Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 21/2024 van 23 februari 2024

Betreft: Advies m.b.t. voorontwerp van decreet *tot oprichting en regeling van het Vlaams Meldpunt voor Grensoverschrijdend Gedrag* (CO-A-2023-606)
Sleutelwoorden: beroepsgeheim – catch all bepaling – beveiliging – SharePoint als bewaarplaats voor de bijzondere categorieën gegevens – toestemming – verantwoordingsplicht om toestemming te bewijzen – objectieve criteria bewaartermijn – maximale bewaartermijn één jaar – bijzondere categorieën gegevens en proportionele beveiligingsmaatregelen – gradaties in toegankelijkheid – specificeren van categorieën betrokken en gegevens – gezamenlijke verwerkingsverantwoordelijkheid – onverenigbaarheid protocol

Het Kenniscentrum van de Gegevensbeschermingsautoriteit (hierna: de Autoriteit), aanwezig mevrouw Cédrine Morlière, mevrouw Nathalie Ragheno en mevrouw Griet Verhenneman en de 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 Zuhal Demir, Vlaams minister van Justitie en Handhaving, Omgeving, Energie en Toerisme, (hierna: de aanvrager) ontvangen op 26/12/2023;

brengt op 23 februari 2024 het volgend advies uit:

I. Kadering van de aandachtspunten:

1) Toepassingsgebied vereist verdere nauwkeurigheid
2) Vaststelling gezamenlijke verwerkingsverantwoordelijkheid
3) Onverenigbaarheid protocol voor de gezamenlijke verwerkingsverantwoordelijken
4) Het beginsel van de minimale gegevensverwerking en de proportionaliteit is over de hele lijn onvoldoende in acht genomen
5) Binnen het kader van integriteit, vertrouwelijkheid en beveiliging is verdere aandacht vereist m.b.t. verschillende graden van gemachtigde toegang, de uitzonderingen op het beroepsgeheim
6) Voorwaarden van een geldige toestemming en invoering van bewijsverplichting voor de verwerkingsverantwoordelijke
7) Rechten van de betrokkenen, m.n. de informatieverplichting
8) Bewaartermijn mag niet langer dan 1 jaar zijn, tenzij uitdrukkelijke motivering, en moet rekening houden met de aard van de gegevens

II. VOORWERP VAN DE ADVIESAANVRAAG

1. Op 26 december 2023 verzocht de aanvrager het advies van de Autoriteit met betrekking tot een voorontwerp van decreet *tot oprichting en regeling van het Vlaams Meldpunt voor Grensoverschrijdend Gedrag* (hierna: het ontwerp).

2. Het ontwerp beoogt grensoverschrijdend gedrag in de Vlaamse sectoren aan te pakken. Hiertoe wordt binnen het Agentschap Justitie en Handhaving (hierna: AJH) een onafhankelijke werking gecreëerd, het meldpunt AJH, als onderdeel van het Vlaams Meldpunt voor Grensoverschrijdend Gedrag.[1] Deze werking moet het mogelijk maken om grensoverschrijdend gedrag op een laagdrempelige wijze te kunnen melden. Om dit te bewerkstelligen wordt een samenwerking tussen het AJH en het Vlaams Mensenrechteninstituut (hierna: VMRI) voorzien.

3. Dit alles veronderstelt verwerking van persoonsgegevens door het AJH teneinde enerzijds *meldingen van grensoverschrijdend gedrag te ontvangen en er passende gevolgen aan te verbinden* en anderzijds *aanbevelingen formuleren* door het monitoren en in kaart brengen van de meldingen van grensoverschrijdend gedrag binnen de Vlaamse sectoren.

[1] MvT art. 5, al. 1: "*Het meldpunt AJH is een onderdeel van het Vlaams Meldpunt voor Grensoverschrijdend Gedrag binnen AJH en bestaat dus niet als afzonderlijk meldpunt noch aanspreekpunt, maar zal louter en alleen als onderdeel van het Vlaams Meldpunt voor Grensoverschrijdend Gedrag handelen.*"

III. ONDERZOEK TEN GRONDE

a. Rechtsgrond

- Algemene principes

4. Elke verwerking van persoonsgegevens moet een rechtsgrond of een rechtmatigheidsgrond hebben, zoals bepaald in artikel 6, lid 1, van de AVG. Gegevensverwerkingen die bij een normatieve maatregel zijn ingevoerd, zijn bijna altijd gebaseerd op artikel 6, lid 1, punt c) of e), van de AVG.[2]

5. Een norm die de verwerking van persoonsgegevens regelt (en die van nature een inmenging vormt in het recht op bescherming van persoonsgegevens) moet niet alleen noodzakelijk en evenredig zijn, maar ook voldoen aan de eisen van voorspelbaarheid en nauwkeurigheid, zodat de betrokkenen, over wie gegevens worden verwerkt, een duidelijk beeld krijgen van de verwerking van hun gegevens. Krachtens artikel 6.3 van de AVG, gelezen in samenhang met artikel 22 van de Grondwet en artikel 8 van het EVRM, moet dergelijke wettelijke norm de essentiële elementen van de met de overheidsinmenging gepaard gaande verwerkingen beschrijven. Het 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.

---

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

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

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

- Toepassing van deze principes

6. De verwerking van persoonsgegevens waartoe het voor advies voorliggende ontwerp aanleiding geeft, berust op artikel 6(1)(e) AVG.[3] De doeleinden van de verwerking en de te verwerken categorieën van persoonsgegevens, in aanmerking genomen, is de Autoriteit van oordeel dat er sprake is van een belangrijke inmenging in de rechten en vrijheden van de betrokkenen. Het betreft immers een verwerking van persoonsgegevens van kwetsbare natuurlijke personen die tevens ook betrekking kan hebben op bijzondere categorieën van persoonsgegevens (gevoelige gegevens) in de zin van de artikelen 9 en/of 10 van de AVG en/of hoogstpersoonlijke gegevens.

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

b. Doeleinden

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

9. Uit artikel 3, §1 lid 2, van het ontwerp volgt dat een onafhankelijk Vlaams Meldpunt voor Grensoverschrijdend Gedrag wordt opgericht met het oog op **de aanpak van grensoverschrijdend gedrag in de Vlaamse sectoren.** Het bepalen van het toepassingsgebied, zorgt *ipso facto* voor een verdere afbakening van het doeleinde. Doch moet het toepassingsgebied voldoende nauwkeurig omschreven zijn, zodat er sprake kan zijn van een 'welbepaalde' omlijning. Bijgevolg wordt de aandacht gevestigd op het materiële en personele toepassingsgebied van het ontwerp.

10. Wat het materiële toepassingsgebied betreft volgt uit artikel 2, 7°, van het ontwerp, dat:

> "*7° **grensoverschrijdend gedrag**: elke aantasting van de integriteit van een persoon wegens ongewenst seksueel gedrag, geweld, pesterijen of discriminerende intimidatie;*"

11. Hieronder vallen consequent ook meldingen aangaande artikel 2, 5°, 6°, 10°, 11° van het ontwerp, zoals hiernavolgend weergeven:

> "*5° **discriminerende intimidatie**: intimidatie als vermeld in artikel 17, §1, van het decreet van 10 juli 2008;*
>
> *6° **geweld**: elke feitelijkheid waarbij iemand psychisch of fysiek wordt bedreigd of aangevallen;*

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

*10° **ongewenst seksueel gedrag**: seksuele intimidatie als vermeld in artikel 17, §2, van het decreet van 10 juli 2008;*

*11° **pesterijen**: onrechtmatig geheel van verschillende, vergelijkbare of uiteenlopende, gedragingen die plaatsvinden gedurende een bepaalde tijd, en die tot doel of gevolg hebben dat de persoonlijkheid, de waardigheid of de fysieke of psychische integriteit van een persoon wordt aangetast, dat zijn betrekking in gevaar wordt gebracht of dat een bedreigende, vijandige, beledigende, vernederende of kwetsende omgeving wordt gecreëerd;*"[4]

12. Voorts stipuleert artikel 5, lid 5, van het ontwerp, het volgende:

"*Het meldpunt AJH is toegankelijk voor elke persoon met een melding over grensoverschrijdend gedrag in alle aangelegenheden die onder de bevoegdheden van de Vlaamse Gemeenschap en het Vlaams Gewest vallen.*"

13. Het materiële toepassingsgebied moet aldus als volgt worden begrepen: meldingen over een "*grensoverschrijdend gedrag*" in "*alle aangelegenheden die onder de bevoegdheden van de Vlaamse Gemeenschap en het Vlaams Gewest vallen.*"

14. Terzake specifieert artikel 5, vierde en vijfde alinea, van de Memorie van Toelichting:

"*Het is niet noodzakelijk dat het grensoverschrijdend gedrag in het kader van een organisatie wordt gesteld, het is **voldoende dat er een rechtstreekse link is met een bepaalde sector of organisatie.** Op die manier wordt grensoverschrijdend gedrag door bijvoorbeeld een freelance fotograaf of door een student op kot niet uitgesloten bij het toepassingsgebied van het decreet.*

***Organisaties is een ruim begrip waarmee ook ondernemingen, instellingen, voorzieningen**,… worden gevat.*"

15. De Autoriteit interpreteert het materiële toepassingsgebied als zijnde elke melding:
    - over een grensoverschrijdend gedrag (hetgeen gelet op de definities een uitermate verrijkende reikwijdte heeft);
    - die een "rechtstreekse" link moet hebben (om maar niet te zeggen enige, gelet op de brede interpretatie);
    - met "*[…] organisaties en sectoren die […] onder de bevoegdheid van de Vlaamse Gemeenschap of het Vlaams Gewest [vallen],*" waarbij expliciet aangegeven wordt dat organisaties geïnterpreteerd moet worden als een ruim begrip.

[4] Vet toegevoegd door de Autoriteit.

16. Concreet wil dit zeggen dat zolang het betrekking heeft op een "grensoverschrijdend gedrag" en er enige link is met de bevoegdheden van de Vlaamse Gemeenschap en het Vlaams Gewest, het geacht wordt ontvankelijk te zijn.

17. Het personele toepassingsgebied zoals voorzien in artikel 5, lid 5 van het ontwerp en weergeven in punt 12, **draagt niet bij tot een nauwere omkadering**. Aldus "*[is] het meldpunt toegankelijk voor elke persoon*." Zo specifieert de Memorie van Toelichting verder dat "*[h]et meldpunt […] zich in eerste instantie [richt] tot slachtoffers, maar de toegang […] daar niet toe beperkt [is]. In principe kunnen ook verwanten, getuigen, derden en organisaties en zelfs plegers een melding doen omtrent grensoverschrijdend gedrag.*" Bovendien volgt uit de Memorie van Toelichting dat "*[h]et meldpunt […] zich niet specifiek of alleen tot kinderen en jongeren [richt], maar ook zij […] terecht [kunnen] […].*" **Met andere woorden iedereen, van kinderen, jongeren tot volwassenen, zonder enige vorm van onderscheid.** Desalniettemin merkt de Autoriteit op dat hoewel het ontwerp en de Memorie van Toelichting nadrukkelijk aangeeft dat "elke persoon" beoogd wordt, niet anders dan geopperd kan worden dat de insteek voornamelijk van kinderen en jongeren uit vertrekt. Dit volgt onder meer uit stellingen zoals "*[d]it ontwerp van decreet vertrekt vanuit verschillende kinderrechten en basisbeginselen, vermeld in het kinderrechtenverdrag […]"* of nog *"vertrekt dus vanuit het belang van het kind en streeft een versterking van de hogervermelde kinderrechten na.*"

18. Onder de **aanpak** van grensoverschrijdend gedrag in de Vlaamse sectoren valt enerzijds de meldingen en het passend gevolg en anderzijds de beleidsadviezen, zoals voorzien in artikel 7, van het ontwerp, die de twee kernopdrachten uitlicht.

19. Ten eerste, **meldingen** van grensoverschrijdend gedrag **ontvangen en er een passend gevolg** aan verbinden. Overeenkomstig artikel 7, lid 2, van het ontwerp, kaderen volgende deelopdrachten binnen deze eerste overkoepelende opdracht:

> "*1° meldingen van grensoverschrijdend gedrag ontvangen en op basis daarvan aan vraag- en aanbodverheldering doen;*
> *2° gesprekken voeren met het oog op ondersteuning en erkenning;*
> *3° ondersteuning bieden en een melding van grensoverschrijdend gedrag en de daaropvolgende procedure binnen een specifieke sector of organisatie opvolgen;*
> *4° een warme doorverwijzing bieden naar een extern aanbod;*
> *5° een kortdurend psychologisch ondersteunend traject aanbieden;*
> *6° een juridisch consult aanbieden over de burgerrechtelijke, strafrechtelijke of tuchtrechtelijke mogelijkheden;*
> *7° bemiddelingsgesprekken en herstelgesprekken voeren.*"

20. Om dit te bewerkstelligen wordt een samenwerking voorzien tussen het meldpunt AJH en het VMRI – verdere bespreking in punten 104 t.e.m. 108.

21. Binnen dit kader verwerkt het meldpunt AJH en het VMRI overeenkomstig artikel 13, van het ontwerp, de gegevens van de "*melders*" en van "*de personen die betrokkenheid vertonen met de context van het grensoverschrijdend gedrag*" – verder toegelicht in punten 68 t.e.m. 71.

22. Het geheel in acht genomen, komt de Autoriteit tot het besluit dat het doeleinde uitdrukkelijk is en een gerechtvaardigd belang nastreeft. De aanvullende motivering van de aanvrager, m.b.t. het ruime toepassingsgebied, staaft de ruime invulling van het begrip "grensoverschrijdend gedrag" en bevestigt eerdere vaststelling omtrent het ruime kader van de bevoegdheden van de Vlaamse Gemeenschappen en Gewesten.[5] De Autoriteit, heeft begrip voor de beoogde opzet, m.n. het aanpakken van grensoverschrijdend gedrag. De ruime invulling van **de definiëring** van "grensoverschrijdend gedrag," kan gelet op de nauwkeurige en duidelijke motivering, **in lijn met artikel 5(1)(b) AVG** beschouwd worden. De Autoriteit is van mening dat de formulering "alle aangelegenheden die onder de bevoegdheden van de Vlaamse Gemeenschap en het Vlaamse Gewest vallen" niet volledig voldoet aan de vereiste van welbepaaldheid. Het feit dat de melding betrekking kan hebben op alle mogelijke aangelegenheden, zolang er maar een rechtstreekse link is, lijkt op een soort 'catch all bepaling'. Hierbij wordt benadrukt dat de nauwkeurigheidsvereiste enerzijds een waarborg vormt voor de voorspelbaarheid en de rechtszekerheid van de betrokkenen, en anderzijds noodzakelijk is voor de toepassing van andere vereisten met

[5] Op het verzoek van de Autoriteit voor een aanvullende motivering, naast het algemene doeleinde van 'de aanpak van grensoverschrijdend gedrag in de Vlaamse sectoren', die een dergelijk verreikend toepassingsgebied (materieel en personeel) rechtvaardigt, preciseerde de aanvrager het volgende: "*Het Meldpunt is bevoegd voor meldingen rond grensoverschrijdend gedrag in alle aangelegenheden die onder de bevoegdheden van de Vlaamse Gemeenschap en het Vlaams Gewest vallen.*

Grensoverschrijdend gedrag, zoals gedefinieerd in artikel 2, punt 7° van het voorontwerp, maakt altijd een aantasting uit van de integriteit van een persoon. Het recht op eerbiediging van de fysieke en psychische integriteit is een grondrecht dat, onder meer, vervat ligt in artikel 3 van het EU Handvest en artikel 22 van de Grondwet. De doelstelling van het Meldpunt om meldingen, op een laagdrempelige wijze, mogelijk te maken in functie van de aanpak van grensoverschrijdend gedrag in de Vlaamse sectoren betreft derhalve de bescherming van een grondrecht.

Het Meldpunt kan meldingen ontvangen in alle aangelegenheden die onder de bevoegdheden van de Vlaamse Gemeenschap en het Vlaamse Gewest vallen.

Artikel 7, lid 3, 4° van het voorontwerp bakent het toepassingsgebied strikt af door te bepalen dat meldingen die buiten de aangelegenheden vallen die tot bevoegdheden van de Vlaamse Gemeenschap en het Vlaamse Gewest behoren, niet ontvankelijk zijn. Deze bepaling bevestigt dat het toepassingsgebied van het voorontwerp bevoegdheidsconform moet worden gelezen (cf. de afbakening van het Gelijkekansendecreet en de bevoegdheden van het VMRI). Uit deze bepaling volgt dat het Meldpunt casus per casus zal moeten controleren of er sprake is van een melding die binnen de Vlaamse bevoegdheden valt, zoals afgebakend in de Grondwet en de Bijzondere Wet tot hervorming der instellingen.

