Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 69/2022 van 22 april 2022

Betreft: Advies m.b.t. 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* (CO-A-2022-059)

Het Kenniscentrum van de Gegevensbeschermingsautoriteit (hierna: de Autoriteit), aanwezig mevrouw Marie-Hélène Descamps 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 de heer Pierre-Yves Dermagne, Vice-eersteminister en minister van Economie en Werk, (hierna: de aanvrager) ontvangen op 03/03/2022;

brengt op 22 april 2022 het volgend advies uit:

I. VOORWERP VAN DE ADVIESAANVRAAG

1. Op 03/03/2022 verzocht de aanvrager het advies van de Autoriteit met betrekking tot het 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* (hierna: het ontwerp) (in het bijzonder de artikelen 9, §2, 13, 15, 16, 19, 21 – 23 en 32).

2. Het ontwerp betreft (in hoofdzaak[1]) 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). 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, met behoud van bepaalde specifieke kenmerken die verband houden met de gereglementeerde sectoren. Daarnaast worden ook gemeenschappelijke minimumnormen voor bescherming vastgesteld op bepaalde gebieden van Europees beleid waar er behoefte is aan krachtigere handhaving; waar de niet-melding van mistoestanden de handhaving in het gedrang brengt en waar de inbreuken tot ernstige schade voor het algemeen belang kunnen leiden. In toepassing van artikel 2.2 van de richtlijn werd er in het ontwerp, omwille van doeltreffendheid en rechtszekerheid, voor geopteerd om de bescherming voor melders onverkort toe te passen in alle door de richtlijn geviseerde gebieden, te weten:

   "i) overheidsopdrachten;
   ii) financiële diensten, producten en markten en voorkoming van witwassen van geld en terrorismefinanciering;
   iii) productveiligheid en product;
   iv) veiligheid van het vervoer;
   v) bescherming van het milieu;
   vi) stralingsbescherming en nucleaire veiligheid;
   vii) veiligheid van levensmiddelen en diervoeders, diergezondheid en dierenwelzijn;
   viii) volksgezondheid;
   ix) consumentenbescherming;
   x) bescherming van de persoonlijke levenssfeer en persoonsgegevens, en beveiliging van netwerk- en informatiesystemen;
   xi) bestrijding van belastingfraude;
   xii) sociale fraudebestrijding.[2]*"*

[1] Artikel 1 van het ontwerp omschrijft een groot aantal bijkomende richtlijnen en verordeningen dewelke door het ontwerp worden omgezet, dan wel uitgevoerd.

[2] Zie artikel 2 van het ontwerp. Artikel 3 van het ontwerp identificeert voor elk gebied de toepasselijke nationale en Europeesrechtelijke regelgeving.

3. Het ontwerp doet geen afbreuk aan de bepalingen inzake het melden van inbreuken die reeds van kracht zijn overeenkomstig het nationale of Europese recht[3]. Het beoogt daarentegen het toepassingsgebied van dergelijke beschermingsregimes in belangrijke mate uit te breiden (in overeenstemming met de richtlijn).

4. Binnen dit kader geeft het ontwerp aldus aanleiding tot de verwerking van persoonsgegevens van de melders en elke andere betrokkene en derde die in de melding wordt vermeld, hetzij – bij een interne signalering – door het bedrijf waarvoor zij werkzaam zijn, hetzij door de bevoegde autoriteiten en/of de federale ombudsman (coördinator) bij een externe signalering.

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) 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] Dergelijke meldingssystemen bestaan vandaag de dag reeds in de financiële sector (via de FSMA en de NBB) en, eerder beperkt, in het arbeidsrecht (antidiscriminatiewetgeving en de welzijnswet). Ook in de openbare sector bestaan er mechanismes voor het melden van inbreuken in de strijd tegen corruptie. Voor een uitgebreide toelichting ter zake verwijst de Autoriteit naar de Memorie van toelichting bij het ontwerp.

6. De ter advies voorgelegde regeling 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 geviseerde 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.

III. ARTIKELSGEWIJZE 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 van het ontwerp wordt bepaald dat de wet tot doel heeft "de tenuitvoerlegging van het Unierecht en -beleid op specifieke gebieden te verbeteren door de vaststelling van gemeenschappelijke minimumnormen die zorgen voor een hoog niveau van bescherming van melders van inbreuken op het Unierecht. Zij voorziet in de 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 met betrekking tot de juridische entiteiten in de private sector in het licht van de verplichtingen van de federale regering*."

