in de AVG.... Er is in dat geval immers sprake van een onrechtmatige verwerking van persoonsgegevens van de in de openbaarmaking geïdentificeerde personen door de melder (voor zover de openbaarmaking dergelijke gegevens bevat). Het bovenstaande laat uiteraard onverlet dat wanneer de bevoegde autoriteiten besluiten om naar aanleiding van een openbaarmaking een onderzoek in te stellen naar de vermoede inbreuk(en), zij verantwoordelijk zijn voor de gebeurlijke verwerkingen van persoonsgegevens in dat kader.

ARTIKEL 25

44. Artikel 25 van het ontwerp zet artikel 16 van de richtlijn om, dat van geheimhouding een essentiële maatregel *ex ante* maakt om represailles te voorkomen. Een dergelijke maatregel is eveneens vereist in het licht van het recht op persoonlijke levenssfeer en de gegevensbescherming. Hoewel artikel 16 van de richtlijn niet uitdrukkelijk verwijst naar de betrokkenen (lees: de door de melding geïdentificeerde personen), de facilitators en de derden in de zin van de richtlijn, is het aangewezen ook hen een vertrouwelijke behandeling te verlenen. Zulks vloeit eveneens voort uit artikel 9 van de richtlijn volgens hetwelk de kanalen voor de ontvangst van interne meldingen zodanig moeten worden ontworpen, opgezet en beheerd dat ze *“op beveiligde wijze de vertrouwelijkheid van de identiteit van de melder van eventuele in de melding genoemde derden beschermen”*. In dit kader neemt de Autoriteit akte van artikel 25, §5, van het ontwerp dat bepaalt: *“Desgevallend zijn de in paragraaf 1 tot en met 3 aangehaalde beschermingsmaatregelen ook van toepassing op de in artikel 5, § 2, 1° et 2°, bedoelde personen.”*
45. De identiteit van de melder en van de overige betrokkenen mag in geen geval zonder hun *vrije en uitdrukkelijke toestemming*²¹ 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, de interne en externe meldingskanalen ertoe gehouden zijn om passende technische en organisatorische maatregelen te treffen zodanig dat een passende beveiliging van de persoonsgegevens wordt gewaarborgd. Ter zake vraagt de Autoriteit om in het ontwerp uitdrukkelijk te specificeren welke handelingen een *‘vrije en uitdrukkelijk toestemming’* constitueren. In dit kader kan gewezen worden op de voorwaarden voor een geldige toestemming in de zin van de AVG²².
46. 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

²¹ Het is aangewezen om in de Franstalige versie van het ontwerp dezelfde terminologie als in de AVG te gebruiken, namelijk: *consentement explicite et libre* in plaats van *consentement exprès et libre*.

²² Zie daartoe de Richtsnoeren 05/2020 van de EDPB *inzake toestemming overeenkomstig Verordening 2016/679*. Te raadplegen via: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_nl.pdf.

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.

ARTIKEL 26

47. Artikel 26 heeft betrekking op de verwerking van persoonsgegevens krachtens het ontwerp, met inbegrip van de uitwisseling of doorgifte van persoonsgegevens door de externe meldingskanalen.
48. In eerste instantie merkt de Autoriteit op dat paragraaf 1 van dit artikel geen enkele juridische meerwaarde heeft:
- de leden 1 en 2 bevestigen louter de toepasbaarheid van de AVG, de Richtlijn (EU) 2016/680 en de Verordening (EU) 2018/1725, zonder dat er evenwel een mogelijkheid bestaat om de geviseerde verwerkingen, uitwisselingen of doorgiften van informatie uit te sluiten van het toepassingsgebied van de voormelde Europese wetgeving;
 - het derde lid betreft een (gedeeltelijke) parafrasering van het verantwoordelijkheidsbeginsel – meer bepaald van artikel 25 AVG – en geeft aldus aanleiding tot een schending van het overschrijfverbod van de AVG²³;
 - met betrekking tot het laatste lid merkt de Autoriteit op dat de rechtmatigheid van een verwerking die noodzakelijk is om te voldoen aan een wettelijke verplichting of 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, beoordeeld moet worden in het licht van de kwaliteit van de wetgeving die deze verplichting of taak van algemeen belang in het leven roept. Daartoe moet worden nagegaan of de wezenlijke elementen van de verwerking (zie de punten 5 – 6) op afdoende wijze zijn vastgesteld in een wettelijke norm. In het onderhavige geval bestaat er immers geen twijfel over de rechtsgrond waarop de verwerking is gestoeld.