Luidens de Bijzondere Wet tot hervorming der instellingen is de Vlaamse Gemeenschap en het Vlaamse Gewest bevoegd voor onder meer sport, cultuur, onderwijs, media, welzijn, gezondheidszorg, …. Een gelijkaardige omschrijving werd ook opgenomen in andere decreten, onder meer het decreet houdende de verplichting voor bepaalde organisaties om een uittreksel uit het strafregister als vermeld in artikel 596, tweede lid, van het Wetboek van Strafvordering, te controleren voor bepaalde nieuwe medewerkers en het decreet houdende de machtiging van de Vlaamse deelnemers aan en de regeling van de modaliteiten van deelname aan de lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme.

Ook in het decreet tot oprichting van het Vlaams Mensenrechteninstituut wordt in artikel 6 verwezen naar het beschermen en bevorderen van mensenrechten in alle aangelegenheden die onder de bevoegdheden van de Vlaamse Gemeenschap en het Vlaamse Gewest vallen. Op die manier sluit de bevoegdheid van het meldpunt AJH aan bij de bevoegdheid van het VMRI, dit is immers noodzakelijk in het kader van hun samenwerking om uniform te kunnen handelen als Vlaams Meldpunt voor Grensoverschrijdend Gedrag."

betrekking tot de kwaliteit van de gegevens, zoals het feit dat de verzamelde gegevens toereikend, ter zake dienend, evenredig en juist dienen te zijn, evenals voor de vereisten met betrekking tot de bewaartermijn. In het licht hiervan vraagt de Autoriteit om **de reikwijdte nauwkeurig af te bakenen van hetgeen onder 'rechtstreekse link' en 'alle aangelegenheden die onder de bevoegdheden van de Vlaamse Gemeenschap en het Vlaamse Gewest' valt**. Tevens is het noodzakelijk dat de reikwijdte ook nauwkeurig en gedetailleerd aan de burger gecommuniceerd wordt.

23. Ten tweede, op eigen initiatief of op verzoek, **beleidsadviezen verstrekken aan organisaties**. Dit omvat het monitoren en in kaart brengen van de meldingen van grensoverschrijdend gedrag binnen de Vlaamse sectoren bij het meldpunt. Binnen dit kader is het Vlaams Meldpunt voor Grensoverschrijdend Gedrag belast met het rapporteren van anonieme gegevens[6] aan de Vlaamse Regering en het Vlaams Parlement zoals gestipuleerd in artikel 4, van het ontwerp.

24. De Autoriteit verwijst naar de redenering uit punt 64, aangaande de aanbeveling om in het kader van het voorbereidend werk voor beleidsadviezen, reeds gebruik te maken van pseudonimisering of anonimiseringstechnieken.

25. Hoewel anonieme gegevens niet langer als persoonsgegevens beschouwd worden, en niet langer onderworpen zijn aan de AVG, wijst de Autoriteit erop dat **zolang deze gegevens nog niet anoniem zijn, de AVG toepasselijk blijft**. In dit verband 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. De Autoriteit wijst erop dat transparantie m.b.t. de gebruikte anonimiseringsmethode en een analyse van de risico's verbonden aan heridentificatie elementen zijn die bijdragen tot een weloverwogen aanpak van het anonimisatieproces. Voor het overige verwijst de Autoriteit naar advies 05/2014 van de Werkgroep « Artikel 29 » over gegevensbescherming, voorganger van het Europees Comité voor gegevensbescherming, over de anonimiseringstechnieken.

26. In de mate dat hiernavolgend opgesomde artikelen betrekking hebben op anonieme gegevens, geldt punt 25 naar analogie.
    - Artikel 7, lid 6 en 7, van het ontwerp, aangaande het verstrekken van beleidsadviezen en de aanwijzing van een coördinator;
    - Artikel 9 van het ontwerp, aangaande beleidsadviezen;
    - Artikel 13, §5, van het ontwerp, aangaande de rapportering.

[6] Anonieme gegevens: informatie die niet aan een geïdentificeerde of identificeerbare natuurlijke persoon kan worden gekoppeld (art. 4.1) AVG, a contrario).

c. Verwerkingsverantwoordelijke(n)

27. De aanduiding van de verwerkingsverantwoordelijke moet overeenstemmen met de rol die deze actor in de praktijk zal opnemen en met de zeggenschap die hij heeft over de middelen die voor de verwerking zullen worden ingezet.[7]

28. Ofschoon het AJH in artikel 13, §3, van het ontwerp, expliciet als verwerkingsverantwoordelijk aangeduid wordt, volgt uit een analyse van het geheel van het ontwerp **dat er een gezamenlijke doeleinde te verwezenlijken** valt voor onderscheiden entiteiten, *i.e.*, het AJH en het VMRI. Waarbij deze laatste conform artikel 28, §2 van het decreet tot oprichting van een Vlaams Mensenrechteninstituut (hierna: VMRI-decreet) als verwerkingsverantwoordelijke aangeduid wordt voor de verwerking van gegevens onder hun bevoegdheid. Met het oog op de verwezenlijking hiervan zullen ze ieder **binnen hun bevoegdheid** 'structureel' samenwerken en complementair zijn. Zoals aangegeven in de Memorie van Toelichting zullen beide instanties "*[…] vanuit een andere invalshoek, bevoegd zijn voor meldingen van grensoverschrijdend gedrag. […].*"[8] Aldus wordt expliciet bevestigt dat *"[h]oewel het meldpunt AJH en het VMRI een ander dienstverleningsaanbod hebben, […] er qua toepassingsgebied wel een overlap [bestaat].*"[9] Dit staaft de veronderstelling dat t.a.v. de verwerking van persoonsgegevens ieder binnen eigen bevoegdheid[10] zal samenwerken tot de bewerkstelliging van een gezamenlijk doeleinde[11].

29. In het licht hiervan acht de Autoriteit het nuttig om het bestaande kader rond de gezamenlijke verwerkersverantwoordelijkheid, met name artikel 26 AVG en de rechtspraak van het Hof van Justitie, naar voren te brengen. De gezamenlijke verwerkingsverantwoordelijkheid vloeit voort uit 2 invalshoeken:

---

[7] Zowel de Werkgroep 29 – voorganger van de EDPB – als de Autoriteit hebben benadrukt dat het concept verwerkingsverantwoordelijke vanuit een feitelijk perspectief moet worden benaderd. Zie: Werkgroep 29, Advies 1/2010 over de begrippen "verantwoordelijke voor de verwerking" en "verwerker", 16 februari 2010, blz. 9 (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf 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).

[8] Artikel 3, alinea 2, Memorie van Toelichting.

[9] Artikel 3, alinea 2, Memorie van Toelichting.

[10] Het meldpunt AJH is bevoegd voor al hetgeen ressorteert onder de definitie van "grensoverschrijdend gedrag," (zie punten 9-11). Het VMRI is bevoegd voor meldingen over feiten van schendingen van mensenrechten en discriminatie die zich minder dan 5 jaar hebben voorgedaan.

[11] Gezamenlijke bevoegdheid zullen meldingen zijn over feiten van discriminerende en seksuele intimidatie die zich minder dan 5 jaar geleden hebben voorgedaan.

- In eerste instantie, is er het kader die uit artikel 26 AVG[12] en artikel 4(7) AVG[13] voortvloeit, waarbij er sprake van gezamenlijke verantwoordelijke, wanneer verschillende partijen gezamenlijk[14] het doel van en de essentiële middelen voor de verwerkingsactiviteit bepalen. Het gaat om complementaire voorwaarden die beoordeeld worden op basis van feitelijke omstandigheden. Aldus moet er sprake zijn van: i*) een gezamenlijke deelname van twee of meer entiteiten, aan de bepaling van ii) het doel en iii) de essentiële middelen van een verwerking*.[15]

- In tweede instantie, is er de situatie van 'gezamenlijke deelname', die uit de rechtspraak van het Hof van Justitie voortvloeit. Het gaat met name om beslissingen, die hoewel ze niet tezamen genomen zijn, als samenvallend of convergerend beschouwd worden m.b.t. de doeleinden en middelen. Zulks dat ze elkaar aanvullen en noodzakelijk zijn om de verwerking derwijze toe te laten dat het doel en de middelen van de verwerking tastbaar beïnvloed wordt. De vaststelling dat de verwerking niet mogelijk zou zijn geweest zonder de medewerking van beide partijen, in die zin dat de verwerking door elke partij onscheidbaar is, d.w.z. onlosmakelijk met elkaar verbonden, is doorslaggevend voor de kwalificering als samenlopende beslissing.[16]

30. Het is deze laatste situatie die, *in casu*, aanleiding geeft tot de vaststelling dat er *de facto* een situatie van gezamenlijke verwerkingsverantwoordelijkheid aanwezig is. Er is immers krachtens artikel 3, §2, van het ontwerp, sprake van een gezamenlijke doelstelling tussen verschillende entiteiten, zoals hiernavolgend gestipuleerd:

> "***Het meldpunt AJH en het VMRI werken structureel samen aan de verwezenlijking van de doelstelling***, *vermeld in paragraaf 1, tweede lid. In die voormelde samenwerking*

---

[12] Artikel 26 AVG: Gezamenlijke verwerkingsverantwoordelijken: "*1.Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Zij stellen op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze verordening vast, met name met betrekking tot de uitoefening van de rechten van de betrokkene en hun respectieve verplichtingen om de in de artikelen 13 en 14 bedoelde informatie te verstrekken, door middel van een onderlinge regeling, tenzij en voor zover de respectieve verantwoordelijkheden van de verwerkingsverantwoordelijken zijn vastgesteld bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijken van toepassing is. In de regeling kan een contactpunt voor betrokkenen worden aangewezen.*

2.Uit de in lid 1 bedoelde regeling blijkt duidelijk welke rol de gezamenlijke verwerkingsverantwoordelijken respectievelijk vervullen, en wat hun respectieve verhouding met de betrokkenen is. De wezenlijke inhoud van de regeling wordt aan de betrokkene beschikbaar gesteld.

3.Ongeacht de voorwaarden van de in lid 1 bedoelde regeling, kan de betrokkene zijn rechten uit hoofde van deze verordening met betrekking tot en jegens iedere verwerkingsverantwoordelijke uitoefenen."

[13] De begrippen verwerkingsverantwoordelijke en verwerker zijn gedefinieerd in artikelen 4, 7) en 8 van de AVG. Lees eveneens het Advies G29, 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", (WP169) 16 februari 2010.

[14] *In casu*, moet "gezamenlijk" geïnterpreteerd worden als 'samen met' of 'niet alleen'.

[15] EDPB, richtsnoeren 07/2020 06/2014 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG, 22.

[16] HvJ (3e k.) 11 januari 2024, nr. C-231/22, ECLI:EU:C:2024:7, Belgische Staat / Gegevensbeschermingsautoriteit; EDPB, richtsnoeren 07/2020 06/2014 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG, 23; S. De Smedt en M. Caproni, "[Inleiding] Toepassingsgebied van de AVG: wat u zeker moet weten" in, *Praktische gids privacy in de onderneming*, Mechelen, Kluwer, 29.

werkt het VMRI binnen zijn bevoegdheden en mandaat, vermeld in titel 3 van het decreet van 28 oktober 2022, en werkt het meldpunt AJH binnen de bevoegdheden en opdrachten, vermeld in hoofdstuk 3 van dit decreet. […]"[17]

31. Het spreekt voor zich dat een gezamenlijke doelstelling, tot gevolg zal hebben dat elke entiteit voor zich en met betrekking tot haar bevoegdheden zal bepalen of een klacht of melding al dan niet samen zal worden behandeld. Dit komt *de facto* neer op een situatie waarbij twee verwerkingsverantwoordelijken enerzijds **een gezamenlijk doel nastreven**,[18] en anderzijds een eigen beslissing, die als convergerend beschouwd kan worden en in praktijk tot gevolg heeft dat bepaald wordt welke persoonlijke gegevens verwerkt zullen worden. Met andere woorden "*de verwerking zou niet mogelijk zijn geweest zonder de medewerking van beide partijen aan het doel en de middelen, in die zin dat de verwerking door elke partij onscheidbaar is, d.w.z. onlosmakelijk met elkaar verbonden*."[19]

32. Dat de beslissing over het gezamenlijke doeleinde niet door de verwerkingsverantwoordelijken genomen is geweest, maar door een wetgevende norm bepaald is, doet hieraan geen afbreuk.[20] Overeenkomstig een recent arrest van het Hof van Justitie, kan de "*vaststelling van de doelstellingen van en de middelen voor de verwerking en, in voorkomend geval, de aanwijzing van die verantwoordelijke in het nationale recht, niet alleen expliciet maar ook impliciet […] zijn.*"[21] Hieruit volgt dat de 'doelstelling, 'middelen' en 'verwerkingsverantwoordelijke', zowel **impliciet als expliciet uit een norm kunnen volgen**.[22] Bijgevolg kan de Autoriteit, niet anders dan vaststellen dat er, *in casu*, een gezamenlijke verwerkingsverantwoordelijkheid is tussen het AJH en het VMRI. **Derhalve zal met betrekking tot de gezamenlijke doelstelling en de samenlopende beslissingen over de verwerking van gegevens zowel het AJH als het VMRI gezamenlijk verantwoordelijk zijn voor de naleving van de AVG**.[23] Het AJH en het VMRI, zijn derhalve elk voor zich apart verwerkingsverantwoordelijken voor al hetgeen niet onder de gezamenlijke bevoegdheid valt.

---

[17] Vet toegevoegd door de Autoriteit.

[18] Concl. AG L. Medina, ECLI:EU:C:2023:468, bij HvJ (3e k.) 11 januari 2024, nr. C-231/22, ECLI:EU:C:2024:7, vn. 25: "*De in artikel 4, punt 7, juncto artikel 5, lid 1, onder b), AVG neergelegde verplichting om de doeleinden vast te stellen en te omschrijven, vereist evenwel ten minste dat elke indirecte vaststelling van de doeleinden van de verwerking voortvloeit uit de wettelijke bepalingen die ten grondslag liggen aan de activiteit van de betrokken autoriteit.*"

[19] EDPB, richtsnoeren 07/2020 06/2014 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG, 23.

[20] Zie voetnoot 18.

[21] HvJ (3e k.) 11 januari 2024, nr. C-231/22, ECLI:EU:C:2024:7, *Belgische Staat / Gegevensbeschermingsautoriteit*, randnr. 30.

[22] Concl. AG L. Medina, ECLI:EU:C:2023:468, bij HvJ (3e k.) 11 januari 2024, nr. C-231/22, ECLI:EU:C:2024:7, randnr. 51: "*Het is ook mogelijk dat de wet een entiteit als verwerkingsverantwoordelijke aanwijst, zij het impliciet. Wanneer bijvoorbeeld de nationale wetgeving de entiteit in kwestie de verplichting oplegt om bepaalde gegevens onder zich te houden of te verstrekken, wordt deze entiteit beschouwd als verantwoordelijke voor de verwerking die noodzakelijk is voor de nakoming van die verplichting. Een dergelijke impliciete aanwijzing in de nationale wetgeving vindt plaats wanneer uit de rol, de taken en de bevoegdheden van deze autoriteit blijkt dat zij het doel van en de middelen voor de betrokken verwerking vaststelt […].*"

[23] Overweging 79 AVG.

33. Gelet op het beoogd doelpubliek, de gevoeligheid van gegevens en de voor een leek complexiteit van de materie, zou het de rechtszekerheid ten goede komen, als **het ontwerp en het decreet VMRI verder zouden worden aangevuld zodat naast de verwerkingsverantwoordelijkheid, ook expliciet gewezen wordt op het bestaan van een gezamenlijke verwerkingsverantwoordelijkheid**. Meer concreet moet worden uitgeklaard wanneer, en onder welke voorwaarden de bevoegde autoriteiten optreden als verwerkingsverantwoordelijke, dan wel als verwerker of gezamenlijke verwerkingsverantwoordelijke.[24] In lijn met andere adviezen van de Autoriteit wordt er ook sterk benadrukt dat er één enkel contactpunt[25] beschikbaar moet zijn voor betrokkenen. Met het oog op een efficiënte en volledige bescherming van betrokkenen, wordt de decreetgever aangemoedigd om hier gehoor aan te geven. Op die manier is het voor betrokkenen duidelijk tot wie ze zich kunnen wenden om hun rechten uit te oefenen.[26]

34. Tenslotte noteert de Autoriteit dat dit ook implicaties zal hebben voor artikel 3, §2, lid 2, van het ontwerp, betreffende het samenwerkingsprotocol, zoals wordt uiteengezet in punten – 104 t.e.m. 108.

d. Minimale gegevensverwerking/ Proportionaliteit

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

36. Voorafgaand wenst de Autoriteit aan te geven dat artikel 13, van het ontwerp, een cluster is van alle te verwerken (categorieën van) persoonsgegevens, al de verwerkingswijzen, alle mogelijke betrokkenen, verwerkingsgronden en de bewaartermijn. Door de algemene beschrijving van de diverse elementen en het gebrek aan een link tussen de elementen, heeft de decreetgever er voor gezorgd dat het geheel ontransparant is. Tegen deze achtergrond ziet de Autoriteit zich genoodzaakt om het geheel van de procedure m.b.t. de gegevensverwerkingen in het kader van meldingen, te ontleden en stapsgewijs te begeleiden met observeringen. Terzake wordt *i) eerst het geheel van een melding besproken; ii) nadien wordt de aandacht gevestigd op de categorieën van persoonsgegevens die opgelijst zijn; iii) dit wordt opgevolgd door de meldingskanalen en de daarmee samenhangende persoonsgegevens; iv) voorts wordt ook ingegaan op het*

[24] Advies nr. 69/2022 van 22 april 2022, randnr. 34.