10. Ter zake merkt de Autoriteit evenwel op dat, in tegenstelling tot wat wordt beweerd in het aanvraagformulier, het doeleinde van de wet niet zonder meer gelijk is aan het doeleinde van de door het ontwerp geïntroduceerde verwerking(en) van persoonsgegevens. Het doeleinde van de gegevensverwerking bij een melding moet daarentegen worden afgeleid uit de artikelen 11 – 13, 14 – 16, 19 en 20 van het ontwerp; namelijk het ontvangen en opvolgen 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.

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 gespecifieerd.

ARTIKELEN 2 – 6

12. De artikelen 2 – 6 van het ontwerp omschrijven het materieel toepassingsgebied van de wet (artikel 2 bepaalt de gebieden waarbinnen een beroep kan worden gedaan op een bescherming voor melders; artikel 3 specifieert de concrete reglementaire bepalingen voor elk van deze gebieden; de artikelen 4 en 5 verduidelijken dat het ontwerp geen afbreuk doet aan de reeds van kracht zijnde regels betreffende het melden van inbreuken in bepaalde sectoren; tot slot bepaalt artikel 6 de gebieden die buiten het toepassingsgebied van de wet vallen).

13. Ter zake kan worden opgemerkt dat de Belgische wetgever gebruik heeft gemaakt van de door artikel 2.2 van de richtlijn toegekende manoeuvreerruimte om het toepassingsgebied van het beschermingsregime uit te breiden tot alle handelingen die binnen de in artikel 2 opgesomde gebieden vallen[4] (en aldus niet te beperken tot de handelingen die uitdrukkelijk worden gespecifieerd in de bijlage bij de richtlijn).

14. De bepalingen inzake het materieel toepassingsgebied geven geen aanleiding tot bijzondere opmerkingen betreffende de verwerking van persoonsgegevens.

ARTIKEL 7

15. Artikel 7 bepaalt het personeel toepassingsgebied van het ontwerp. In overeenstemming met artikel 4 van de richtlijn is het beschermingsregime van toepassing op natuurlijke personen die in een werkgerelateerde context kennis krijgen van informatie over inbreuken. Het gaat daarbij minstens over (vroegere, huidige en toekomstige) werknemers, zelfstandigen, aandeelhouders en personen die behoren tot het bestuurlijk, leidinggevend of toezichthoudend orgaan van een onderneming, vrijwilligers en bezoldigde of onbezoldigde stagiairs, en eenieder die werkt onder toezicht en leiding van aannemers, onderaannemers en leveranciers. In voorkomend geval wordt

[4] De redenen daarvoor worden uitvoerig toegelicht in de Memorie van toelichting bij het ontwerp.

het beschermingsregime uitgebreid tot "*facilitators*[5]*; 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"*.

16. Ook de regels inzake het personeel toepassingsgebied van het ontwerp geven geen aanleiding tot bijzondere opmerkingen betreffende de verwerking van persoonsgegevens.

ARTIKEL 9

17. Artikel 9, §1, van het ontwerp bepaalt de voorwaarden waaraan een melder moet voldoen om in aanmerking te komen voor bescherming in de zin van hoofdstukken 6 en 7 van het ontwerp. De melders zullen met name moeten kunnen aantonen dat; *"(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 13 of extern overeenkomstig artikel 16 informatie meldden, of informatie openbaar maakten overeenkomstig artikel 20."*

18. 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 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*

[5] Artikel 8, 10°, van het ontwerp: *""facilitator": een natuurlijke persoon die een melder bijstaat in het meldingsproces en wiens bijstand vertrouwelijk moet zijn".* De Memorie van toelichting bij het ontwerp verklaart in dat opzicht tevens 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 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."*

motieven van de melders om te melden moeten losstaan van de beslissing of zij bescherming moeten krijgen[6]". 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*[7]".

19. 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.