De eerste paragraaf van artikel 26 van het ontwerp dient aldus geschrapt te worden.

²³ De rechtstreekse toepasselijkheid van Europese verordeningen houdt een verbod in om deze in nationaal recht om te zetten omdat een dergelijke procedure "een dubbelzinnigheid kan creëren over zowel de juridische aard van de toepasselijke bepalingen als het tijdstip van hun inwerkingtreding". Zie: HJEU, 7 februari 1973, Commissie c. Italië (C-39/72), Recueil de jurisprudence, 1973, p. 101, § 17). Zie ook: HJEU 10 oktober 1973, Fratelli Variola S.p.A. c. Italiaanse Belastingdienst (C-34/73), Recueil de jurisprudence, 1973, p. 981, § 11; HJEU, 31 januari 1978, Ratelli Zerbone Snc c. Amministrazione delle finanze dello Stato, Recueil de jurisprudence (C-94/77), 1978, p. 99, §§ 24-26.

49. Zoals reeds toegelicht in de punten 10 – 11 van dit advies is het daarentegen aangewezen om in artikel 26 van het ontwerp de concrete en precieze doeleinden van de verwerking vast te stellen.
50. Daarnaast, tenzij analoge bepalingen worden opgenomen in de hoofdstukken 3 (interne meldingen en opvolging) en 5 (openbaarmaking) van het ontwerp, verdient het aanbeveling om de bepalingen betreffende de vaststelling van de te verwerken categorieën van persoonsgegevens bij externe meldingen (de artikelen 15, §2, 18, §1, en 19 van het ontwerp) over te hevelen naar artikel 26 van het ontwerp (zie ook de punten 35 – 38).
51. Tot slot wijst de Autoriteit op de verplichting om in het licht van artikel 6.3 AVG, in samenlezing met artikel 22 van de *Grondwet*, te voorzien in een maximale bewaartermijn van de te verwerken persoonsgegevens rekening houdend met de onderscheiden doeleinden en de categorieën van gegevens. De Autoriteit stelt vast dat op heden geen dergelijke termijn is bepaald in functie van de doeleinden van de verwerking. De bewaartermijn overeenkomstig artikel 27, §1 van het ontwerp heeft immers louter betrekking op het register van de meldingen (en constitueert bovendien geen geldige bewaartermijn in de zin van de AVG – *infra* punt 56). Het is aldus noodzakelijk om in het ontwerp een **maximale** bewaartermijn te voorzien, of toch minstens de criteria op te nemen die toelaten om deze bewaartermijn te bepalen. Bovendien moet in dit kader een onderscheid worden gemaakt tussen de meldingen die effectief aanleiding geven tot een opvolging en de meldingen die onontvankelijk worden verklaard. Het spreekt voor zich dat in het laatste geval een kortere bewaartermijn moet worden gehanteerd.
52. De paragrafen 2 tot en met 5 van artikel 26 van het ontwerp voorzien in een beperking van de rechten van de betrokkenen (zowel de melder als elke andere natuurlijke persoon van wie persoonsgegevens worden verwerkt in het kader van een melding). In het belang van de opvolging van de melding, de vertrouwelijkheid van het onderzoek en de geheimhouding ervan, hebben de beperkingen betrekking op de rechten bedoeld in de artikelen 14 – 16 AVG.
53. Artikel 23 AVG biedt de lidstaten de mogelijkheid de reikwijdte van de rechten van de betrokkenen te beperken, mits een dergelijke beperking de essentie van de fundamentele rechten en vrijheden eerbiedigt en in een democratische samenleving een noodzakelijke en evenredige maatregel is om een van de in artikel 23.1 AVG genoemde gerechtvaardigde doeleinden te verwezenlijken. Bovendien moet iedere wettelijke maatregel die voorziet in een dergelijke beperking voldoen aan de vormvereisten vastgesteld in artikel 23.2 AVG. Ter zake is de Autoriteit van oordeel dat, **voor zover er gevolg wordt gegeven aan de onderstaande opmerkingen**, er sprake is van een rechtmatige beperking van de rechten van de betrokkenen:

- de te verwerken categorieën van persoonsgegevens (minstens voor wat betreft de interne meldingen) nader preciseren in het ontwerp (zie ook de punten 35 – 38 en 50);
- specificeren van een uitdrukkelijke en bijzondere bewaartermijn voor de persoonsgegevens die het voorwerp uitmaken van de beperking;
- preciseren van de duurtijd van de beperkingen (op heden bepaalt artikel 26, §3, tweede lid, van het ontwerp louter wanneer de beperkingen aanvang (kunnen) nemen). Het is immers vereist dat de beperking van de rechten beperkt blijft tot wat strikt noodzakelijk is voor zowel de omvang **als de duur**²⁴.