[25] De oprichting van één enkel contactpunt impliceert uiteraard de invoering van de nodige procedures die deze centralisatie ook effectief doen functioneren.

[26] Artikel 26(3) en art. 82(4) AVG; HvJ, (Gr. Kam.) 13 mei 2014, nr. C-132/12, *GOOGLE SPAIN SL, GOOGLE INC. v/ AEPD*, randnr. 34; HvJ (Gr. Kam.) 5 juni 2018, nr. C-210/16, *UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIM v/ WIRTSCHAFTSAKADEMIE SCHLESWIG-HOLSTEIN GMBH*), randnr. 28.

meldingsregister; v) waarna oog zal zijn voor de categorieën van betrokkenen; vi) dit wordt nagegaan door het onderdeel over anonieme meldingen en vii) ten slotte beëindigd met de wijze van verwerking.

- Proces van een melding

37. Uit de Memorie van Toelichting kan afgeleid worden, dat een melding bij het meldpunt AJH in verschillende fases onderverdeeld kan worden. Hetgeen *de facto* implicaties heeft voor de hoeveelheid gegevens die verwerkt worden. Zo wordt in de laatste alinea van artikel 5 uit de Memorie van Toelichting gesteld:

"*[…] Dat wil echter niet zeggen dat er op basis van elke melding automatisch een volledig traject zal worden gestart […].*"

38. Wat nadien nogmaals onderstreept wordt in de tweede alinea van artikel 6 van de Memorie van Toelichting die het volgende stelt:

"*[…] Het meldpunt vertrekt vanuit de noden van de melder. Het aanbod verloopt vraaggestuurd, op maat en op het tempo van de melder. Na elke melding volgt een uitgebreide vraagverheldering. Op basis van de specifieke vragen van een melder wordt het passende aanbod besproken met de melder. […]*"

39. Verder voorziet artikel 7, lid 3, van het ontwerp het volgende:

"*In de volgende gevallen is de melding niet ontvankelijk:*

1° de melding is kennelijk ongegrond;

2° de melding is kennelijk roekeloos of tergend;

3° de melding is al behandeld door het meldpunt AJH;

4° de melding heeft geen betrekking op aangelegenheden die onder de bevoegdheden van de Vlaamse Gemeenschap en het Vlaams Gewest vallen."

40. Het geheel in acht genomen kan geconstateerd worden dat er in eerste instantie een melding moet zijn (eerste fase). In tweede instantie zal "***na elke melding*** *[…] een uitgebreide vraagverheldering [volgen]*," (tweede fase). In derde instantie moet de ontvankelijkheid beoordeeld worden en een passend aanbod voorzien worden. Het onderscheid tussen deze verschillende fases is van belang, omdat het een invloed heeft op de hoeveelheid gegevens die noodzakelijk zijn voor de verwerking, maar ook meespeelt bij de beoordeling van de bewaartermijn.

41. Het is op heden onduidelijk of de beoordeling van de ontvankelijkheid van een melding, onmiddellijk in eerste fase of na de tweede fase, *i.e.*, de vraagverheldering, plaatsvindt. Er kan

aangenomen worden dat in bepaalde gevallen, reeds in de eerste fase, uitspraak gedaan kan worden over de (on)ontvankelijkheid. Dit zou onder meer mogelijk zijn wanneer uit de melding klaarblijkelijk volgt dat het geen grensoverschrijdend gedrag betreft of dat het buiten de bevoegdheid van de Vlaamse overheid is. Zoals verder toegelicht, kan de inhoud van een melding sterk variëren met als gevolg dat dergelijke beoordeling omwille van onvoldoende informatie in de eerste fase, pas mogelijk is na "*de uitgebreide vraagverheldering*". Dit uitgangspunt werd door de aanvrager bevestigd.[27] Niettemin stemt het antwoord niet volledig overeen met hetgeen overeenkomstig artikel 6, tweede alinea van de Memorie van Toelichting gesteld wordt, namelijk dat er "*na elke melding […] een uitgebreide vraagverheldering [zou volgen]*." Hoewel de keuze voor dergelijke werkwijze, verstaanbaar is in deze specifieke context en in het licht van het beoogd doel van algemeen belang, lijkt een systematische "*uitgebreide vraagverheldering*" ook daar waar de melding klaarblijkelijk onontvankelijk is, verregaand **omdat er meer gegevens verwerkt zullen worden dan hetgeen werkelijk noodzakelijk is.** Zodoende lijkt het aangeraden om voor een geval per geval beoordeling te opteren, alvorens over te gaan tot een "uitgebreide vraagverheldering." Om dubbelzinnigheden te vermijden adviseert de Autoriteit om de Memorie van Toelichting op één lijn te brengen met het antwoord van de aanvrager, zodat er niet systematisch na elke melding een "uitgebreide vraagverheldering" volgt.

- <u>Categorieën van persoonsgegevens</u>

42. Uit artikel 13, §1 van het ontwerp, volgt dat het meldpunt AJH hiernavolgende categorieën van gegevens kan verwerken:

> "*1° **identificatiegegevens, waaronder voor- en achternaam en het rijksregisternummer of het identificatienummer van de Kruispuntbank van de Sociale Zekerheid;***
> *2° contactgegevens;*
> *3° beroepsgegevens;*
> *4° persoonsgegevens die blijken uit de feitelijke omstandigheden van de melding van grensoverschrijdend gedrag;*
> *5° persoonsgegevens die blijken uit de opvolging van een melding van grensoverschrijdend gedrag;*
> *6° bijzondere categorieën van persoonsgegevens als vermeld in artikel 9 van de algemene verordening gegevensbescherming;*

[27] Op de vraag van de Autoriteit naar het tijdstip van de beoordeling van de ontvankelijkheid – bij ontvangst of na de vraagverheldering, preciseerde de aanvrager het volgende: "*De beoordeling vindt zo vroeg mogelijk plaats maar beide mogelijkheden zijn van toepassing. Als er bij de eerste contactname voldoende informatie wordt meegegeven door de melder om de ontvankelijkheidstoets te maken kan de beoordeling mbt ontvankelijkheid onmiddellijk gebeuren. Afhankelijk van het medium van de contactname, dient soms bijkomende informatie opgevraagd worden en kan de ontvankelijkheid maar later getoetst worden. Het is ook niet altijd meteen duidelijk of alle ontvankelijkheidsvoorwaarden voldaan zijn en dan moet extra opzoekwerk achter de schermen gebeuren.*"

7° politionele en gerechtelijke gegevens. […]"[28]

43. De Autoriteit merkt, vooreerst, op dat het gebruik van het begrip *"INSZ"* (‘identificatienummer van de sociale zekerheid’) moet worden vermeden, aangezien het *a priori* geen wettelijk bestaan heeft. Volgens artikel 8 van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid* worden het Rijksregisternummer en het bisnummer (zijnde het uniek persoonlijk identificatienummer, bedoeld in artikel 8, § 1, 2° van de KSZ-wet, dat door de KSZ wordt toegekend aan elke persoon die niet in het Rijksregister is opgenomen, maar die in België socialezekerheidsrechten geniet) binnen het netwerk van de sociale zekerheid als identificatiemiddelen gebruikt. In plaats van te verwijzen naar het ‘INSZ’ moet bijgevolg worden verwezen naar het identificatienummer van het Rijksregister en het identificatienummer bis zoals bedoeld in artikel 8, § 1, 2° van de KSZ-wet.

44. Met betrekking tot het Rijksregisternummer, vestigt, de Autoriteit, de aandacht van de aanvrager op het feit dat het Rijksregisternummer alleen mag worden gebruikt/verwerkt onder de voorwaarden als bepaald in artikel 8 van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen.[29] **Het verdient de aanbeveling om de rechtsgrond, nl. artikel 8 van voormelde wet, expliciet te vermelden in het ontwerp**. De Autoriteit herinnert er ook in het algemeen aan dat unieke identificatienummers een bijzondere bescherming genieten. Artikel 87 AVG voorziet dat de lidstaten die een nationaal identificatienummer vaststellen, er moeten over waken dat dit alleen wordt gebruikt met passende waarborgen voor de rechten en vrijheden van de betrokkene. Zo vestigde de Commissie voor de bescherming van de persoonlijke levenssfeer, de rechtsvoorganger van de Autoriteit, reeds eerder[30] de aandacht op in acht name van volgende waarborgen terzake:
    - het gebruik van een algemeen identificatienummer moet worden beperkt tot de gevallen waarin dit strikt noodzakelijk is aangezien dit gebruik risico's impliceert inzake koppeling van bestanden;
    - de doeleinden moeten duidelijk en expliciet worden gepreciseerd zodat men de beoogde soorten verwerkingen kan vermoeden/voorzien;
    - de bewaartermijn en de eventuele mededelingen aan derden moeten eveneens worden omkaderd;

---

[28] Vet toegevoegd door Autoriteit.

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

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

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

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

- technische en organisatorische maatregelen moeten het beveiligd gebruik passend omkaderen; en
- de niet-naleving van de bepalingen die het gebruik omkaderen moeten worden gesanctioneerd aan de hand van effectieve, proportionele en ontradende sancties.

45. Terzake wijst de Autoriteit erop dat het ontwerp en de Memorie van Toelichting niet verduidelijken waarvoor het Rijksregisternummer of het of het identificatienummer van de Kruispuntbank van de Sociale Zekerheid, gebruikt zullen worden. Er wordt enkel gesteld dat het verwerkt kan worden. Ofschoon vermoed kan worden dat het ter identificering van de personen in kwestie gaat, kan het gebruik niet overgelaten worden aan het loutere feit van een vermoeden. Bovendien veronderstelt de Autoriteit bij gebrek aan verdere informatie dat het betrekking zal hebben op eender wie van de betrokkenen. De Autoriteit merkt voorts op dat het vaststaat dat er doorgiftes zullen zijn, doch wordt de inhoud niet gekaderd, ook niet voor het Rijksregisternummer. Daarnaast wijst de Autoriteit op het feit dat deze op een SharePoint bijgehouden zullen worden, hetgeen wederom te wensen laat in termen van technische en organisatorische maatregelen – zoals besproken in punt 57. Hoewel het beroepsgeheim een zeker kader met sancties verbindt, blijft het noodzakelijk om expliciete richtlijnen te voorzien voor het gebruik van het Rijksregisternummer, met daaraan gekoppelde sancties.

46. Voorts is het voor de Autoriteit, onduidelijk wat bedoeld wordt met "*persoonsgegeven die blijken […]* " in punten 4 en 5. Dergelijke ruime beschrijving, is een blanco cheque om eender welke gegevens te kunnen verwerken. Derhalve moet verdere duiding voorzien worden zodat concreet en ondubbelzinnig geconcludeerd kan worden welke soort gegevens hiermee bedoeld worden en er in een tweede fase enkel de absoluut noodzakelijke gegevens bewaard kunnen blijven.

47. Ten aanzien van artikel 13, §1, 7°, van het ontwerp, betreffende de "**politionele en gerechtelijke**" gegevens, wijst de Autoriteit op de toepassing van artikel 10 AVG. Terzake mag de verwerking van dergelijke gegevens enkel gebeuren onder toezicht van een overheid of andere daar waar door norm (nationaal of Europees) voorziet in passende waarborgen voor de rechten en vrijheden van de betrokkenen. Omvattende registers van strafrechtelijke veroordelingen mogen alleen worden bijgehouden onder toezicht van de overheid. *In casu*, kwalificeert het AJH als een Vlaamse overheid en is ze bijgevolg bij machte om dergelijke verwerkingen uit te voeren. Niettemin brengt de Autoriteit aan dat gelet op het karakter van deze gegevens enige voorzichtigheid geboden is. Aangezien – zoals besproken in punt 62 – in het ontwerp zelf, geen vermelding wordt gemaakt over een (melding)register of de inhoud ervan, **raadt de Autoriteit ten stelligste af om deze gegevens in de vorm van een register bij te houden.** Bovendien voorziet het ontwerp onvoldoende maatregelen die als "bijkomende passende waarborgen voor de rechten en vrijheden van de betrokkenen" kunnen kwalificeren. Zo wordt nergens allusie

gemaakt naar een lijst van de categorieën van personen die toegang hebben tot de persoonsgegevens, met een beschrijving van hun hoedanigheid ten opzichte van de verwerking van de beoogde gegevens.[31]

48. Voorts constateert de Autoriteit dat het VMRI, net zoals het meldpunt AJH als een Vlaamse overheid gekenmerkt kan worden. Krachtens artikel 28, §5, 7°, van het VMRI-decreet, kan het VMRI, **in de mate dat het proportioneel is** ook politionele of gerechtelijke gegevens verwerken. Doch wordt in tegenstelling met onderhavig ontwerp geen verwijzing gemaakt naar artikel 10 AVG. Niettemin zal het VMRI, net zoals het meldpunt AJH t.a.v. de gemeenschappelijke bevoegdheden, bij machte zijn om het toezicht te hebben over de verwerking van dergelijke gegevens. Desondanks onderstreept de Autoriteit dat dit toezicht duidelijker omkaderd moet worden. T.a.v. een register aangaande strafrechtelijke veroordelingen, geldt dezelfde aanbeveling als in punt 47, m.n., zich onthouden van strafrechtelijke gegevens bij te houden in de vorm van een register.

49. Zoals reeds toegelicht, moet een melding bij het meldpunt in verschillende fases beoordeeld worden. Enerzijds de eerste fase, betreffende de gegevens die in de eerste melding gedeeld worden. En Anderzijds, de tweede fase die betrekking heeft op het geheel van informatie na "*de uitgebreide vraagverheldering*."

50. Ten aanzien van de eerste melding merkt de Autoriteit op dat er nergens expliciet aangegeven is welke gegevens het moet bevatten. Afgaand op hetgeen wel vaststaat, namelijk de "*uitgebreide vraagverheldering*" die in de tweede fase plaatsvindt, kan verondersteld worden dat de hoeveelheid van de gegevens uit de eerste fase, *i.e.*, de melding zelf, in praktijk op twee manieren ingevuld kan worden:
    - Enerzijds is de eerste melding vrij, zijnde dat de melder, naar eigen believen, zoveel of zo weinig informatie in de melding kan voorzien. In dit scenario kan de reikwijdte van de informatie die de melding bevat, een grotere omvang hebben dan hetgeen noodzakelijk is en omgekeerd. De tweede fase, zou hier bijdragen tot een beperking of specificering van de gegevens die werkelijk essentieel zijn of omgekeerd een aanvulling, daar waar onvoldoende informatie voorzien is, in de eerste fase.
    - Anderzijds is er het scenario waarbij, de melder over een gerichte kader beschikt en in de eerste fase, op een gerichte wijze informatie gegeven wordt. Hierdoor zal de omvang van de informatie die verkregen wordt van een melder, gelimiteerd worden. Dit zou bijvoorbeeld het geval zijn, bij gebruik van een invulformulier. De tweede fase, zou neerkomen op een aanvulling van de informatie m.b.t. de essentiële elementen.

[31] Artikel 10, §2, lid 1, van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

51. Het onderscheid tussen beide situaties is dat de melder naargelang de situatie reeds in eerste fase potentieel meer of minder gegevens kan doorgeven dan hetgeen werkelijk noodzakelijk is.

52. Hoewel het noch uit de Memorie van Toelichting, noch het ontwerp voortvloeit, heeft de decreetgever door de vorm van de melding te bepalen, impliciet geopteerd voor een situatie waarbij de omvang van de informatie die de melding bevat vrijelijk door de melder bepaald wordt. Zodoende leert verder onderzoek, op de website van het Vlaams Meldpunt voor Grensoverschrijdend Gedrag, dat er **3 manieren zijn: telefonisch, per e-mail en per chat**, waarbij enkel voor deze laatste op de website een beperkte indicatie is over hetgeen zeker vermeld of gevraagd zal worden:
    a. *Vooraleer je kan chatten, geef je je naam of nickname (schuilnaam).*
    b. *We vragen je geslacht en leeftijd. Je vult in wat je zelf wilt.*
    c. *Tijdens het eerste chatgesprek vragen we je naar algemene informatie over datgene dat je wil melden.*
    d. *We proberen een chatgesprek na ongeveer een half uur af te ronden, zodat zoveel mogelijk mensen aan de beurt kunnen komen.*
    e. *Is de chat bezet, probeer het later nog eens of bel of mail ons.* [32]

53. De keuze voor een systeem waarbij in de eerste fase geen beperking is voor de melder t.a.v. de (categorieën van) gegevens en hoeveelheid ervan, heeft tot gevolg dat er **potentieel meer gegevens dan noodzakelijk doorgegeven zullen worden**. Binnen dergelijk systeem is het **onwaarschijnlijk dat de (categorieën van) persoonsgegevens die** door een melder **doorgegeven worden**, **in praktijk werkelijk beperkt zullen zijn tot hetgeen opgesomd is in artikel 13, §1, van het ontwerp**. De Autoriteit herinnert, de decreetgever, eraan dat de verwerking van gegevens "*toereikend, ter zake dienend en niet bovenmatig [...] [hoort te] zijn, uitgaande van de doeleinden waarvoor zij worden verzameld of waarvoor zij vervolgens worden verwerkt.*"[33] Het is van belang dat de decreetgever de nodige afweging maakt om niet in een situatie van 'bovenmatige' gegevensverwerking te belanden, maar ook niet in een situatie van ontoereikende gegevens – zoals aangekaart in punten 65 en 72.