20. Artikel 9, §2, bepaalt vervolgens dat juridische entiteiten in de private sector (behoudens deze met minder dan 250 werknemers), de bevoegde autoriteiten en de federale coördinator ertoe gehouden zijn om anonieme meldingen van inbreuken te ontvangen en te verzekeren dat ze worden opgevolgd. In eerste instantie vraagt de Autoriteit zich af welke de beweegredenen zijn van de Belgische wetgever om het recht om (intern) een anonieme melding te doen zich beperkt tot de werknemers van ondernemingen met meer dan 250 werknemers. Deze verschillende behandeling moet in het licht van artikel 10 en 11 van de Grondwet objectief kunnen worden verantwoord. Dit neemt niet weg dat de Autoriteit van mening is dat een anonieme melding optioneel en uitzonderlijk moet blijven. Niet alleen bemoeilijkt een dergelijke werkwijze de communicatie tussen de melder en de bestemmeling van de melding (dewelke nodig is voor een passende opvolging), bovendien kan dit aanleiding geven tot misbruiken in hoofde van de melders en daarmee gepaard gaande ongeoorloofde verwerking van persoonsgegevens. Hoewel de eindverantwoordelijkheid met betrekking tot de verwerking van persoonsgegevens steeds rust bij de respectieve verwerkingsverantwoordelijken (de onderneming bij een interne melding/ de bevoegde autoriteiten of federale coördinator voor de externe meldingen), dient ook de melder de nodige verantwoordelijkheidszin aan de dag te leggen; een melding kan immers belangrijke gevolgen hebben voor de geviseerde personen. De melder mag geen drempel ervaren om een melding te doen, doch, indien de anonieme melding de norm wordt, glijdt men af naar een verklikkingscultuur en de uitwassen die daarmee gepaard gaan. Het valt dan ook te betreuren – een dergelijke verplichting vloeit immers niet voor uit de richtlijn – dat de aanvrager ervoor heeft geopteerd om te voorzien in een veralgemeend recht om een anonieme melding te doen.

[6] Zie overweging 32 van de richtlijn.

[7] Zie overweging 33 van de richtlijn.

21. In het licht van het proportionaliteits- en evenredigheidsbeginsel lijkt het daarentegen 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 potentiële nadelige gevolgen voor de in de melding geviseerde personen.

ARTIKELEN 11 – 13

22. De voormelde artikelen hebben betrekking op de verplichting voor juridische entiteiten in de private sector (behoudens sommige onderneming met minder dan 50 werknemers[8]) om interne meldingskanalen op te zetten en de procedures voor interne melding en opvolging.

23. In lijn met artikel 8.1 van de richtlijn kunnen de interne meldingskanalen en -procedures slechts worden opgezet na overleg en in samenspraak met de sociale partners. De Autoriteit onderschrijft ter zake de motivatie van de aanvrager, in die zin dat een dergelijk overleg effectief kan bijdragen tot de doeltreffendheid (lees: geloofwaardigheid) van het opgezette meldingssysteem. In dezelfde lijn kan gewezen worden 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*[9] van de Commissie voor de bescherming van de persoonlijke levenssfeer, de rechtsvoorganger van de Autoriteit, waarin werd onderstreept dat een dergelijke overleg moet plaatsvinden met naleving van de wetgeving inzake het collectief arbeidsrecht. Daarnaast ziet de Autoriteit er op het eerste gezicht geen graten in dat het de ondernemingen vrij staat om deze kanalen en procedures ook open te stellen voor andere personen dan werknemers; zelfstandigen, aandeelhouders en personen belast met het dagelijks bestuur, aannemers en personen wier werkrelatie reeds beëindigd is. Immers, aangezien er geen verplichting bestaat om een trapsgewijze procedure te volgen (zie *supra* punt 18), 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. Overeenkomstig artikel 12, §3, van het ontwerp moeten de personen of afdelingen binnen een juridische entiteit in de private sector die bevoegd zijn voor het ontvangen en opvolgen van melding onafhankelijk zijn en mag er geen sprake zijn van belangenconflicten. Zoals destijds reeds

---

[8] In dit kader verduidelijkt de Memorie van toelichting: *"Een dergelijke drempel heeft tot doel rekening te houden met de omvang van de ondernemingen (overweging nr. 48 van de richtlijn) en met de implementatiekosten. In het geval van kleine en micro-ondernemingen lijkt het immers beter en redelijker dat de melder zich rechtstreeks tot de bevoegde autoriteiten wendt (externe melding)."*

[9] Te raadplegen via: https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-1-2006.pdf.

bevestigd door de Commissie voor de bescherming van de persoonlijke levenssfeer[10], 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.