54. Betreffende de ontbrekende elementen kan de aanvrager zich baseren op artikel 56, §2 e.v. van het ontwerp dat betrekking heeft op de beperking van de rechten van de betrokkenen in de context van interne of externe meldingen bij de geïntegreerde politiediensten²⁵.

ARTIKEL 27

55. Dit artikel betreft de omzetting van artikel 18 van de richtlijn en bepaalt dat de juridische entiteiten in de private²⁶ en publieke sector en de bevoegde autoriteiten een register moeten bijhouden van elke ontvangen melding. Deze meldingen mogen niet langer bewaard worden dan noodzakelijk en evenredig om te voldoen aan de vereisten overeenkomstig het ontwerp, de richtlijn of enige andere Europeesrechtelijke of nationale norm. De registratie moet gebeuren in overeenstemming met de in artikel 25 van het ontwerp vastgelegde geheimhoudingsvereisten en kan enkel de vorm aannemen van een opname van het gesprek of een nauwkeurig verslag van het onderhoud, opgesteld door de voor het behandelen van de melding verantwoordelijke personeelsleden. In elk geval moet de melder de mogelijkheid hebben om de schriftelijke weergave van de oproep, het verslag van het gesprek of het verslag van het onderhoud te controleren, te corrigeren en voor akkoord te tekenen.

56. Vooreerst wijst de Autoriteit erop dat de bewaartermijn overeenkomstig artikel 27, §1, van het ontwerp louter het beginsel van de beperking van de opslagtermijn van persoonsgegevens herhaalt en bijgevolg geen enkele bijkomende juridische meerwaarde heeft ten opzichte van

²⁴ Advies nr. 34/2018 van 11 april 2018 *inzake een voorontwerp van wet tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van Verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad 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* en meer in het bijzonder de punten 36 tot 38; Advies nr. 41/2018 van 23 mei 2018 *over een voorontwerp van wet houdende diverse financiële bepalingen*; Advies nr. 88/2018 van 26 september 2018 *over een ontwerp van besluit van de Vlaamse Regering houdende aanpassing van de besluiten van de Vlaamse Regering aan 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 (algemene verordening gegevensbescherming)*, en meer in het bijzonder de punten 17 tot 31.

²⁵ Zoals dit tevens bevestigd wordt in punt 66 van dit advies is de Autoriteit van oordeel dat de desbetreffende beperking van de rechten van de betrokkenen voldoet aan de vereisten neergelegd in artikel 23 AVG.

²⁶ Zie in dat verband het advies nr. 69/2022.

artikel 5.1.e) AVG. Deze 'bewaartermijn' schendt aldus het overschrijfverbod en dient geschrapt te worden. Zoals reeds toegelicht in punt 51 moet in het ontwerp een maximale bewaartermijn worden voorzien voor alle gegevens die worden verwerkt naar aanleiding van de registratie en opvolging van een melding. Vervolgens bepaalt artikel 27, §5, van het ontwerp in dat kader: *"Alle relevante documenten in het kader van een onderzoek van een melding door een intern of extern meldkanaal met name meldingen, zoals vermeld in artikel 6, 10° van de wet, de schriftelijke verklaringen voor de onderzoekers en de onderzoeksrapporten dienen gedurende een periode van tien jaar bijgehouden te worden.*

De bewaartermijn uit het eerste lid is niet van toepassing op de persoonsgegevens die in de rapporten, schriftelijke verklaringen en meldingen vervat zitten. Onverminderd de toepassing van artikel 26, bewaart de gegevensverantwoordelijke persoonsgegevens slechts voor de duur van het onderzoek tenzij:

1° er gerechtelijke procedures of tuchtmaatregelen worden ingeleid tegen de beklaagde of de melder;

2° de melder zijn gegevens zelf heeft bekendgemaakt in overeenstemming met artikel 25 van de wet."