54. In de tweede fase, kan er aangenomen worden dat alvorens een passend aanbod te kunnen voorzien, deze fase een antwoord moet hebben op een aantal gegevens. Hieruit volgt dat de tweede fase gericht gaat kijken naar informatie over een zeker aantal aspecten. Er kan dus gesteld worden dat hoewel er reeds in de eerste fase een verwerking kan zijn van opgesomde categorieën

[32] s.n., Agentschap Justitie en Handhaving, Vlaams Meldpunt Grensoverschrijdend Gedrag is een officiële website van de Vlaamse overheid, laatst geraadpleegd op 15 februari 2024 van https://www.vlaanderen.be/vlaams-meldpunt-grensoverschrijdend-gedrag/chat-met-ons-over-grensoverschrijdend-gedrag.

[33] HvJ 11 december 2019, nr. C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA*, EU:C:2019:1064, punt 48.

van gegevens uit artikel 13, §1, van het ontwerp, het pas in de tweede fase – of later bij kennisneming van nieuwe elementen – zal zijn dat het geheel aan informatie verzameld zal worden.

55. Voorgaande in acht genomen is het voor de Autoriteit onduidelijk hoe het meldpunt AJH bij de **verwerking van de gegevens van een melding (beide fases), zich enkel zal beperken tot de verzameling van relevante gegevens**. Zoals gesteld in punt 53 kan bij de melding in eerste fase, meer gegevens verzameld worden dan noodzakelijk, maar ook meer dan hetgeen mag verwerkt worden krachtens artikel 13, van het ontwerp. In die mate dat de tweede fase overeenkomt met een controle fase, waarbij nadien enkel noodzakelijke informatie m.b.t. de melding bijgehouden wordt, kan de Autoriteit hierin berusten.[34] Niettemin wijst de Autoriteit erop dat de bijkomende redactie, vermeden of alleszins beperkter had kunnen zijn indien melders reeds bij aanvang een duidelijke omkadering zouden krijgen over de hetgeen in een melding voorzien moet zijn. Voorts vraagt de Autoriteit zich af, hoe dit in zijn werk zal gaan voor chatgesprekken en e-mails. Het is raadzaam om hierbij de lijn door te trekken van wat voorzien is voor telefoongesprekken: de chat zelf wordt niet bijgehouden, maar een samenvatting van de inhoud wel.

- <u>Meldingskanalen en persoonsgegevens</u>

56. In het verlengde hiervan en terugkoppelend naar de kanalen van een melding uit punt 52, stelt de Autoriteit vast dat wederom geen informatie voorzien is in het ontwerp en de Memorie van Toelichting over het medium en de vorm. Dat er een leemte is aangaande de inhoud van een melding werd reeds vastgesteld en besproken. Doch moet ook gewezen worden op een andere lacune die hieruit volgt, namelijk worden de gegevens die uit een meldingskanaal komen bijgehouden, hoe wordt dat gedaan en welke gegevens worden bijgehouden. Op vraag van de Autoriteit, specificeerde de aanvrager het volgende:

> "*Dossiers worden bijgehouden in SharePoint (voorzien beveiligde toegang), in afwachting van een op maat gemaakt registratie- en dossieropvolgsysteem (procedure aanbesteding wordt gestart voorjaar 2024).*
>
> *Telefoongesprekken worden niet opgenomen. In het inhoudelijk dossier wordt de inhoud van de melding samengevat. In het dossier wordt enkel informatie opgenomen die noodzakelijk is voor de opvolging en behandeling van de melding.*"

57. Vooreerst wenst de Autoriteit nader in te gaan op het systeem dat gebruikt wordt voor de bewaring van de dossiers. Uit het antwoord van de aanvrager, leidt de Autoriteit af dat de (inhoudelijke)

[34] Er wordt tevens onderstreept dat het beginsel van de juistheid van gegevens krachtens artikel 5(1)(d) AVG, dergelijke check-up vereist.

dossiers bijgehouden zullen worden in SharePoint (die voorzien is van een beveiligde toegang) en later vervangen wordt door een op maat gemaakte registratie- en dossieropvolgsysteem. Ten eerste, wat het gebruik van SharePoint betreft, begrijpt de Autoriteit, dat het om een tijdelijke situatie gaat en dat er in de nabije toekomst een ander systeem ingevoerd zal worden**. Doch wordt onderstreept dat de overschakeling primordiaal is en binnen een redelijke termijn dient te gebeuren**. In acht genomen dat dossiers ook persoonsgegevens kunnen bevatten die onder artikel 9 en artikel 10 AVG vallen, geeft het bewaarmiddel en het feit dat het slechts terloops wordt opgemerkt in een antwoord van de aanvrager, en niet eens het ontwerp of de Memorie van Toelichting, aanleiding tot bezorgdheid. **Er wordt sterk betwijfeld dat een standaard product, zoals SharePoint, voldoende beveiliging biedt voor dergelijke gevoelige gegevens.** Gezien de huidige stand van de techniek, zijn er systemen die hiervoor beter geschikt zijn.[35] **Bovendien wordt onderstreept dat de graad van bescherming in overeenstemming moet zijn met het risico en de aard van de gegevens.** In dat verband wordt aanbevolen om naargelang de aard van gegevens, in een gepaste beveiliging te voorzien. Dit betekent o.m. dat niet alle gegevens even toegankelijk horen te zijn. Met andere woorden, ook in de inhoudelijke dossiers moet de toegang en in het bijzonder het aantal personen dat er toegang toe heeft en de wijze waarop zij die toegang verkrijgen, beperkt worden naargelang bevoegdheid en de aard van de gegevens. Wat betreft de "beveiligde toegang," moet minstens een multifactor authenticatie en logging van de activiteiten, geïmplementeerd zijn. Verder wordt ook aanbevolen om daarbovenop andere maatregelen te voorzien zoals, vervaldata op dossiers, Double Key Encryption voor de opslag van bestanden met zeer gevoelige of bijzondere persoonsgegevens, gradaties in toegang, hantering van trackchanges, het gebruik met toegang door een link vermijden (of beperken tot eenmalig gebruik).

58. Daarnaast vermoedt de Autoriteit, op grond van de voorziene commentaar in het 'formulier voor het aanvragen van een advies over een ontwerp van normatieve tekst', dat het gebruik van de SharePoint vermoedelijk niet eerst aan een gegevensbeschermingseffectenbeoordeling (GEB) onderworpen werd, zoals artikel 35 AVG het vereist. De Autoriteit benadrukt dat alle verplichtingen onder de AVG, nageleefd moeten worden, ook in het kader van het gebruik van SharePoint. Voor verdere informatie, verwijst de Autoriteit, de aanvrager naar de '2022 Coordinated Enforcement Action', van de EDPB aangaande het gebruik van clouddiensten in de publieke sector.[36]

59. Ten tweede, wat het op maat gemaakte registratie- en dossieropvolgsysteem betreft, wordt benadrukt dat de betrokkenen van wie de gegevens zijn bewaard over voldoende garanties moeten beschikken zodat hun persoonsgegevens doeltreffend worden beschermd tegen het risico

[35] Artikel 25(1) AVG.

[36] EDPB, 2022 Coordinated Enforcement Action 17 January 2023, Use of cloud-based services by the public sector, laatste geraadpleegd op 14 februari 2024, van https://edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf.

van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens.[37] De Autoriteit benadrukt dat er passende technische en organisatorische maatregelen geïmplementeerd dienen te worden te om de veiligheid en vertrouwelijkheid van bewaarde informatie te waarborgen. Dit omvat minstens het gebruik van tweefactorauthenticatie, complexe wachtwoorden, logging van communicatie en fingerprinting voor elektronisch verstrekte bestanden. Voorts merkt de Autoriteit op dat, voor dergelijke gevoelige gegevens, de voorkeur gegeven wordt aan elektronische opeslag en gegevensuitwisseling via een beveiligd platform, overeenkomstig eerder geleverde adviezen.[38]

60. Tenslotte verduidelijkt de aanvrager dat telefoongesprekken niet opgenomen, maar samengevat en bijgehouden zullen worden in het inhoudelijke dossier. De Autoriteit herinnert de aanvrager eraan dat de melder reeds dan geïnformeerd moet worden over de verwerking van de gegevens en de wijze waarop de informatie bijgehouden wordt, namelijk een geschreven samenvatting van het telefoongesprek. De Autoriteit merkt op dat dit extra aandacht zal vergen voor de juistheid van de gegevens. Met betrekking tot e-mail en chat, verwijst de Autoriteit naar de observering in punt 55.

61. Terzake vraagt de Autoriteit om bij voorkeur in het ontwerp of minstens in de Memorie van Toelichting, kenbaar te maken langs welke kanalen de melder een melding kan maken. Daarnaast dienen deze documenten aangevuld te worden met de antwoorden van de aanvrager en de observaties van de Autoriteit.

- <u>Meldingsregister</u>

62. Het oogmerk om te voorzien in een adequate opvolging van een melding van grensoverschrijdend gedrag lijkt onlosmakelijk verbonden te zijn met het hebben van een register. Hetgeen in lijn ligt met de procedure van een melding bij het meldpunt AJH, die opgebouwd is uit verschillende fases. Het risico op een ernstige inbreuk van de rechten en vrijheden van de betrokkenen, maakt het **absoluut noodzakelijk dat het ontwerp zelf expliciet toelichting geeft over het bestaan van een meldingsregister, de inhoud en het gebruik**. Terzake stelt de Autoriteit vast dat het ontwerp, behoudens een oppervlakkige vermelding over een verdere uitwerking in een samenwerkingsprotocol van een centraal register, verder niet verwijst naar een meldingsregister of een gelijkaardig register.[39] Merk op dat het eerste betrekking heeft op klachten of meldingen die onder de bevoegdheid van zowel het VMRI als het meldpunt AJH vallen, terwijl het laatste

[37] HvJ 8 april 2014, nrs. C-293/12 en C-594/12, *Digital Rights Ireland e.a.*, EU:C:2014:238, punten 54 en 55.

[38] Advies 160/2023, randnrs. 25 en 58.

[39] Artikel 3, §3, lid 4 van het ontwerp; artikel 3, alinea 8 van de Memorie van Toelichting.

enkel betrekking heeft op klachten en meldingen die alleen onder het meldpunt AJH vallen. Op vraag van de Autoriteit, preciseerde de aanvrager het volgende:

> "*Er wordt gebruik gemaakt van een meldingsregister waarbij limitatief volgende objectiveerbare gegevens worden bijgehouden voor beleidsdoeleinden: datum contactname, aard contactname, medium contactname, aard GOG, organisatie GOG, sector GOG, leeftijd en gender.*
> *Enkel de medewerkers van het meldpunt hebben toegang tot het meldingsregister.*
> *Dit meldingsregister staat los van het inhoudelijk dossier.*
>
> *Ook anonieme meldingen worden in het meldingsregister opgenomen maar daarbij worden identificerende gegevens, indien deze al verstrekt worden, niet opgenomen.*
>
> *Het Meldpunt zal geval per geval afwegen of de registratie van de gegevens in het meldingsregister de anonimiteit afdoende vrijwaart en de combinatie van de gegevens geen aanleiding geeft tot een 'identificeerbare' melding*."

63. De aanvrager, bevestigt dat er gebruik zal worden gemaakt van een meldingsregister. Het blijft **echter onduidelijk of dit 'meldingsregister', hetzelfde register is als het 'centraal register'**. De Autoriteit vraagt om dit te verduidelijken in het ontwerp of minstens in de Memorie van Toelichting.[40] Er wordt bovendien op gewezen dat dit register ongeacht de benaming 'meldingsregister', 'incidenteel register' of 'centraal register' niet gelijkstaat aan het intern register van de verwerkingsactiviteiten dat krachtens artikel 30 AVG verplicht is voor elke verwerkingsverantwoordelijke.

64. Hetgeen wel uitdrukkelijk wordt aangegeven is dat **het meldingsregister voor beleidsdoeleinden bijgehouden zal worden**. Zoals uiteengezet in punten 18 t.e.m. 26 heeft het meldpunt AJH twee opdrachten onder de koepel van 'de aanpak van grensoverschrijdend gedrag'. Enerzijds meldingen ontvangen en er passend gevolg aan geven en anderzijds meldingen over "grensoverschrijdend gedrag" in kaart te brengen en hierover beleidsadviezen te verstrekken. **Tussen deze twee is er een duidelijke afbakening, die ook doorgetrokken moet worden naar de verwerking van de gegevens.** Het is in dat verband merkwaardig dat de aanvrager expliciet stelt dat anonieme meldingen, die tevens in hetzelfde register opgenomen zullen worden, geen identificeerbare gegevens zullen bevatten. Dit houdt, *a contrario*, in dat niet-anonieme meldingen wel identificeerbare gegevens kunnen bevatten. De Autoriteit wijst erop dat met uitsluiting van de anonieme meldingen, **persoonsgegevens bijgehouden kunnen worden voor de behandeling van een melding**. Doch van zodra deze gegevens niet meer noodzakelijk

[40] Noteer in dat verband een gezamenlijke verwerkingsverantwoordelijkheid tot gevolg heeft dat een protocol in de zin van artikel 8 e-govdecreet uitgesloten is – besproken in punten 104 t.e.m. 108.

zijn, lees van zodra er een intern dossier is, mogen deze gegevens in het register niet meer bijgehouden worden of moeten deze gepseudonimiseerd of geanonimiseerd worden. In het kader van beleidsadviezen zijn er twee facetten: enerzijds het voorbereidend werk en anderzijds de aflevering van de adviezen. Aangezien de aanvrager specificeerde dat het meldingsregister bijgehouden zal worden voor beleidsdoeleinden, volgt dat de meldingen *de facto* behandeld zullen zijn geweest en de inhoud bijgevolg gepseudonimiseerd of anonimiseerd horen te zijn. De Autoriteit onderstreept dat dit onderscheiden moet worden van de aflevering van beleidsadviezen en rapporten krachtens de bepalingen besproken in punten 23 t.e.m. 26. Immers wordt krachtens die bepalingen in het ontwerp, uitdrukkelijk gesteld dat het geanonimiseerde gegevens betreft.

65. De verduidelijking dat "*[e]nkel de medewerkers van het meldpunt toegang [hebben] tot het meldingsregister,"* is een vooruitgang op het gebrek aan informatie daaromtrent. Doch blijft de aanduiding van 'medewerkers' uitermate ruim. Het is aangeraden om te werken met gemachtigde personeelsleden, voornamelijk omdat ook de anonieme meldingen inbegrepen zijn in het 'meldingsregister'. Bovendien moet dit register op continue wijze worden nagekeken zodat, stelselmatig persoonlijke gegevens van meldingen die behandeld zijn geweest, gepseudonimiseerd of geanonimiseerd worden en dat anonieme meldingen, gevrijwaardt worden van identificeerbare gegevens. De Autoriteit verwijst naar de observatie in punt 53, aangaande de afweging van de noodzakelijke gegevens voor de verwerking.

66. Voorts merkt de Autoriteit op dat de aanvrager vermelding maakt van het onderscheid tussen het meldingsregister en het inhoudelijk dossier. De vraag stelt zich of ook hier alle 'medewerkers' zonder onderscheid toegang krijgen tot alle inhoudelijk dossiers. Uit het geheel wordt afgeleid dat alle meldingen die binnenkomen, voor elke medewerker, die de opdracht toegekend gekregen heeft om in te staan voor de binnenkomende meldingen, toegankelijk is. Dit doet de Autoriteit vermoeden dat degenen bij ontvangst van een melding instaan om een intern dossier op te starten. Het opstarten, invoegen of aanmaken van dossiers, wilt zeggen dat de toegankelijkheid tot de dossiers voor de werknemers, hoogstwaarschijnlijk vrij ruim geïnterpreteerd moet worden. Hetgeen problematisch is in het licht van de verwerking van de bijzondere categorieën van gegevens en de gevoeligheid die ermee gepaard gaat.