25. 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 door 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 verwerking[11].

26. In beginsel zal het steeds de onderneming zelf zijn die optreedt als verwerkingsverantwoordelijke. Werknemers die binnen een organisatie toegang hebben tot persoonsgegevens worden als dusdanig louter beschouwd 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 rol[12]. Teneinde elke onduidelijkheid hieromtrent te vermijden, vraagt de Autoriteit om uitdrukkelijk in het ontwerp te specifiëren dat wanneer het meldingsbeheer wordt waargenomen door (een) werknemer(s) van de onderneming, de onderneming optreedt als verwerkingsverantwoordelijke.

27. Ook wanneer de onderneming overeenkomstig het ontwerp beroep doet op een derde voor het beheer van het meldingskanaal zal het de onderneming zijn die optreedt als verwerkingsverantwoordelijke (en de derde louter als verwerker). Het feit dat verschillende ondernemingen beroep zouden doen op eenzelfde derde[13] doet hieraan geen afbreuk.

---

[10] Zie ter zake de voormelde aanbeveling nr. 01/2006.

[11] Zowel de Europees Comité voor gegevensbescherming als de Autoriteit hebben benadrukt dat het concept verwerkingsverantwoordelijke vanuit een feitelijk perspectief moet worden benaderd. Zie: Europees Comité voor gegevensbescherming, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 1.0, adopted on 02 september 2020, p 10 et s (https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en) 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,* blz.1 (https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Begrippen_VW_OA.pdf).

[12] Dit wordt bevestigd in de richtsnoeren 07/2020 van de EDPB *over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG*. Te raadplegen via: https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_nl.pdf.

[13] Artikel 12, §4, derde lid, van het ontwerp bepaalt in dat kader: "*Juridische entiteiten in de private sector met minder dan 250 werknemers mogen middelen delen voor het in ontvangst nemen van meldingen en eventueel te verrichten onderzoeken. Dit*

28. Het bovenstaande laat uiteraard onverlet de geheimhoudingsplicht in hoofde van de ontvangers van meldingen/ meldingsbeheerders overeenkomstig artikel 21 van het ontwerp en de sancties waaraan zij zich bij een schending van deze verplichting blootstellen (zie artikel 33, §2 van het ontwerp).

29. Tot slot bepaalt artikel 13 van het ontwerp de modaliteiten van de procedures voor interne melding en opvolging. De concrete elementen van de procedure kunnen nader worden uitgewerkt door de bevoegde autoriteiten, in overleg met de federale coördinator, door middel van een reglement of rondzendbrief. Bij gebrek hieraan worden deze bepaald door de Koning. Deze reglementen of rondzendbrieven zijn bindend en moeten worden bekendgemaakt op de websites van de bevoegde autoriteiten. De Autoriteit stelt zich evenwel vragen bij het bindend karakter van dergelijke documenten. 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 regelementen worden dus bij voorkeur vastgesteld in een koninklijk besluit. Daarnaast kunnen verenigingen en andere instellingen die categorieën van juridische entiteiten in de private sector vertegenwoordigen gedragscodes opstellen, wijzigen of verlengen, teneinde de juiste toepassing van het ontwerp te verzekeren. In dit kader wijst de Autoriteit op richtsnoeren van de Europese Toezichthouder voor gegevensbescherming (EDPS) (EDPS, *Guidelines on processing personal information within a whistleblowing procedure*, december 2019[14]) 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 nationale instanties of autoriteten en private ondernemingen.

30. Volledigheidshalve nog benadrukt de Autoriteit dat de systemen die binnen de onderneming worden opgezet in elk geval moeten voldoen aan de vereisten van gegevensbescherming door ontwerp en door standaardinstellingen in de zin van artikel 25 AVG.

ARTIKELEN 14 – 17 en 19

31. De voormelde artikelen omschrijven de modaliteiten van en de procedures voor de externe meldingskanalen.

doet geen afbreuk aan de verplichtingen die deze wet aan dergelijke entiteiten oplegt in verband met geheimhouding, het verstrekken van feedback en het behandelen van de gemelde inbreuk."

[14] Te raadplegen via: https://edps.europa.eu/sites/default/files/publication/19-12-17_whisteblowing_guidelines_en.pdf.