57. Hoewel de Autoriteit akte neemt van de algemene bewaartermijn (gegevens worden gewist na de voltooiing van het onderzoek), formuleert zij de volgende opmerkingen met betrekking tot de uitzonderingen:
- in punt 1° dient gepreciseerd worden dat in die gevallen de persoonsgegevens bewaard moeten worden totdat de betrokken procedures en de termijnen om in beroep te gaan afgelopen zijn;
 - in punt 2° dient alsnog een maximale bewaartermijn te worden vastgesteld. Het feit dat bepaalde gegevens door de melder zelf werden bekendgemaakt is geen vrijgeleide om deze gegevens onbeperkt te bewaren.
58. Daarnaast stelt de Autoriteit vast dat het op heden niet duidelijk is 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.

HOOFDSTUK 7 (ARTIKELEN 28 – 42)

59. Hoofdstuk 7 van het ontwerp heeft betrekking op de beschermingsmaatregelen, en wordt onderverdeeld in de volgende afdelingen: verbod op represailles, ondersteuningsmaatregelen, de bescherming tegen represailles, maatregelen ter bescherming van de betrokkene en sancties.
60. Overeenkomstig artikel 30 van het ontwerp wordt het Federaal instituut voor de bescherming en de bevordering van de Rechten van de Mens (FIRM) belast met onder andere de volgende opdrachten: toepassen van, of toezien op de toepassing van de ondersteuningsmaatregelen vermeld in artikel 29, §1, 1^o, en 3^o tot 5^o, van het ontwerp, en artikel 29, §1, 2^o, van het ontwerp bij ontstentenis van een bevoegde autoriteit of indien de bevoegde autoriteit niet in staat is deze maatregelen toe te passen of ervoor te zorgen dat ze worden toegepast. De Autoriteit wijst erop dat indien de uitvoering van deze opdrachten aanleiding geeft tot een verwerking van persoonsgegevens, het FIRM aangemerkt moet worden als verwerkingsverantwoordelijke. Ten behoeve van de transparantie en teneinde uitoefening van de rechten van de betrokkenen (waaronder niet alleen de melder, maar tevens de personen die represailles hebben genomen (of daarvan verdacht worden), zoals neergelegd in de artikelen 12 – 22 AVG, te vergemakkelijken, is het aangewezen om dit uitdrukkelijk op te nemen in het ontwerp.
61. Voor het overige geven de beschermingsmaatregelen *an sich* geen aanleiding tot bijzondere opmerkingen betreffende de verwerking van persoonsgegevens.

HOOFDSTUK 8 (ARTIKELEN 43 – 65)

62. Tot slot voorziet hoofdstuk 8 van het ontwerp – onder voorbehoud van het advies van het COC – in een (gedeeltelijk) *lex specialis* regime ten aanzien van de meldingskanalen bij de geïntegreerde politie²⁷.
63. Aangezien de lokale politie ressorteert onder de lokale overheden en hun voogdijoverheden, valt de geïntegreerde politie niet onder de definitie van een federale overheidsinstantie. Desalniettemin, gelet op het eenheidsstatuut dat geldt binnen de geïntegreerde politie, dient een uniform wettelijk kader te worden vastgelegd voor het geheel van de geïntegreerde politiediensten. Om die reden wordt binnen het ontwerp een apart hoofdstuk uitgewerkt voor deze diensten, waarin rekening gehouden wordt met de eigenheid van de politiediensten en waarbij de principes van de richtlijn maximaal geïntegreerd worden in de reeds bestaande controleprocedures en – mechanismen. Daartoe wordt in het bijzonder aandacht besteed aan de uitwerking van het

²⁷ De federale politie en de lokale politie vormen samen de geïntegreerde politie, gestructureerd op twee niveaus.

interne meldkanaal, waarbij duidelijkheid en laagdrempeligheid voor de potentiële melder en objectiviteit van de eventuele opvolging centraal staan.