67. Hoewel het antwoord van de aanvrager enigermate van duidelijkheid schept, onderstreept de Autoriteit nogmaals dat het onontbeerlijk is dat het ontwerp zelf, zich uitspreekt over een meldingsregister, het doel, de inhoud ervan, het gebruik en de gemachtigde personeelsleden die er toegang tot hebben. Voorts wordt benadrukt dat de gegevens in een meldingsregister, beperkt moeten zijn tot het absoluut noodzakelijke voor de verwerking. In dat verband verwijst de

Autoriteit naar eerdere adviezen die ingaan op de inhoud van registers, zoals o.m. advies 69/2022.[41]

- Categorieën van betrokkenen

68. Met betrekking tot de **categorieën van betrokkenen** stipuleert artikel 13, §1, lid 2, van het ontwerp, het volgende:

> *"De personen van wie de persoonsgegevens, vermeld in het eerste lid, kunnen worden verwerkt, zijn de melders van grensoverschrijdend gedrag en de personen die betrokkenheid vertonen met de context van het grensoverschrijdend gedrag dat wordt gemeld."*

69. Zoals reeds toegelicht in punt 17, wordt in de Memorie van Toelichting verduidelijkt **dat melders** een onderscheiden hoedanigheid kunnen hebben, namelijk dat van slachtoffers, plegers, verwanten, getuigen, derden en organisaties. De term heeft aldus betrekking op volwassen, jongeren en kinderen, in elke hoedanigheid. Door in het ontwerp op algemene wijze naar melders te verwijzen, rijst de indruk dat er voor de verwerking van persoonsgegevens geen rekening gehouden wordt met essentiële factoren die een verschillende behandeling, een verschillende hoeveelheid gegevens of andere gegevens vereisen. In het licht hiervan dringt de Autoriteit erop aan om verdere specificering te voorzien betreffende de melders, zodat duidelijk wordt dat persoonsgegevens proportioneel worden verwerkt, afhankelijk van hun hoedanigheid en leeftijd. Dit is bovendien in lijn met de behandelingen van anonieme meldingen – zie punt 72 – die consequent ook onder de term 'melder' vallen.

70. Verder wijst de Autoriteit erop dat de omschrijving aangaande "*personen die betrokkenheid vertonen met de context van het grensoverschrijdend gedrag,*" nietszeggend is. Eender wie met een minimale link in dergelijke situatie zou binnen dit toepassingsgebied kunnen vallen. Derwijze kan men bijvoorbeeld denken aan personen, die zelfs incidenteel in dergelijke context aanwezig zijn. Ergo, dergelijke omschrijving zou een vrijgeleide zijn om gegevens te verwerken over personen die in de feiten zelf redundant zijn. Bijgevolg is het onontbeerlijk dat hetgeen beoogd wordt met "*personen die betrokkenheid vertonen met de context van het grensoverschrijdend gedrag,*" verder op nauwkeurige en duidelijk omlijnde wijze beschreven wordt zodat uit de omschrijving klaarblijkelijk en ondubbelzinnig voortvloeit wie bedoeld wordt.

---

[41] Advies 69/2022, randnr. 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.*"

71. Verder koppelt de Autoriteit terug aan de preliminaire opmerking van punt 36, aangaande het verband tussen de verwerkingselementen. Zoals toegelicht in voorgaand punt 69, is het gevolg van een onderscheiden soort gegevens dat enerzijds gewerkt wordt met gegevens die gekwalificeerd worden als zeer gevoelig en daarom ook als dusdanig behandeld moeten worden. Dit impliceert dat er bijkomende beveiligingsmaatregelen in acht genomen moeten worden. Maar anderzijds verantwoordt de hoedanigheid ook of er meer of minder gegevens vereist worden hetgeen onlosmakelijk verbonden is met de verwerking.

- Anonieme meldingen

72. Tenslotte wenst de Autoriteit nader in te gaan **op de mogelijkheid van anonieme meldingen.** In eerste instantie wordt zoals reeds aangegeven in eerdere adviezen **benadrukt dat een anonieme melding optioneel en uitzonderlijk moet blijven**.[42] Zo werd in voorgaande adviezen al aangegeven dat een dergelijke werkwijze "*de communicatie tussen de melder en de bestemmeling van de melding (dewelke nodig is voor een passende opvolging) [bemoeilijkt], bovendien kan dit aanleiding geven tot misbruiken in hoofde van de melders en daarmee gepaard gaande ongeoorloofde verwerking van persoonsgegevens*."[43] De anonimiteit brengt het proces van een controle van de gegrondheid voorts ook in het gedrang. Hoewel de eindverantwoordelijkheid met betrekking tot de verwerking van persoonsgegevens steeds rust bij de respectieve verwerkingsverantwoordelijken, dient ook de melder de nodige verantwoordelijkheidszin aan de dag te leggen; een melding kan immers belangrijke gevolgen hebben voor de geviseerde personen.[44] Tevens merkt de Autoriteit op dat dit ook aan de finaliteit van de gegevens raakt. *In casu*, wordt verwezen naar de observatie in punt 53, aangaande de afweging van de noodzakelijke gegevens voor de verwerking.

73. In tweede instantie wordt op gewezen dat de mogelijkheid om een anonieme melding te maken terloops in de Memorie van Toelichting[45] wordt vermeld en op de website. Onverminderd de aanbeveling van punt 72, is het aangewezen om **de mogelijkheid van een anonieme melding in het ontwerp zelf vast te stellen.** In het verlengde hiervan lijkt het aangeraden **om in het ontwerp zelf te definiëren wat verstaan wordt onder "*anonieme melding*,"** zodat geen verwarring bestaat omtrent de betekenis ervan.[46] Aansluitend is de Autoriteit van oordeel dat

[42] Advies nr. 69/2022, randnr. 20; Advies nr. 142/2022, randnr. 19.

[43] Advies nr. 69/2022, randnr. 20.

[44] Advies nr. 142/2022, randnr. 19.

[45] "Aangezien het meldpunt vertrekt vanuit de noden van de melder, kan een melder ook anoniem melden."

[46] Op vraag van de Autoriteit naar wat begrepen moet worden onder anonieme melding en hoe dit in praktijk zal worden omgezet, preciseerde de aanvrager het volgende: "*Een anonieme melding is een melding zonder identificatie van de melder.*

Met de melder wordt heel duidelijk afgesproken wat al dan niet geregistreerd mag worden. Indien dit door omstandigheden niet gevraagd kan worden (omdat melder een anonieme mail stuurt of anoniem chat of een telefoongesprek afbreekt) worden een aantal vooraf bepaalde registratiegegevens opgenomen, indien deze worden meegedeeld, en waarbij is afgewogen dat de

minstens uit de Memorie van Toelichting moet blijken op welke wijze de anonimiteit van de melder, verzekerd kan worden.

74. De bijzonderheid van een anonieme melding maakt deze niet onverenigbaar met reeds besproken punt 64 aangaande een meldingsregister. Doch is enige voorzichtigheid geboden aangaande hetgeen in een dergelijk register opgenomen wordt. Zo kan er gewerkt worden met een geanonimiseerde opname in een incidentenregister. **Hoe dan ook dringt de Autoriteit erop aan om in het wetsontwerp of minstens de Memorie van Toelichting, verdere duiding te voorzien.**

75. In ieder geval geldt dat waar toch nog contact opgenomen kan worden met een anonieme melder, de decreetgever, een bepaling moet opnemen in het ontwerp, die uitdrukkelijk aangeeft dat de verwerkingsverantwoordelijke steeds in staat moet zijn om het mondeling akkoord te bewijzen.[47]

- Wijze van verwerking

76. Tenslotte gaat artikel 13, §1, lid 3, van het ontwerp, nader in op de wijze waarop de (categorieën van) persoonsgegevens verwerkt kunnen worden. *In casu*, wordt het volgende gestipuleerd:

> "*De persoonsgegevens, vermeld in het eerste lid, kunnen op de volgende wijzen worden verwerkt:*
>
> *1° de personeelsleden van het Agentschap Justitie en Handhaving die instaan voor de operationele werking van het meldpunt AJH, kunnen de persoonsgegevens verwerken om de opdrachten, vermeld in artikel 7, uit te voeren;*
>
> *2° de personeelsleden van het Agentschap Justitie en Handhaving die instaan voor de operationele werking van het meldpunt AJH, kunnen de persoonsgegevens delen met het openbaar ministerie als dat noodzakelijk is voor de afstemming, vermeld in artikel 10, §1, tweede lid;*
>
> *3° de personeelsleden van het Agentschap Justitie en Handhaving die instaan voor de operationele werking van het meldpunt AJH, kunnen de persoonsgegevens delen met het VMRI met het oog op de toepassing van artikel 3, §3, en artikel 4;*
>
> *4° de personeelsleden van het Agentschap Justitie en Handhaving die instaan voor de operationele werking van het meldpunt AJH, kunnen, met het oog op een*

anonimiteit van de melder gevrijwaard blijft en de combinatie van de gegevens geen aanleiding geeft tot een 'identificeerbare' melding : datum van contactname, medium contactname, aard GOG, sector GOG, gender en leeftijd."

[47] Artikel 5(2) AVG; HvJ (Gr. Kamer) 4 juli 2023, ECLI:EU:C:2023:537, nr. C-252/21, Meta / Bundeskartellamt, randnr. 95.

doorverwijzing, de persoonsgegevens delen met de hulpverlening, op voorwaarde dat de persoon die wordt doorverwezen, minstens mondeling zijn akkoord heeft gegeven om die gegevens mee te delen;

5° de personeelsleden van het Agentschap Justitie en Handhaving die instaan voor de operationele werking van het meldpunt AJH, kunnen, met het oog op de toepassing van artikel 8 en als dat noodzakelijk is om de nodige informatie te verkrijgen, gegevens over de melding van grensoverschrijdend gedrag bezorgen aan de organisatie of het interne meldpunt als de melder minstens mondeling zijn akkoord heeft gegeven om die gegevens te bezorgen."

77. Ten aanzien van het eerste punt, stelt de Autoriteit zich – naar analogie met punten 65 en 66 – de vraag of alle personeelsleden toegang hebben tot en alle persoonsgegevens kunnen verwerken of dat **er beperkingen zijn. Dat laatste zou in het licht van het principe van integriteit en vertrouwelijkheid aangewezen** zijn. Voorts zou het de duidelijkheid ten goede komen indien minstens in de Memorie van Toelichting, **een beschrijving gegeven wordt van hetgeen "de operationele werking" omvat**.

78. Ten aanzien van het tweede punt, verwijst de Autoriteit naar punten 107-110 aangaande de doorgifte van persoonsgegevens tussen overheden en het daarmee samenhangende protocol.

79. Ten aanzien van het derde punt, onderstreept de Autoriteit dat voor de doorgifte van persoonsgegevens die onder de gezamenlijke verwerkingsverantwoordelijkheid kaderen er geen protocol vastgesteld moet worden, zoals verder besproken in punten 104 t.e.m. 108. De doorgifte van gegevens moet beperkt zijn tot wat noodzakelijk is voor het doeleinde.

80. Ten aanzien van het vierde punt, is de observatie uit punt 78 eveneens toepasselijk. Verder merkt de Autoriteit op dat er een voorafgaande (en minstens mondeling) akkoord van de doorverwezen persoon vereist wordt, alvorens over te gaan tot een doorgifte. Binnen dit kader kan een (minstens mondeling) akkoord, gelijkgesteld worden met een toestemming. Consequent is het kader van geldige toestemming hier toepasselijk. Zo dient toestemming vrij, geïnformeerd, specifiek en ondubbelzinnig te zijn.[48] Terzake merkt de Autoriteit op dat het mondelinge akkoord een heikel punt is. Een mondeling akkoord kan *i) in een vlaag van emotie gegeven worden; ii) verkeerd geïnterpreteerd worden; kan betwist worden; is moeilijk aantoonbaar, etc*. **Tegen deze**

[48] De betrokkene die instemt moet een werkelijke keuze krijgen, zonder dat er enige sprake is van bedrog, intimidatie of dwang en geen aanzienlijke negatieve gevolgen loopt bij weigering. Alvorens toestemming te verlenen moet de betrokkene over informatie beschikken die kwalitatief, gemakkelijk toegankelijk is, begrijpbaar nauwkeurig en volledig is. Deze toestemming moet specifiek worden gegeven voor het doel van de verwerking, die duidelijk en op ondubbelzinnige wijze moet worden beschreven. Deze toestemming moet voorts ondubbelzinnig zijn, in die mate dat er geen redelijke twijfel mag bestaan over het feit dat de betrokkene zijn toestemming gegeven heeft.

achtergrond vraagt de Autoriteit, aan de decreetgever, om een bepaling in het ontwerp op te nemen die de verwerkingsverantwoordelijke verplicht om steeds aan te kunnen tonen dat een mondeling akkoord gegeven is geweest. Daarnaast moet **minstens in de Memorie van Toelichting, gespecifieerd worden hoe de andere voorwaarden van een geldige toestemming in de zin van de AVG[49] bewerkstelligd worden**, en in het bijzonder t.a.v. minderjarigen (ouder en jonger dan 13 jaar).

81. Ten aanzien van het vijfde punt, gelden de observaties in punten 78 en 80 aangaande het protocol voor doorgifte en het kader van de geldige toestemming, naar analogie. De Autoriteit begrijpt dat om personen te horen, informatie in te winnen of documenten op te vragen, zoals gestipuleerd in artikel 8 van het ontwerp, er ook enige vorm van informatie gegeven moet worden om enerzijds te kaderen welke gegevens noodzakelijk zijn, en anderzijds dergelijke handelingen te verantwoorden. **Niettemin gaat het desbetreffende artikel over het bekomen van bijkomende informatie en niet de doorgifte van gegevens**. In de mate dat gegevens die verstrekt worden niet als algemeen beschouwd kunnen worden en de identiteit van de betrokkene uit blijkt, moet minstens de noodzakelijkheid gemotiveerd worden. Terzake vraagt de Autoriteit om in artikel 13, §1, lid 3, 5°, van het ontwerp, te preciseren dat de noodzakelijkheid steeds gemotiveerd moet worden. Gelet op de verregaande bevoegdheid die artikel 8, van het ontwerp, met zich meebrengt, wordt ook een kanttekening gemaakt bij het statuut dat samengaat met de opdracht. Het ontwerp geeft geen aanwijzing over het kader en de personen die dergelijke opdrachten mogen uitvoeren. Bijgevolg lijkt elke werknemer van het meldpunt AJH in aanmerking te kunnen komen om personen te horen, informatie in te winnen of documenten op te vragen. Dergelijke ruime opdracht lijkt disproportioneel en vormt dusdanig onvoldoende waarborgen t.a.v. de betrokkenen. **De Autoriteit dringt erop aan om een onderscheid te maken in de categorieën personen die enerzijds toegang krijgen tot inhoudelijke dossiers, meldingsregister, maar ook die onder een bijzonder statuut vallen die de opdrachten onder artikel 8 verantwoorden.** Daarnaast merkt de Autoriteit ook op dat er onvoldoende omkadering is in artikel 8, van het ontwerp, zodat eender welk gegeven opgevraagd lijkt te kunnen worden.

e. Authenticatie en beschikbaarheid

82. De in het ontwerp beoogde gegevensverwerking heeft gedeeltelijk betrekking op een bijzondere categorie van gegevens, waarvan de verwerking in principe verboden is.[50] Dit verbod is echter niet van toepassing wanneer "*de verwerking noodzakelijk [is] om redenen van zwaarwegend*

[49] EDPB, Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679. Te raadplegen via: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_nl.pdf.

[50] Artikel 9(1) AVG.

algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen[51] *worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene*."[52]

83. Deze passende en specifieke maatregelen kaderen binnen artikel 5(1)(f) AVG die bepaalt dat een passende beveiliging van de verwerking van gegevens gewaarborgd moet worden door het nemen van passende technische of organisatorische maatregelen, zodat bescherming geboden wordt tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (principe van integriteit en vertrouwelijkheid).[53] De draagwijdte van dit beginsel is niet alleen essentieel om duidelijk te bepalen welke persoonsgegevens kunnen of mogen worden verwerkt, maar ook hoe dat moet gebeuren en met name hoe dat die gegevens daarbij moeten worden beveiligd.[54]

84. Het beginsel van vertrouwelijkheid, integriteit en beschikbaarheid van persoonsgegevens kan bewerkstelligd worden met de invoering van beveiligingsmaatregelen in de zin van artikel 32 van de AVG, die de integriteit, authenticiteit en beschikbaarheid van persoonsgegevens garanderen en vermijden dat persoonsgegevens onrechtmatig vernietigd of ongeoorloofde bekendgemaakt zouden worden. Het is ook noodzakelijk om garanties te bieden met betrekking tot de mogelijkheid om de verwerking van persoonsgegevens te controleren (controle van wie wat heeft gedaan, met welke persoonsgegevens en op welk tijdstip). Deze maatregelen moeten een passend veiligheidsniveau waarborgen, rekening houdend met de aard van de te beschermen gegevens en de potentiële risico's.

85. Bovendien, in de mate dat het betrekking heeft op persoonsgegevens die strafbare feiten kunnen vormen als bedoeld in artikel 10 van de AVG, zijnde, "persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten," moet de verwerkingsverantwoordelijke en, in voorkomend geval, zijn verwerker ook een lijst opstellen van de categorieën van personen die toegang hebben tot de persoonsgegevens, met een beschrijving van hun functie in het kader van de verwerking van de betrokken gegevens. Deze lijst wordt ter beschikking gehouden van de bevoegde toezichthoudende autoriteit. [55]

---

[51] Onderstreping toegevoegd door de Autoriteit.