32. Ten algemene titel merkt de Autoriteit op dat de bevoegde autoriteiten, en bij gebreke daaraan de federale ombudsman (de federale coördinator), – al naargelang het geval in overeenstemming met de bepalingen van het ontwerp – optreden als verwerkingsverantwoordelijke voor wat betreft de verwerking van persoonsgegevens in het kader van het ontvangen en opvolgen van externe meldingen.

33. In principe treedt de federale ombudsman louter op als coördinator voor de externe meldingen afkomstig uit de private sector; hij staat in voor het onderzoek van de ontvankelijkheid van de melding en de gebeurlijke doorverwijzing naar een bevoegde autoriteit. Indien er evenwel geen bevoegde autoriteit is, of de bevoegde autoriteit aangeeft niet in staat te zijn om de opvolging uit te voeren, zal de federale coördinator de externe meldingen ten gronde behandelen. Indien een melding rechtstreeks bij een bevoegde autoriteit wordt gedaan, brengt deze autoriteit de federale coördinator op de hoogte. De bevoegde autoriteit kan de melding ook overmaken aan een andere autoriteit indien hij vaststelt niet bevoegd te zijn. Welke de concrete uitkomst ook is, de melder, behoudens wanneer dit ingevolge een anonieme klacht niet mogelijk is, moet steeds op de hoogte worden gebracht.

34. Het verdient aanbeveling om in het ontwerp, of desgevallend naderhand in een bindend regelement in de zin van artikel 15, §5 van het ontwerp, de concrete verhouding vast te stellen tussen de bevoegde autoriteiten en de federale coördinator. Meer concreet moet worden uitgeklaard wanneer, en onder welke voorwaarden de bevoegde autoriteiten en de federale coördinator optreden als verwerkingsverantwoordelijke, dan wel als verwerker of gezamenlijke verwerkingsverantwoordelijke[15].

35. Naar analogie met de procedureregels voor interne meldingen herneemt de Autoriteit haar opmerkingen overeenkomstig de punt 30.

36. Betreffende de opzet van de externe meldingskanalen (artikel 16 van het ontwerp) stelt de Autoriteit vast dat het een quasi letterlijke omzetting betreft van artikel 12 van de richtlijn. Een enkel verschil betreft §6 van artikel 16 dat de geheimhoudingsplicht overeenkomstig artikel 21 van het ontwerp uitdrukkelijk van toepassing maakt op de personeelsleden van de bevoegde autoriteiten en de federale coördinator. De Autoriteit neemt er akte van.

[15] 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*

ARTIKEL 20

37. Artikel 20, §1, bepaalt de voorwaarden, naast degene die reeds zijn neergelegd in artikel 9 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 13, paragraaf 1, 6°, of artikel 15, paragraaf 2, 4°, genoemde termijn; of*
2° in geval van een directe openbaarmaking: de persoon heeft gegronde redenen om aan te nemen dat:
a) de inbreuk 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 inbreuk 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 inbreuk of bij de inbreuk betrokken is."

38. Voorts bepaalt §2 van datzelfde artikel 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.

39. Tot slot bepaalt artikel 33, §3 van het ontwerp in dit kader dat; "*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 geviseerde 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.

40. Voor het overige formuleert de Autoriteit geen opmerkingen met betrekking tot de openbaarmaking.

ARTIKEL 21

41. Artikel 21 van het ontwerp zet artikel 16 van de richtlijn om, dat een geheimhoudingsplicht in hoofde van de ontvangers van meldingen/ meldingsbeheerders vaststelt. Deze geheimhoudingsplicht heeft niet alleen betrekking op de identiteit van de melder, maar wordt overeenkomstig artikel 32 van het ontwerp uitgebreid tot de identiteit van de personen aan wie de inbreuk wordt toeschreven of met wie de inbreuk in verband wordt gebracht (hierna: de betrokkenen) (zolang de onderzoeken lopen).

42. De identiteit van de melder en van de betrokkenen gedurende de looptijd van de onderzoeken mag in geen geval bekend worden gemaakt zonder hun vrije en uitdrukkelijk toestemming aan anderen dan de gemachtigde personeelsleden die bevoegd zijn voor de ontvangst of opvolging van meldingen. Ter zake vraagt de Autoriteit om in het ontwerp uitdrukkelijk te specifiëren 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 AVG[16].