64. Vooreerst dient opgemerkt te worden dat krachtens artikel 43 van het ontwerp, de artikelen 2, 3, §§2 tot 4, 4 (inzake het materiaal toepassingsgebied), 5, §§1 en 3 (inzake het personeel toepassingsgebied), 6, 5°, 8° tot 11°, 13° tot 18°, 21°, 23° en 24° (definities), 7, §§1, 3 en 4 (inzake de voorwaarden voor bescherming van de melders), 12 (inzake de procedures voor interne melding en opvolging), 14, §§3 en 4, 1° tot 7°, 15 tot 22 (inzake de externe meldingen en opvolging), 24 (openbaarmaking) en 25 tot 27 (inzake de geheimhoudingsplicht, de verwerking van persoonsgegevens en de registratie van de meldingen) van het ontwerp, overeenkomstig van toepassing zijn op dit hoofdstuk. Ter zake benadrukt de Autoriteit dat de opmerkingen die werden geformuleerd ten aanzien van voormelde artikelen *mutatis mutandis* gelden voor de geïntegreerde politie.
65. Onverminderd de opmerkingen inzake de verwerking van persoonsgegevens (zie daartoe in het bijzonder de punten 44 – 58), is de Autoriteit van oordeel dat de bijzondere regelgeving betreffende de interne meldingskanalen bij de geïntegreerde politiediensten zoals neergelegd in de artikelen 46 – 51 en 53 – 56 van het ontwerp geen aanleiding geeft tot bijkomende opmerkingen. De Autoriteit laat zich daarentegen gunstig uit over de uitdrukkelijke aanduiding van de verwerkingsverantwoordelijke in dit kader²⁸.
66. Met betrekking tot de beperking van de rechten van de betrokkenen overeenkomstig artikel 56, §2 e.v. van het ontwerp stelt de Autoriteit vast dat is voldaan aan de vormvereisten neergelegd in artikel 23.2 AVG.

**OM DEZE REDENEN,
de Autoriteit,**

formuleert de volgende opmerkingen met betrekking tot het ontwerp:

- vaststellen van de concrete en precieze doeleinden van de verwerking van persoonsgegevens (punten 10 – 11 en 49);

²⁸ Artikel 56, §1, tweede en derde lid, van het ontwerp bepaalt: "Voor wat betreft de interne meldingskanalen van de lokale politie is de korpchef de verwerkingsverantwoordelijke.

Voor wat betreft het interne meldingskanaal van de federale politie is de commissaris-generaal de verwerkingsverantwoordelijke."

- het recht om een anonieme melding te doen beperken tot de gevallen waar de risico's voor de melder duidelijk opwegen tegen de potentieel nadelige gevolgen voor de in de melding geviseerde personen (punten 19 – 20);
- uitdrukkelijk vaststellen dat de federale overheidsinstanties optreden als verwerkingsverantwoordelijke met betrekking tot de gegevens die worden verwerkt in het kader van interne meldingen (punten 25 – 27);
- aanduiden dat de federale ombudsman, het Comité P, of het Comité I, wanneer zij dienstdoen als extern meldingskanaal, optreden als verwerkingsverantwoordelijke ten aanzien van de gegevens die in dat kader worden verwerkt (punt 31);
- de bewoording van artikel 14, §2, laatste lid, van het ontwerp aanpassen overeenkomstig punt 33;
- preciseren van de verhouding tussen de ontvangende autoriteiten en de bevoegde autoriteiten in het geval van overdracht of kennisgeving van meldingen (punt 34);
- nader preciseren van de (categorieën van) persoonsgegevens die verwerkt kunnen worden in het kader van een interne melding (en in de mate van het mogelijke, de openbaarmaking) (punten 38 en 50);
- uitdrukkelijk speciëren welke handelingen een vrije en uitdrukkelijk toestemming constitueren in de zin van het ontwerp (punt 45);
- schrappen van artikel 26, §1, van het ontwerp (punt 48);
- voorzien in een maximale bewaartermijn van de persoonsgegevens die kunnen worden verwerkt in het kader van de opvolging van een melding, of toch minstens de criteria opnemen die toelaten deze bewaartermijn te bepalen (punt 51);
- de bij artikel 26, §2 e.v., van het ontwerp voorziene beperking van de rechten van de betrokkenen in overeenstemming brengen met de vormvereisten neergelegd in artikel 23.2 AVG (punten 52 – 54);
- de bewaartermijnen die gelden ten aanzien van het register van de meldingen verder uitwerken overeenkomstig de punten 56 – 57;
- nader preciseren van zowel de doeleinden als de vorm (inhoud) van het meldingenregister (punt 58).

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