[52] artikel 9(2)(g) AVG.

[53] Artikel 5(1)(f) AVG.

[54] D., De Bot, *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*. Wolters Kluwer Belgium, 2020, 501.

[55] artikel 10, § 2, van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

- Vertrouwelijkheid

86. In het ontwerp, heeft vertrouwelijkheid, twee invalshoeken, die in aanmerking genomen moeten worden voor de beoordeling. Zo stelt artikel 10, §2 van het ontwerp, het volgende:

> "*De documenten die worden opgemaakt en de mededelingen die worden gedaan in het kader van een bemiddelingsgesprek of herstelgesprek als vermeld in artikel 7, tweede lid, 7°, zijn vertrouwelijk. De voormelde vertrouwelijkheid is niet van toepassing op de documenten waarvoor de partijen instemming verlenen om de gerechtelijke instanties en de geschillenkamer van het VMRI, vermeld in artikel 34 van het decreet van 28 oktober 2022, ervan op de hoogte te brengen.*"

87. Vooreerst wordt gevraagd, om in voormeld artikel, dat de term 'instemming' te vervangen met 'toestemming'.

88. Hieruit volgt dat hetgeen aan bod komt in het kader van een bemiddelingsgesprek of herstelgesprek als vertrouwelijk bestempeld wordt. Het is onduidelijk voor de Autoriteit of het bemiddelingsgesprek die onder artikel 7, lid 2, 7°, van het ontwerp gelijkgesteld kan worden met een bemiddelingsprocedure onder het Gerechtelijk Wetboek. In het positieve geval, gelden al de bepalingen m.b.t. bemiddeling van het Gerechtelijk Wetboek onverminderd.

89. In het negatieve geval, is er ruimte voor interpretatie en invulling. Ofschoon verondersteld wordt dat de globale beginselen van bemiddeling, m.b.t. 'vertrouwelijkheid', hier nog een rol zullen spelen, zorgt de vrijere invulling voor ambiguïteit. Immers wordt expliciet gesteld dat vertrouwelijkheid uitgesloten is voor de documenten waarvoor "*de partijen instemming verlenen om ze […] [te delen].*" Dit geeft aanleiding tot een aantal vragen, met name:

I. Wat omvat de term 'partijen'? In het kader waar bemiddeling dezelfde invulling krijgt als onder het Gerechtelijk Wetboek, moeten alle partijen akkoord zijn. Doch zitten we hier in een situatie waar ruimere invulling mogelijk is. Bijgevolg zou idealiter vermeld moeten worden of alle partijen unaniem moeten instemmen of niet.

II. De besproken paragraaf betreft bemiddelingsgesprekken of herstelgesprekken. Bijgevolg wordt aangenomen dat de vrijstelling van vertrouwelijkheid alleen betrekking heeft op de documenten – waarvoor partijen toestemming geven, zoals uiteengezet in voorgaand punt en – die aan bod komen tijdens het bemiddelingsgesprek of herstelgesprek. Indien de uitzondering dusdanig is dat vertrouwelijkheid op eender welk document uitgesloten kan worden met instemming van de partijen, waarvan dat laatste ook verdere duiding vereist, vraagt de Autoriteit om dit afzonderlijk te kaderen en toe te lichten.

III. De impact die de invulling uit punten i en ii tot gevolg kan hebben, brengt de Autoriteit ertoe om een kanttekening te maken bij het determinerend gewicht dat verbonden kan worden aan de inhoud van dergelijke documenten, in gerechtelijke procedures. Hetgeen vragen doet rijzen t.a.v. de rechten van verdediging, het hoorrecht bij de vorming of opmaak van deze documenten.

IV. De rechten van de betrokkenen worden later besproken in punten 123 t.e.m. 133.

90. Samenhangend met het vertrouwelijkheidsbeginsel is het beroepsgeheim, die ingevoerd wordt door artikel 14, van het ontwerp, en het volgende stelt:

> "*De personeelsleden van het Agentschap Justitie en Handhaving die betrokken zijn bij de operationele werking van het meldpunt AJH, zijn onderworpen aan het beroepsgeheim conform artikel 458 van het Strafwetboek.*"

91. Beroepsgeheim omvat in de eerste plaats alles wat wordt besproken met een persoon die wettelijk wordt geacht een beroepsgeheim te hebben vanuit zijn functie en/of beroep. Daarnaast valt ook informatie onder het beroepsgeheim die expliciet of impliciet aan een vertrouwenspersoon is toevertrouwd, evenals alle informatie die wordt gezien of gehoord tijdens de uitoefening van het beroep. Dit omvat ook informatie over derden en bedrijfsgeheimen.[56]

92. Niettemin worden ook een aantal uitzonderingen bepaald in het ontwerp. In eerste instantie een expliciet in de norm bepaalde vrijstelling van het beroepsgeheim in volgende artikelen:
    - artikel 8, lid 4, van het ontwerp, stipulerend dat "*[d]e personen die […] gevraagd [worden] om informatie of documenten te bezorgen, […] ten aanzien van het meldpunt ontheven [zijn] van hun plicht tot geheimhouding over feiten waarvan ze op de hoogte zijn en over gegevens waarover ze beschikken door hun staat of beroep, met uitzondering van de gegevens die door het medisch geheim beschermd zijn*."[57]
    - artikel 17, van het ontwerp, die het volgende stelt: "*Medewerkers in sectoren en van organisaties waarvoor de Vlaamse Gemeenschap of het Vlaamse Gewest bevoegd is, kunnen, met het oog op de bescherming van de integriteit van een slachtoffer, grensoverschrijdend gedrag waarvan ze bij de uitoefening van hun beroep kennis hebben gekregen, bij het Vlaams Meldpunt voor Grensoverschrijdend Gedrag melden zonder dat die medewerkers wegens eventuele miskenning van het beroepsgeheim strafbaar kunnen*

[56] V. Dooms, « Hoofdstuk 5. - Raakvlakken tussen privacy en beroepsgeheim » in Blockx, F. *et al.* (ed.), *De uitholling van het beroepsgeheim?*, 1e editie, Bruxelles, Intersentia, 2018, 94-95.

[57] De Memorie van Toelichting licht verder toe Deze personen die gevraagd worden informatie en documentatie over te leggen zijn ten aanzien van het meldpunt ontheven van hun plicht tot geheimhouding in verband met feiten waarvan zij kennis hebben en gegevens waarover zij beschikken door hun staat of beroep, met uitzondering van die welke door het medisch geheim beschermd. Deze bepaling heeft geen impact op de reeds bestaande concepten zoals het gedeeld beroepsgeheim, de noodtoestand en het gezamenlijk beroepsgeheim. Deze blijven van toepassing.

worden gesteld op basis van artikel 458 van het Strafwetboek. De medewerkers kunnen ***alleen de noodzakelijke informatie*** *meedelen aan het meldpunt als ze de integriteit van het slachtoffer niet zelf of met behulp van anderen kunnen garanderen*."[58]

93. De Autoriteit wenst een kanttekening op te merken met betrekking tot de zeer ruime uitzondering die wordt geïntroduceerd in artikel 17 van het ontwerp. Uit dit artikel blijkt dat het beroepsgeheim kan worden doorbroken zonder dat er een vereiste van enige ernst aanwezig is. Dit roept considerabele bezorgdheid op, aangezien het beroepsgeheim cruciaal is voor het onderhouden van een vertrouwensrelatie. Als het beroepsgeheim zonder enige vorm van ernst kan worden doorbroken, kan dit de vertrouwensrelatie aantasten en ondermijnen. Het verdient de aanbeveling om hier rekening mee te houden bij de aanpassing van het ontwerp.

94. Daarnaast verdient het de aanbeveling om **verdere duiding te geven omtrent hetgeen deel uitmaakt van "*noodzakelijke informatie.*"**

95. In tweede instantie de **situaties waar de betrokken persoon akkoord gaat met de vrijgave van informatie.[59]** Het gaat desbetreffend om artikelen: **[60]**
    - artikel 13, §1, lid 3, 5°, van het ontwerp – zoals uiteengezet in punt 81 – waarbij een mondeling akkoord van de melder vereist is voor de doorgifte van gegevens;
    - artikel 3, §3, van het ontwerp, stelt dat in overleg tussen het VMRI of het meldpunt AJH en in overleg met de melder of klager, beoordeeld wordt of een melding samen of afzonderlijk behandeld wordt door het VMRI of het meldpunt AJH;
    - artikel 7, lid 2, 4°, van het ontwerp, betreffende de warme doorverwijzing naar een extern aanbod;[61]
    - artikel 10, §2, van het ontwerp – zoals reeds besproken in punten 86 t.e.m. 89 – die de betrokkenen van een geheimhoudingsplicht ontslaat voor documenten waar de partijen instemmen om ze met gerechtelijke instanties of de geschillenkamer van het VMRI te delen.

---

[58] Vet toegevoegd door de Autoriteit.

[59] Zie hiervoor eerder geleverd advies nr. 142/2022 van 19 juli 2022, randnr. 45 betreffende een gelijkaardig kader en de vereiste van een uitdrukkelijke toestemming bij de bekendmaking van de identiteit van de melder aan anderen dan de gemachtigden personeelsleden die bevoegd zijn voor ontvangst en opvolging.

[60] De Autoriteit koppelt terzake terug aan punt 80, aangaande het kader voor een geldige toestemming, die hier naar analogie ook geldt.

[61] Memorie van Toelichting stelt dienaangaande het volgende: "*Het bieden van warme doorverwijzing houdt in dat wanneer een ander aanbod beter aansluit bij de vraag van de melder en als de melder hiermee akkoord gaat, hij/zij kan worden toegeleid naar een passend hulpaanbod zoals een CAW, lotgenotengroep, politie,… Afhankelijk van de noden van de melder worden contactgegevens bezorgd aan de melder, kan de dossierbehandelaar een afspraak maken voor de melder bij de dienst waarnaar verwezen wordt of kan gevraagd worden aan de dienst waarnaar verwezen wordt om actief contact te nemen met de melder. Mits uitdrukkelijke toestemming van de melder kan info-overdracht plaatsvinden zodat de melder niet alles opnieuw moet vertellen*."

96. In derde instantie de situaties die onder een noodsituatie kaderen of indien er een noodsituatie dreigt. Het ontwerp stelt met artikel 6, 3°, van het ontwerp, dat "*bij de uitvoering van de opdrachten, vermeld in artikel 7, […] de veiligheid van de slachtoffers of potentiële slachtoffers centraal geplaatst [wordt]*." Terzake licht de Memorie van Toelichting verder toe dat dat het meldpunt acties kan ondernemen, conform de meldrechten en hulpverleningsverplichting, als een (potentieel) slachtoffer actueel en/of acuut gevaar loopt.[62] De Autoriteit wijst in dat verband naar een mogelijke overlapping met de laatste zin uit artikel 10, §1, lid 2, van het ontwerp – die later in punten 111 t.e.m. 113 aan bod komt – aangaande het voorafgaande akkoord van de melder en het Openbaar Ministerie.

97. Informatie waarbij alle concrete namen en details zijn weggelaten, zodat het een situatiebeschrijving in algemene termen wordt, behoort niet tot het beroepsgeheim.[63] In de mate dat artikel 10, §1, van het ontwerp, niet verder gaat, kan de vrijgave van informatie hieronder worden ingedeeld. **In het tegengestelde geval moet de uitzondering van de kennisgeving worden opgenomen in het ontwerp**. Hoe dan ook moet de doorgifte van gegevens beperkt blijven tot het absoluut noodzakelijke, aangezien het nog steeds om persoonsgegevens kan gaan.

98. Voorts wijst de Autoriteit op andere situaties die niet in het ontwerp opgenomen zijn, maar desgevallend ook een uitzondering op het beroepsgeheim kunnen rechtvaardigen o.m. bij ouders van een minderjarige, aangezien zij aansprakelijk zijn en beslissingsrecht hebben over fundamentele aspecten van de opvoeding zoals onderwijs en gezondheid of bij wilsonbekwaamheid.[64] De Autoriteit leidt uit de precisering van de aanvrager dat deze uitzondering niet aanmerking genomen wordt.[65] **Gelet op de zeer brede definitie van "grensoverschrijdend gedrag," verdient de aanbeveling om in het ontwerp of minstens in de Memorie van Toelichting in te gaan op deze uitzonderingssituaties.**

---

[62] Dienaangaande stelt de Memorie van Toelichting het volgende: "De *veiligheid van de slachtoffers of potentiële slachtoffers staat centraal.* ***Als een (potentieel) slachtoffer actueel en/of acuut gevaar loopt, kan het meldpunt acties ondernemen,*** *door bijvoorbeeld politie in te schakelen of een organisatie (al dan niet anoniem) op de hoogte te brengen van de melding. Ook als er kans is dat er in de toekomst andere personen slachtoffer kunnen worden van eenzelfde vermeende pleger of eenzelfde situatie, kan het meldpunt acties ondernemen, dit steeds conform bestaande meldrechten (bv. artikel 458bis Sw. of de noodtoestand) en de hulpverleningsplicht (o.b.v. artikel 422bis Sw.).*"

[63] V. Dooms, "Raakvlakken tussen privacy en beroepsgeheim" in F., Blockx , P., Hoet, B. Dejmeppe, V., Dooms, T., Goffin, P., Hoet en J. Van Malleghem (ed.), *De uitholling van het beroepsgeheim?*, 1e editie, Brussel, Intersentia, 2018, 94.

[64] V. Dooms, "Raakvlakken tussen privacy en beroepsgeheim" in F., Blockx, et al. (ed.), *De uitholling van het beroepsgeheim?*, 1e editie, Brussel, Intersentia, 2018, 94.

[65] Op de vraag van de Autoriteit betreffende gevallen met minderjarigen onder 13 jaar en meldingen door hen of over hen, en de wijze waarop dit zich verhoudt t.o.v. ouders, in zaken waar ouders niet als plegers gecategoriseerd kunnen worden antwoorde de aanvrager als volgt: " *We vertrekken vanuit de principes van het burgerlijk recht die stellen dat een minderjarige tot aan zijn/haar meerderjarigheid principieel onder het gezag van zijn/haar ouders valt en ouders als wettelijke vertegenwoordigers de rechten van hun minderjarige kinderen uitoefenen.*

Een minderjarige, ook onder 13 jaar, kan een melding maken bij het Meldpunt. Ook hier zijn de dossierbehandelaars gebonden door het beroepsgeheim maar zullen ze zoveel mogelijk proberen de minderjarige aan te zetten om in gesprek te gaan met zijn/haar ouders."

99. Het geheel in acht genomen, komt de Autoriteit tot het besluit dat de passende en specifieke maatregelen die ingevoerd werden o.m. de vertrouwelijkheidsvereiste en het beroepsgeheim zijn. Dat beroepsgeheim lijkt zonder uitzondering op alle personeelsleden van het Agentschap Justitie en Handhaving die instaan voor de operationele werking van het meldpunt betrekking te hebben. **Doch zoals aangegeven in punten 66 en 77, kan niet exact afgeleid worden wie hieronder valt. Dienaangaande vraagt de Autoriteit om dit verder te specifiëren.**

100. Buiten het feit dat inhoudelijke dossiers toegankelijk zijn voor werknemers, kan de Autoriteit nergens uit afleiden dat de toegang tussen de werknemers beperkt zou worden.[66] Bijgevolg lijkt deze leemte te impliceren dat werknemers van het meldpunt AJH allemaal evenveel toegang krijgen tot interne dossiers – zoals ook eerder uiteengezet in punten 66 en 77. De Autoriteit wijst met het oog op de beveiliging dat ook intern gewerkt zou moeten worden met autorisaties. Op deze manier wordt de toegang tot de inhoudelijke dossiers enerzijds beperkt tot een kleinere groep mensen, maar anderzijds wordt er ook bijgehouden wie het dossier heeft kunnen bekijken of aanpassen. Hoe dan ook, geldt – zoals aangehaald in punt 85 – dat er opgelijst moet worden welke categorieën van personen toegang hebben tot de gegevens die onder artikel 10 AVG vallen.

101. De opgesomde uitzonderingen die uit het ontwerp blijken, dienen strikt geïnterpreteerd te worden en desgevallend verder toegelicht en / of gespecifieerd.

- <u>Integriteit</u>

102. Zoals aangehaald in punten 57 t.e.m. 59 is de Autoriteit van mening dat het huidige systeem, m.n. een SharePoint systeem, onvoldoende betrouwbaar is om het hoofd te bieden aan mogelijke ongeoorloofde of onopzettelijke wijzigingen van persoonsgegevens.[67] Bovendien geldt overeenkomstig de observatie van punt 100, dat een open toegang risico's met zich meebrengt t.a.v. de juistheid en volledigheid van de gegevens. In het licht hiervan wordt ten strengste aangedrongen om in afwachting van een nieuw systeem maatregelen te implementeren, zoals tweefactorauthenticatie, uitgebreide logging en encryptie. Vervolgens kan worden overwogen om een specifieke oplossing te selecteren die een hoger niveau van beveiliging kan bieden, afgestemd op de specifieke behoeften en vereisten van de gevoelige gegevens.