43. In afwijking van de algemene regel mogen de identiteit van de melder (en van de betrokkenen) *"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 worden zij daarvan in kennis gesteld, tenzij die informatie de gerelateerde onderzoeken of gerechtelijke procedures in het gedrang zou brengen. Ter illustratie verduidelijkt de Memorie van toelichting in dat kader dat de algemene regels en verplichtingen inzake bestuurlijke transparantie op zich geen rechtvaardigingsgrond vormen om van de geheimhoudingsplicht af te wijken. 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, lid 4, AVG, gelezen in samenhang met artikel 57, lid 1, c), en overweging 96 van diezelfde verordening, eerst ter advies moet worden voorgelegd aan de Autoriteit.

[16] 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.

ARTIKEL 22

44. Artikel 22 handelt over de verwerking van persoonsgegevens en bepaalt daartoe het volgende: *"Elke verwerking van persoonsgegevens krachtens deze wet, met inbegrip van de uitwisseling of doorgifte van persoonsgegevens door de bevoegde autoriteiten of de federale coördinator, gebeurt in overeenstemming met Verordening (EU) 2016/679 en de wettelijke bepalingen inzake de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens. Elke uitwisseling of doorgifte van informatie door de instellingen, organen of instanties van de Unie gebeurt volgens Verordening (EU) 2018/1725.*

Persoonsgegevens die duidelijk niet relevant zijn voor de behandeling van een specifieke melding, worden niet verzameld*, of worden, indien onbedoeld verzameld, onmiddellijk gewist."*

45. De Autoriteit wijst erop dat het eerste lid van voormeld artikel geen enkele juridische meerwaarde heeft. De AVG is op iedere verwerking van persoonsgegevens van toepassing. De betrokken passage dient bijgevolg geschrapt te worden. Eenzelfde opmerking gaat op voor het eerste deel van het tweede lid (vetgedrukt) dat louter een parafrasering van het proportionaliteitsbeginsel betreft en aldus aanleiding geeft tot een schending van het overschrijfverbod van de AVG[17]. Daarnaast, hoewel de Autoriteit onderschrijft dat niet relevante gegevens gewist moeten worden indien ze onbedoeld verzameld werden, vraagt ze zich af hoe dit in zijn werk zal gaan. In het bijzonder bij een schriftelijke klacht[18] lijkt het immers niet opportuun dat de persoon die de melding ontvangt naar eigen goeddunken bepaalde passages kan schrappen en/of anonimiseren zonder dat de melder daarvan op de hoogte is[19], of, in het geval van een anonieme klacht, kan worden gebracht. Het verdient aanbeveling om ter zake nadere procedureregels vast te stellen (bijvoorbeeld bij koninklijk besluit).

46. Meer algemeen met betrekking tot de verwerking van persoonsgegevens vraagt de Autoriteit in eerste instantie om in dit artikel de concrete en precieze doeleinden van de verwerking vast te stellen (zie daartoe de punten 10 – 11).

---

[17] 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. Italie (C-39/72), Recueil de jurisprudence, 1973, p. 101, § 17). Zie ook : HJEU 10 oktober 1973, Fratelli Variola S.p.A. c. Italiaanse Belastingsdienst (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.

[18] Bij een telefonische klacht kan er tijdens het gesprek reeds overleg plaatsvinden over welke gegevens al dan niet pertinent zijn.

[19] Dit kan immers problemen opleveren bij de verdere opvolging (bijvoorbeeld in het kader van (buiten)gerechtelijke procedures) van de melding.

47. Ten tweede is het noodzakelijk om in het ontwerp, desgevallend per sector of gebied, uitdrukkelijk vast te stellen welke (categorieën van) persoonsgegevens van de melder en, in voorkomend geval, van de facilitator(s) of elke andere derde die met de melder in verband staat verwerkt kunnen worden bij de registratie en opvolging van een melding (ter zake is de Autoriteit van oordeel dat dit beperkt kan blijven tot de naam en contactgegevens en in voorkomend geval de functie binnen de onderneming). Voor wat betreft de gegevens van de betrokkenen die afgeleid kunnen worden uit een melding kan er gespecifieerd worden 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.

48. Tot slot wijst de Autoriteit op de verplichting om in het licht van artikel 6.3 AVG 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 23, §1 van het ontwerp heeft immers louter betrekking op het register van de meldingen. 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.