103. Ofschoon niet aangegeven wordt hoe een doorgifte van gegevens zal plaatsvinden, wenst de Autoriteit alvast op te merken dat het verzenden van een e-mail met het inhoudelijke dossier in bijlage of waarvan gegevens van het inhoudelijke dossier in verwerkt zijn, geen passende

[66] Bijvoorbeeld tot eigen dossiers.

[67] D., De Bot, *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*. Wolters Kluwer Belgium, 2020, 785.

beveiliging waarborgt. Naar analogie met eerder geleverd advies 160/2023 geldt dat een e-mail als medium onvoldoende veilig is volgens de maatstaven van de organisatorische maatregelen.[68] In dat verband verwijst de Autoriteit naar de aanbevelingen en goede praktijken die aangekaart werden betreffende het gebruik van communicatiekanalen voor de verzending van gegevens die als bijzonder of uiterst gevoelig kwalificeren.[69]

f. Doorgifte

- De doorgifte van gegevens tussen het meldpunt AJH en het VMRI:

104. Krachtens artikel 3, §2, lid 2, van het ontwerp, zal de samenwerking van het meldpunt AJH en het VMRI aan de verwezenlijking van de aanpak van grensoverschrijdend gedrag vastgesteld worden in een samenwerkingsprotocol, zoals hiernavolgend weergeven:

"*De samenwerking, vermeld in het eerste lid, wordt vastgelegd in een samenwerkingsprotocol.*"

105. Verdere vermeldingen van het samenwerkingsprotocol kan men vinden onder:

- artikel 3, §3, lid 4, van het ontwerp: "*In het samenwerkingsprotocol, vermeld in paragraaf 2, tweede lid, worden* ***nadere afspraken gemaakt over het overmaken en de centrale registratie van meldingen en klachten*** *als vermeld in het eerste lid, tussen het VMRI en het meldpunt AJH*";
- artikel 6, lid 2, van het ontwerp: "*Met het oog op de toepassing van het werkingsprincipe, vermeld in het eerste lid, 4°,* ***zal het meldpunt AJH een samenwerkingsprotocol sluiten met de betreffende overheden die afhangen van*** *de Vlaamse Gemeenschap of het Vlaamse Gewest, voor zover deze laatste dit wenselijk achten*";
- artikel 25, van het ontwerp, die een vierde lid toevoegt aan het VMRI decreet: "*Het VMRI werkt structureel samen met het meldpunt AJH om samen het Vlaams Meldpunt Grensoverschrijdend Gedrag te vormen.* ***De voormelde samenwerking wordt vormgegeven in een samenwerkingsprotocol****. In het samenwerkingsprotocol worden conform artikel 13, §3, vierde lid, onder meer afspraken gemaakt over het uitwisselen van meldingen en klachten tussen het meldpunt AJH en het VMRI en over de jaarlijkse rapportage over meldingen en klachten."*

106. De Autoriteit vermoedt dat de decreetgever aan de term 'samenwerkingsprotocol', dezelfde invulling geeft als aan de term 'protocol' die respectievelijk uit artikel 20 van de wet van 30 juli

[68] Terzake kan een e-mail gehackt worden, een bestaand e-mail kan nagemaakt worden, versturen van e-mails naar onbevoegde personen, zwakke wachtwoorden, etc.

[69] Advies nr. 160/2023, randnrs. 17-28.

2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens – die het beginsel van protocolplicht vastlegt voor de doorgifte van gegevens tussen overheden – en artikel 8 van het decreet betreffende het elektronische bestuurlijke gegevensverkeer (hierna: e-govdecreet), volgt.

107. In het licht hiervan vestigt de Autoriteit de aandacht op artikel 8, §1 van de e-govdecreet dat het volgende stelt:

> "*Elke elektronische mededeling van persoonsgegevens door een instantie naar een andere instantie of naar een externe overheid of naar een private organisatie vereist een protocol, gesloten tussen de betreffende verwerkingsverantwoordelijken.* ***Tussen gezamenlijke verwerkingsverantwoordelijken worden geen protocollen gesloten.***"

108. Doch werd eerder – in punten 27 t.e.m. 32 – reeds toegelicht dat uit de gezamenlijke doelstelling in het ontwerp, de overlappende bevoegdheden en de convergerende beslissingen die een verwerking tot gevolg hebben, impliciet afgeleid kan worden, dat er een gezamenlijke verwerkingsverantwoordelijkheid is tussen het AJH en het VMRI. **Bijgevolg stelt de Autoriteit vast dat de opzet van een samenwerkingsprotocol uit het ontwerp onverenigbaar is met het bestaande normatieve kader.**

- <u>De doorgifte tussen het meldpunt AJH en andere, dan het VMRI, organisaties of tuchtorganen:</u>

109. Het ontwerp voorziet krachtens artikel 10, §1, lid 1, van het ontwerp, in de mogelijkheid voor het meldpunt AJH om na te gaan of er over de feiten die het voorwerp van de melding uitmaken, reeds een lopend traject is bij een andere instantie, zoals hiernavolgend weergeven:

> "*Het meldpunt AJH gaat bij een melding na of er over de feiten die het voorwerp uitmaken van de melding, reeds een lopend traject is bij een andere instantie, waaronder een intern meldpunt binnen een organisatie of een tuchtorgaan.[…]*"

110. Dit houdt onder meer in dat er een doorgifte van gegevens zal plaatsvinden. In dat verband verwijst de Autoriteit naar punt 107, en artikel 8 van het e-govdecreet, aangaande de verplichting van de invoering van een protocol voor de doorgifte van gegevens tussen overheden. In de mate dat de doorgifte plaatsvindt met een andere instantie, die niet het VMRI is in het kader van de gezamenlijke verwerkingsverantwoordelijkheid of enige andere instantie waarmee het meldpunt AJH als gezamenlijke verwerkingsverantwoordelijke gekwalificeerd kan worden, **<u>is het gebruik en vastlegging van een protocol aan de orde. Bovendien benadrukt de Autoriteit dat het protocol op zich geen wettelijke basis vormt voor de toelating van gegevensmededelingen</u>.** Elke uitwisseling op basis van artikel 6.1.e) AVG hoort hoe dan ook

over een duidelijke wettelijke grondslag te beschikken **vooraleer de gegevensuitwisseling en de daarbij horende afsluiting van een protocol mogelijk is**. De Commissie voor de bescherming van de persoonlijke levenssfeer benadrukte dit trouwens ook in punt 154 van haar advies nr. 33/2018 van 11 april 2018.[70] De Autoriteit is daarom van mening dat het voor advies voorgelegd ontwerp, een passend kader moet bieden voor deze gegevensuitwisseling overeenkomstig de vereiste voorspelbaarheidscriteria (artikel 6.3 van de AVG), zodat dit ontwerp de rechtsgrondslag daarvoor vormt.

111. Daar waar de feiten uit de melding het voorwerp uitmaken van een strafrechtelijk onderzoek of vervolging stelt artikel 10, §1, lid 2, van het ontwerp het volgende:

"Bij een lopend strafrechtelijk onderzoek of in geval van strafrechtelijke vervolging kan het meldpunt AJH de deelopdrachten, vermeld in artikel 7, tweede lid, 1° tot en met 6°, van dit decreet, uitvoeren. Om de deelopdracht, vermeld in artikel 7, tweede lid, 7°, van dit decreet, uit te voeren, verwijst het meldpunt AJH bij een lopend strafrechtelijk onderzoek of in geval van strafrechtelijke vervolging naar de organisaties die hiertoe gesubsidieerd worden conform hoofdstuk 2 van het besluit van de Vlaamse Regering van 15 februari 2019 houdende de subsidiëring van initiatieven die voorzien in een herstelgericht en constructief hulp- en dienstverleningsaanbod voor verdachten, in verdenking gestelde personen, beklaagden, veroordeelden of geïnterneerden, en voor slachtoffers van misdrijven, alsook voor hun onmiddellijke omgeving, dat niet wordt verstrekt ter uitvoering van een beslissing van een gerechtelijke of administratieve overheid. ***Als het meldpunt AJH het voornemen heeft om bepaalde acties te ondernemen met betrekking tot de melding van grensoverschrijdend gedrag, met uitzondering van acties naar de melder toe, stemt het meldpunt AJH voorafgaand en met akkoord van de melder af met het openbaar ministerie****.*

112. Ook hier geldt naar analogie met punten 107 en 110, dat elke doorgifte aan de vastlegging van een protocol onderhevig is.

113. Met het oog op de voorzienbaarheid vraagt de Autoriteit om minstens in de Memorie van Toelichting verdere duiding te geven over hetgeen bedoeld wordt met "*bepaalde acties te ondernemen met betrekking tot de melding van grensoverschrijdend gedrag.*" In dit verband is het onduidelijk of het betrekking heeft op i) alle acties; ii) acties die tot een strafrechtelijk onderzoek kunnen leiden; iii) acties m.b.t. het horen van andere personen of het inwinnen van informatie en opvragen van documenten, krachtens artikel 8 van het ontwerp. Bovendien volgt uit "*met uitzondering van acties naar de melder toe, stemt het meldpunt AJH voorafgaand en met*

[70] CBPL, advies van 11 april 2018, nr. 33/2018, randnr. 154.

akkoord van de melder af met het openbaar ministerie," dat er eerst een toestemming van de melder moet zijn, alvorens het meldpunt AJH zich naar het Openbaar Ministerie mag richten, tenzij voor de acties die naar de melder toe gericht zijn.[71] Voor acties naar de melder toe zal er consequent geen voorafgaand akkoord van de melder worden gevraagd, maar zal rechtstreeks overleg plaatsvinden met het Openbaar Ministerie.

g. Bewaartermijn

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

115. Ter zake bepaalt artikel 13, §4, van het ontwerp het volgende:

"*De persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor het doeleinde, vermeld in artikel 3 §1, tweede lid. De maximale bewaartermijn van de persoonsgegevens die verwerkt worden naar aanleiding van een melding van grensoverschrijdend gedrag, bedraagt tien jaar. De voormelde termijn vangt aan op de datum dat het dossier bij het meldpunt wordt afgesloten."*[72]

116. Op vraag naar de motivering van een bewaartermijn die beschreven wordt als 'zolang als noodzakelijk', stelde de aanvrager het volgende:[73]

"*Persoonsgegevens worden niet langer bewaard dan noodzakelijk en maximaal 10 jaar. Wat noodzakelijk is, hangt af van de specifieke casus. Noodzakelijk om de melding van grensoverschrijdend gedrag op een correcte manier te kunnen aanpakken, om duplicaten te vermijden, "veelmelders" te herkennen en informatie beschikbaar te houden zodat deze indien de melder dit wenst in de toekomst nog kan gebruikt worden.*

We denken hier bijvoorbeeld aan slachtoffers van seksueel ongewenst gedrag. Zij moeten vaak al een grote drempel overwinnen om een melding te maken bij een officiële instantie en een heel traject van empowerment doorlopen vooraleer ze klaar zijn om naar de organisatie of vermeende pleger te stappen."

---

[71] Noteer dat het kader van geldige toestemming hier wederom van toepassing is, met de aanbeveling om te werken met een wettelijke bepaling die de verwerkingsverantwoordelijke verplicht om steeds een mondeling akkoord te kunnen bewijzen.

[72] Onderstreping toegevoegd door de Autoriteit.

[73] Op de vraag of een redelijk een redelijk termijn voor opvolging, beantwoording of reactie na melding of uitgebreide vraagverheldering voorzien wordt, beantwoorde de aanvrager het volgende: "*De doorlooptijden zijn moeilijk vooraf te bepalen gezien de gevoeligheid en complexiteit van de dossiers, denk bijvoorbeeld aan een casus over een universiteitsprofessor die al jaren zijn assistentes lastigvalt*."

117. Het ontwerp zelf, stelt dat persoonsgegevens die verwerkt worden naar aanleiding van een melding, niet langer dan noodzakelijk en maximaal tien jaar bijgehouden worden na afsluiting van het dossier. De connotatie die in dergelijke formulering schuilt valt niet weg te cijferen. De bijkomende toelichting van de aanvrager, stelt terecht dat de noodzakelijkheid geval per geval beoordeeld moet worden. Dit neemt niettemin niet weg **dat het nog steeds aan objectieve criteria van gegevensbewaring ontbreekt, op grond waarvan een exacte periode van bewaring van gegevens – die kan variëren tot maximum 10 jaar na afsluiten van het dossier –** kan worden vastgesteld om ervoor te zorgen dat een dergelijke periode tot het strikt noodzakelijke beperkt blijft.[74] De Autoriteit herinnert eraan dat zelfs een "*oorspronkelijk rechtmatige verwerking van gegevens na verloop van tijd onverenigbaar kan worden met [de AVG], wanneer deze gegevens niet langer noodzakelijk zijn voor dergelijke doeleinden en dat de gegevens moeten worden gewist zodra deze doeleinden zijn bereikt.*"[75] Bovendien merkt de Autoriteit op dat het ontwerp niet expliciet in een afzonderlijke maximumbewaartermijn voorziet voor de verschillende categorieën van persoonsgegevens. De Autoriteit is van mening dat het disproportioneel is om alle gegevens, ongeacht hun aard, voor een gelijke maximumbewaartermijn bij te houden. In het licht hiervan moet het ontwerp dusdanig worden aangepast zodat **het evenredige karakter van gegevensbewaring na de periode waarin de melding daadwerkelijk in behandeling is geweest, uitdrukkelijk gerechtvaardigd wordt.[76] De** afzonderlijke maximumtermijnen voor de verschillende gegevenscategorieën, waarvan de noodzaak en evenredigheid naar behoren worden gemotiveerd, moeten dan in het bijzonder vastgesteld worden. **Zo niet, dan is de Autoriteit van mening dat de maximale bewaartermijn niet langer dan 1 jaar mag zijn na afsluiting van het dossier.[77]**

118. De Autoriteit wijst erop dat, ongeacht een geval per geval beoordeling, er in bepaalde situaties geen twijfel bestaat over de interpretatie van 'niet langer dan noodzakelijk':

- gegevens die reeds bij de behandeling van de melding incidenteel blijken te zijn, horen niet bijgehouden te worden. Waar dergelijke gegevens voor beleidsdoeleinden relevant zouden zijn, hoort – zoals eerder aangekaart in punt 64 – toepassing gemaakt te worden van pseudonomisering of anonimisering technieken. De Autoriteit benadrukt dat

[74] HvJ (gr. Kamer) 8 april 2014, gevoegde zaken nrs. C-293/12 en C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e.a.* en *Kärntner Landesregiering e.a.*, randnrs. 63 en 64; FRA en RVA, Handboek Europese gegevensbeschermingswetgeving, editie 2018, Luxemburg, 2021, 155.

[75] HvJ 20 oktober 2022, nr. C-77/21, *Digi*, randnr. 54.

[76] De Autoriteit onderstreept dat de aanvullende motivering in punt 116 van onderhavig advies of een gelijkaardige motivering niet voldoet aan de vereiste. *In casu*, hoort het **om een proportionele bewaartermijn te gaan, rekening houdend met de aard van de gegevens die uitdrukkelijk gerechtvaardigd wordt**, bijvoorbeeld omwille van andere wettelijk verplichte bewaartermijnen.

[77] In dat verband wijst de Autoriteit, de decreetgever, erop dat een bewaartermijn van één jaar in lijn is met huidige regelgeving, denk bijvoorbeeld aan artikel 8 van het Koninklijk besluit houdende vaststelling van de voorwaarden waaraan de ombudsfunctie in de ziekenhuizen moet voldoen.

gepseudonimiseerde gegevens nog steeds persoonlijke gegevens zijn en derhalve ook hier een motivering noodzakelijk is wanneer deze onder deze vorm bijgehouden worden;

- gegevens van meldingen die onterecht of onontvankelijk blijken te zijn – zoals verder uiteengezet in punt 120.
- 'duplicaten vermijden', vereist niet noodzakelijk dat alle gegevens van een melding bijgehouden worden.

119. De Autoriteit stelt zich voorts vragen bij de intentie om "'veelmelders' te herkennen." Hoewel het voor de goede werking van het meldpunt, noodzakelijk is om de valse meldingen eruit te kunnen halen, kan het niet de bedoeling zijn om melders te profileren of te categoriseren. Bovendien kan dergelijke informatie niet als noodzakelijk bestempeld worden dat het langer dan een korte periode bijgehouden kan worden. Zo lijkt het bijhouden van dergelijke informatie voor langere periodes dan één jaar, aangaande meldingen die niet consecutief gedaan worden, disproportioneel.

120. Op vraag van de Autoriteit, specificeerde de aanvrager m.b.t. de onterechte en onontvankelijke meldingen het volgende:

> "*In de meeste gevallen blijkt niet meteen uit de melding of een dossier onterecht of onontvankelijk is. Wanneer duidelijk is dat een melding onterecht of onontvankelijk is, wordt de informatie net zoals bij een ontvankelijke melding niet langer bewaard dan noodzakelijk en identificeerbare gegevens zullen zoveel als mogelijk worden weggelaten*."

121. De Autoriteit preciseert dat verwerkingen van persoonsgegevens over meldingen die onterecht of onontvankelijk zijn, verder gaat dan hetgeen noodzakelijk is voor de verwerking van het doeleinde. Bijgevolg, is de Autoriteit van mening dat vanaf het ogenblik van kennisneming over de onontvankelijkheid of onterechtheid, er geen grond is om dergelijke gegevens verder te bewaren of te verwerken. In het licht hiervan horen deze verwijderd, gepseudonimiseerd of geanonimiseerd te worden. Waar dergelijke gegevens bijgehouden worden in een andere vorm dan een geanonimiseerde, dient telkens een motivering te worden verstrekt die het behoud ervan verantwoordt voor dat specifieke geval.

122. Het geheel in aanmerking genomen is de Autoriteit niet overtuigd dat het in het ontwerp bepaalde bewaartermijn voldoende waarborgen biedt om gegevens niet langer dan noodzakelijk bij te houden voor het doeleinde waarvoor deze gegevens worden verwerkt. In tegendeel, de vaagheid omtrent wat "niet langer als noodzakelijk" in samenhang met een maximale bewaartermijn van 10 jaar na afsluiting van een dossier, wekt het vermoeden dat er een zeer ruime interpretatie toegepast zal worden. De Autoriteit wijst erop dat het niet de bedoeling is om de bewaartermijn van alle gegevens te strekken tot 10 jaar na afsluiten van dossiers. Zoals werd

aangevuld door de aanvrager, hoort telkens een geval per geval beoordeling, waarbij op recurrente wijze gecontroleerd wordt of gegevens werkelijk nog dienend zijn voor het doel. **Terzake vraagt de Autoriteit, zoals reeds aangegeven in punt 117, om in het ontwerp, een <u>proportionele maximale bewaartermijn</u> voor de bewaring van gegevens na de behandeling en / of opvolging van een melding, te voorzien en deze, minstens in de Memorie van Toelichting, uitdrukkelijk te rechtvaardigen. En in het bijzonder te voorzien in een afzonderlijke bewaartermijn, rekening houdend met de aard van de gegevens. <u>Bij gebrek hieraan geldt dat de bewaartermijn niet langer dan één jaar na afsluiten van het dossier, mag zijn</u>.**

h. Rechten van de betrokkenen

123. De betrokkene beschikt krachtens de AVG (de artikelen 12 tot en met 22)[78] over verschillende rechten.

124. Dienaangaande bepaalt artikel 15, van het ontwerp, het volgende:

"*Het Agentschap Justitie en Handhaving* ***neemt passende maatregelen met het oog op transparantie*** *ten aanzien van melders en andere personen die betrokken zijn bij een melding van grensoverschrijdend gedrag.*

De maatregelen, vermeld in het eerste lid, hebben onder meer tot doel dat de globale regeling voor de gegevensverwerking in het kader van het meldpunt AJH voldoende duidelijk is, en dat het voor de betrokkenen duidelijk is op welke wijze de verplichtingen en de rechten, vermeld in artikel 12 tot en met 21 van de algemene verordening gegevensbescherming, worden toegepast."[79]

125. Vooreerst brengt de Autoriteit in herinnering dat de communicatie in verband met de verwerking in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm, die bovendien in duidelijke en eenvoudige taal ontvangen dient te worden. Dit geldt in het bijzonder wanneer de informatie specifiek voor een kind bestemd is.[80] Terzake komt de Autoriteit terug op punt 17 waar uiteengezet wordt dat voornamelijk, maar niet alleen, jongeren en kinderen, geviseerd worden. In de mate dat het uitreikt naar jongeren en kinderen, acht de Autoriteit dat de huidige algemene privacyverklaring onvoldoende afgemeten is op de uiteenlopende

[78] Deze kunnen betrekking hebben op:

- de aanvang van de verwerking: recht op informatie (artt. 13-14 AVG) en recht op verzet (artt. 21-22 AVG);
- de duurtijd van de verwerking: recht op toegang / inzage (art. 15 AVG), recht op verzet (artt 21-22 AVG), recht op verbetering (art. 16 AVG), recht op overdraagbaarheid (art. 20 AVG), recht op beperking (art. 18 AVG);
- de beëindiging van de verwerking: recht op verzet (artt21-22 AVG), recht op wissing (art. 17 AVG), recht op beperking (art. 18 AVG), recht op overdraagbaarheid (art. 20 AVG).

[79] Vet toegevoegd door de Autoriteit.

[80] Artikel 12(1) AVG.

leeftijdscategorieën die hier potentieel onder kunnen vallen. Het gebruik van de in punt 127 toegelichte twee-stap procedure, zou hier hoofd aan kunnen bieden.

126. Met betrekking tot het recht op informatie krachtens artikelen 13 en 14 van de AVG, werd op vraag van de Autoriteit verduidelijkt dat:

> "*[d]e melder of personen die betrokkenheid vertonen met de context van het grensoverschrijdend gedrag en over wie de persoonsgegevens worden verwerkt, […] recht [hebben] op informatie. Dit recht op informatie omvat onder andere dat de melder of andere betrokkene mag weten welke gegevens over hem worden verwerkt, door wie, hoe lang deze worden bewaard*.
>
> *Binnen het meldpunt AJH wordt volgende aanpak gehanteerd:*
>
> - *De privacyverklaring wordt via de website van het Meldpunt actief publiek gemaakt;*
> - *Er wordt op de chat site verwezen naar de privacyverklaring;*
> - *E-mails vanuit zowel de generieke mailbox als vanuit de persoonlijke mailbox van de dossierbehandelaars bevatten een disclaimer."*[81]

127. Hieruit volgt voor de situatie onder artikel 13 AVG, wanneer de persoonsgegevens bij de betrokkene zelf verzameld worden, dat het meldpunt AJH gebruik maakt van een algemene privacyverklaring en een disclaimer, die bij gebrek aan verdere duiding hieromtrent vermoedelijk een verwijzing naar de algemene privacyverklaring betreft. Gelet op de bijzondere context, meent de Autoriteit dat het behoedzamer is om gebruik te maken van **een twee-stap procedure**. Enerzijds zoals reeds gesteld een algemene privacyverklaring op het moment dat de persoonsgegevens verkregen worden en voor verdere verwerking voor de verwerking plaatsvindt. Anderzijds een op de individu afgestemde specifieke privacyverklaring, die rechtstreeks aan deze bezorgd wordt van zodra het praktisch haalbaar is. De Autoriteit vraagt om de Memorie van Toelichting aan te vullen met de verduidelijking van de aanvrager en met inbegrip van de aanbevolen twee-stap procedure.

128. Verder werd door de aanvrager t.a.v. artikel 14 AVG gepreciseerd dat:

> *"[o]vereenkomstig artikel 14 (5)(d) van de AVG dient de persoon van wie de persoonsgegevens onrechtstreeks worden verzameld, niet op de hoogte te worden gebracht van de verwerking in zoverre deze gegevens vertrouwelijk moeten blijven uit hoofde van een (wettelijk of statutair) beroepsgeheim. Het voorontwerp bepaalt in artikel 14 dat de medewerkers van het Meldpunt gebonden zijn door het beroepsgeheim voorzien in artikel 458 van het Strafwetboek. De personen die in een melding geïdentificeerd worden, zullen derhalve niet op de hoogte worden gebracht van de gegevensverwerking.*

[81] Uitlijning toegevoegd door de Autoriteit.

Door het actief publiek maken van de privacyverklaring via de website worden de rechten van de personen van wie de gegevens onrechtstreeks worden verzameld gevrijwaard.

In zoverre de voormelde persoonsgegevens echter niet langer als geheim worden behandeld, bijvoorbeeld omdat zij met de toestemming van de melder worden gedeeld met de betrokken organisatie (artikel 13, §1, derde lid, 5° van het voorontwerp), zal de betrokkene ten laatste op het ogenblik dat zijn persoonsgegevens worden gedeeld op de hoogte worden gebracht overeenkomstig artikel 14 (3)(c) AVG."

129. Wat de uitzonderingsregel op de informatieplicht betreft, krachtens artikel 14(5)(d) AVG, deelt de Autoriteit hetzelfde uitgangspunt als de aanvrager.

130. Voorts verwijst de Autoriteit hier naar de twee-stap procedure uit punt 127, die ook toepassing vindt in een situatie waarbij de gegevens op onrechtstreeks wijze verkregen zijn, doch met dien verstande dat dit enkel aan de orde is wanneer de persoonsgegevens niet langer als geheim behandeld worden.

131. Ten aanzien van het recht op inzage krachtens artikel 15 van de AVG, verduidelijkt de aanvrager het volgende:

"*De melder of een andere betrokkene kan zich eveneens beroepen op de AVG om toegang te krijgen tot de persoonsgegevens die het meldpunt AJH over hem of haar verwerkt hebben. Als de melder of andere betrokkene een aanvraag doet, dient het meldpunt AJH steeds contact op te nemen met de DPO van het agentschap om dit verder af te handelen.*

De dossierbehandelaars zijn gebonden door het beroepsgeheim (artikel 14 voorontwerp), op basis hiervan zal geval per geval, rekening houdend met de rechten en vrijheden van de melder (cf. artikel 15 (4) AVG), moeten worden bekeken of en in welke mate er kan ingaan worden op de vraag tot informatie of inzage."

132. In overeenstemming met de aanvrager, meent de Autoriteit, dat een geval per geval beoordeling gepast is. Doch onderstreept de Autoriteit dat er minstens interne regels voorhanden moet zijn. Bovendien moet steeds de proportionaliteit en noodzakelijkheid getoetst worden. Vervolgens moet elke beslissing gepaard gaan met een motivatie naar de betrokkene toe.

133. Daarnaast vraagt de Autoriteit om minstens in de Memorie van Toelichting, verdere duiding te verschaffen aangaande de "passende maatregelen," zodat enerzijds de antwoorden van de

aanvrager dienaangaande inbegrepen worden en anderzijds de maatregelen op ondubbelzinnige wijze vastgesteld zijn.

134. De Autoriteit verwijst de aanvrager naar de aanbeveling van de Commissie voor de bescherming van de persoonlijke levenssfeer, nr. 01 / 2006 van 29 november 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, voor verdere inlichting aangaande de andere rechten van de betrokkenen.

OM DEZE REDENEN,
de Autoriteit,

formuleert de volgende opmerkingen met betrekking tot het ontwerp:

- voorzien in een duidelijke omkadering van het materiële toepassingsgebied, o.m. door af te grenzen wat een rechtstreekse link is, zodat het doeleinde werkelijk welbepaald is (punten 15, 22-**Error! Reference source not found.**);
- akte nemen van de gezamenlijke verwerkingsverantwoordelijkheid en dit uitdrukkelijk aangeven in het ontwerp (punten 31-33);
- gelet op het tijdstip van de kennisneming van de (on)ontvankelijkheid van een melding is het aangeraden om te opteren voor een geval per geval beoordeling i.p.v. systematisch na elke melding een uitgebreide vraagverheldering uit te voeren. Het wordt aanbevolen om de Memorie van Toelichting op één lijn te brengen met het antwoord van de aanvrager (punt 41);
- de verwijzing naar het identificatienummer van de Kruispuntbank van de Sociale Zekerheid, schrappen uit artikel 13, §1, lid 1 van het ontwerp schrappen (punt 43);
- voorzien in een correcte machtiging om het Rijksregister te raadplegen en te gebruiken overeenkomstig artikel 5 en 8 van de wet van 8 augustus 1983 *tot regeling van een rijksregister van de natuurlijke personen* (punten 43-45);
- verdere duiding voorzien voor hetgeen bedoeld wordt met "persoonsgegevens die blijken" in artikel 13, §1, lid 1, 4°, 5°, van het ontwerp, zodat elke categorie van gegevens die hieronder valt concreet en ondubbelzinnig gespecifieerd is (punt 46);
- onthouden van het bijhouden van register van gegevens die onder artikel 10 AVG kaderen, het invoeren van een systeem met onderscheiden autorisaties voor de bijzondere categorieën van gegevens, voorzien in bijkomende waarborgen (punten 47-48);
- bij gebruik aan een systeem dat de melding in eerste fase duidelijk omkadert, helder aangeven wat de categorieën van gegevens zijn die in de twee fases van een melding kunnen zitten en

aangeven dat de tweede fase als een controle fase dient, waar alle niet-essentiële gegevens verwijderd moeten worden (punt 55);

- bij voorkeur in het ontwerp, verduidelijken waar een melding kan gebeuren en onder welke vorm (punt 56);
- binnen redelijke termijn een overschakeling voorzien van SharePoint naar een adequater systeem (punt 57);
- uitvoeren van een GEB, inclusief voor de SharePoint systeem en het vervangend systeem (punt 57);
- verdere duiding voorzien omtrent de verschillende meldingskanalen en de inhoudelijke vorm (samenvatting) waarop de informatie bijgehouden wordt (punt 61);
- het ontwerp en de Memorie van Toelichting in lijn brengen met de aanvullende antwoorden van de aanvrager (punt 61);
- uitdrukkelijk duiding geven over het bestaan van een meldingsregister, de inhoud, het gebruik en de toegang, periodieke redactie, doel, bewaartermijn (punten 62-67);
- aangeven of het meldingsregister gelijk is aan het centraal register (punt 63);
- onder het kader van beleidsadviezen afleveren, rekening houden dat het voorbereidend werk bij voorkeur met geanonimiseerde of gepseudonimiseerde gegevens gebeurt (punt 64);
- in het ontwerp uitdrukkelijk specificeren of er verschillende categorieën van personen zijn met onderscheiden machtigingen en toegang tot het inhoudelijk dossier (punten 65-66, 77);
- categorieën van betrokkenen verder specificeren (punten 69-71);
- uitdrukkelijk in het ontwerp de mogelijkheid om een anonieme melding te maken te vermelden en anonieme melding definiëren (punten 72-75);
- in het ontwerp of minstens in de Memorie van toelichting een beschrijving geven van hetgeen onder operationele werking valt (punt 77);
- een bepaling invoeren die de verwerkingsverantwoordelijke verplicht om steeds in staat te zijn om het mondelinge akkoord te kunnen bewijzen (punten 80-81);
- artikel 13, §1, lid 3, 5°, van het ontwerp aanvullen zodat gepreciseerd wordt dat de noodzakelijkheid steeds gemotiveerd moet worden (punt 81);
- in artikel 10, §2, van het ontwerp, instemming vervangen met toestemming (punt 87);
- ontwerp aanvullen met de verplichting van het opstellen van een lijst van de categorieën van personen die toegang hebben tot de gegevens onder artikel 10 AVG en bij voorkeur werken met een systeem van diverse graden van autorisaties (punt 85);
- artikel 10, §2, van het ontwerp voorzien van verdere duiding zodat ingegaan wordt op de term partijen, de unanimiteit van instemming, de vrijstelling van vertrouwelijkheid en welke documenten het betrekking op heeft en de toepassing van de rechten van de betrokkenen (punt 89);
- in artikel 17, van het ontwerp verdere duiding voorzien voor hetgeen bedoeld wordt met "noodzakelijke informatie" (punt 94);

- uitzonderingen van het beroepsgeheim uitdrukkelijk specificeren en verder kaderen (punten 95-101);
- gebruik van een onderlinge verwerkingsovereenkomst voor hetgeen onder de gezamenlijke bevoegdheid valt van het VMRI en het AJH (punten 104-108);
- in het ontwerp een passend kader voorzien voor de doorgifte van gegevens en het samenhangende protocol (punten 109-112);
- voorzien van verdere duiding aangaande hetgeen bedoeld wordt met "bepaalde acties te ondernemen met betrekking tot de melding van grensoverschrijdend gedraag" (punt 113);
- het ontwerp voorzien van een uitdrukkelijk gerechtvaardigde en proportionele maximumbewaartermijn en, rekening houdend met de aard van de gegevens, voorzien in afzonderlijke bewaartermijnen. Bij gebrek hieraan geldt dat de maximumbewaartermijn niet langer dan één jaar, na afsluiting van het dossier, mag zijn (punten 114-118 en 122);
- onthouden van 'veelmelders' te categoriseren of te profileren (punt 119);
- voorzien van een beperking op de bewaring van gegevens aangaande meldingen die onontvankelijk of onterecht blijken te zijn (punt 121-122);
- voorzien van een afgemeten privacyverklaring aan de diverse leeftijdscategorieën (punt 125);
- invoeren van een twee-stap procedure voor de kennisgeving (punten 125, 127 en 130);
- uitdrukkelijk in het ontwerp voorzien van een motivering aangaande beslissingen over de inzage (punt 132);
- duidelijk en op ondubbelzinnige wijze verdere duiding geven over "passende maatregelen" in artikel 15, van het ontwerp (punt 133).

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