ARTIKEL 23

49. Dit artikel betreft de omzetting van artikel 18 van de richtlijn en bepaalt dat de juridische entiteiten in de private 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 21 vastgelegde geheimhoudingsvereisten en kan enkel de vorm aannemen van een opname van het gesprek of een nauwkeuring verslag van het onderhoud, opgesteld door de voor het behandelen van de melding verantwoordelijke personeelsleden.

50. Vooreerst wijst de Autoriteit erop dat de bewaartermijn overeenkomstig artikel 23, §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

artikel 5.1.e) AVG. Deze 'bewaartermijn' schendt aldus het overschrijfverbod en dient geschrapt te worden. Zoals reeds toegelicht in punt 48 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. Indien de aanvrager van oordeel is dat ten aanzien van de gegevens in het register een bijzondere bewaartermijn moet gelden, dan moet dit uitdrukkelijk vastgesteld worden in het ontwerp.

51. 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 elke onderneming of bevoegde autoriteit 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, de federale coördinator en de private ondernemingen… Deze elementen moeten in het ontwerp worden gepreciseerd. Op basis daarvan kunnen naderhand bijkomende richtlijnen of werkingsmodaliteiten worden vastgesteld.

52. Tot slot neemt de Autoriteit er akte van dat aan de melder steeds de mogelijkheid wordt geboden de schriftelijke weergave van het verslag van het onderhoud te controleren, te corrigeren en voor akkoord te tekenen.

OVERIGE OPMERKINGEN

53. Overeenkomstig artikel 26 van het ontwerp wordt het Federaal instituut voor de bescherming en de bevordering van de Rechten van de Mens (hierna: FIRM) belast met onder andere de volgende opdrachten: het toepassen van, of toezien op de toepassing van de ondersteuningsmaatregelen vermeld in artikel 25, §1, 1°, en 3° tot 5° van het ontwerp, en artikel 25, §1, 2° van het ontwerp bij ontstentenis van een bevoegde autoriteit of indien de bevoegde autoriteit niet in staat is deze maatregelen toe te passen. 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.

54. Dezelfde opmerking gaat op voor wat betreft de opdrachten die de federale coördinator uitoefent in het kader van de buitengerechtelijke procedure overeenkomstig artikel 26/1 van het ontwerp

voor de beslechting van conflicten tussen enerzijds melders die (beweren) slachtoffer (te) zijn van represailles en anderzijds de entiteiten en/of personen die represailles uitoefenen.

OM DEZE REDENEN,
de Autoriteit,

formuleert de volgende opmerkingen met betrekking tot het ontwerp:

- nader specifiëren van de beweegredenen om het recht om (intern) een anonieme melding te doen te beperken tot de werknemers van ondernemingen met meer dan 250 werknemers (punt 20);
- uitdrukkelijk vaststellen dat de ondernemingen optreden als verwerkingsverantwoordelijke met betrekking tot de gegevens die worden verwerkt via interne meldingen (punten 25 – 27);
- preciseren van de verhouding tussen de bevoegde autoriteiten en de federale ombudsman (coördinator) in het geval van overdracht of kennisgeving van meldingen (punt 34);
- uitdrukkelijk specifiëren welke handelingen een vrije en uitdrukkelijk toestemming constitueren in de zin van het ontwerp (punt 42);
- vaststellen van de concrete en precieze doeleinden van de verwerking van persoonsgegevens (punten 10 – 11 en 46);
- voorzien in een maximale bewaartermijn van de persoonsgegevens die kunnen worden verwerkt in het kader van zowel de registratie als de opvolging van een melding, of toch minstens de criteria opnemen die toelaten deze bewaartermijn te bepalen (punten 48 en 50);
- specifiëren van de (categorieën van) persoonsgegevens van de melder, de facilitator of elke andere derde verbonden met de melder en van de in de melding geviseerde personen die naar aanleiding van een melding verwerkt kunnen worden (punt 47);
- nader preciseren van zowel de doeleinden als de vorm (inhoud) van het meldingenregister (punt 51);
- aanduiden dat het FIRM en de federale coördinator optreden als verwerkingsverantwoordelijke voor wat betreft de verwerking van persoonsgegevens in het kader van hun respectieve opdrachten inzake ondersteuningsmaatregelen voor melders (punten 53 – 54).

Voor het Kenniscentrum,
(get.) Rita Van Nuffelen - Verantwoordelijke a.i. van het Kenniscentrum