Vlaamse overheid

Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens

Advies wetgeving VTC nr. 2022/109 van november 2022

(zie datum ondertekening)

over

tekst	voorontwerp van decreet
van	van de Vlaamse Regering
titel	tot bescherming van klokkenluiders in het onderwijs in de Vlaamse Gemeenschap
roepnaam	(decreet klokkenluiders onderwijs)
datum	zoals principieel goedgekeurd op 10 november 2022

De Vlaamse Toezichtcommissie (hierna "de VTC");

Gelet op het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer (hierna: "het e-govdecreet"), inzonderheid artikel 10/4, §1;

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), inzonderheid artikel 36, 4, artikel 57, 1, c) en artikel 58, 3;

Gelet op de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (hierna "WVG");

Gelet op het verzoek om advies van de heer Ben Weyts, Viceminister – president van de Vlaamse regering, Vlaams minister van Onderwijs, Sport, Dierenwelzijn en Vlaamse Rand van 10 november 2022, ontvangen door de VTC op 18 november2022;

Gelet op de behandeling in schriftelijke procedure;

Brengt het volgend advies uit:

I. VOORWERP VAN DE ADVIESAANVRAAG

1. De Vlaamse minister bevoegd voor Onderwijs (hierna "de adviesvrager") verzocht om het advies van de Vlaamse Toezichtcommissie (hierna "VTC") over een voorontwerp van decreet *tot bescherming van klokkenluiders in het onderwijs in de Vlaamse Gemeenschap* (hierna "het Ontwerp"), zonder aanduiding van specifieke artikelen.

2. Aangezien de adviesbevoegdheid van de VTC op grond van artikel 10/4, § 1 van het e-govdecreet betrekking heeft op de verwerkingen van persoonsgegevens, is haar adviesverlening hiertoe beperkt.

Context

3. Het Ontwerp handelt over de omzetting van de Europese klokkenluidersrichtlijn voor het onderwijs in de Vlaamse Gemeenschap.

4. Op 23 oktober 2019 namen het Europees Parlement en de Raad richtlijn 2019/1937 inzake de bescherming van personen die inbreuken op het Unierecht melden, aan. Het doel van deze richtlijn is om personen te beschermen die in de werkomgeving verkregen informatie over inbreuken op bepaalde EU-regelgeving melden. Lidstaten moeten enerzijds de oprichting van interne en externe meldkanalen regelen en anderzijds beschermingsmaatregelen voor klokkenluiders invoeren.

5. De richtlijn is zowel op de private als op de publieke sector van toepassing en moet bijgevolg ook omgezet worden voor het Vlaamse onderwijs. Gelet op de domeinen waarop de klokkenluidersrichtlijn van toepassing is, zal de toepasbaarheid van de richtlijn binnen het onderwijs eerder beperkt zijn.

6. Omwille van de duidelijkheid voor het onderwijsveld en de praktische haalbaarheid van de juridische uitwerking wordt de regeling voor de hogescholen en universiteiten opgenomen in de Codex Hoger Onderwijs van 11 oktober 2013. Voor de andere onderwijsniveaus wordt de regeling als autonome bepalingen in het Ontwerp opgenomen.

7. De VTC gaf reeds advies 2022/006 over een voorontwerp van decreet van de Vlaamse Regering tot wijziging van het Provinciedecreet van 9 december 2005, het decreet van 22 december 2017 over het lokaal bestuur en het Bestuursdecreet van 7 december 2018, wat betreft klokkenluiders.[1]

8. De volgende bepalingen van het Ontwerp hebben betrekking op de verwerking van persoonsgegevens :

Artikel 8.

"§1. Iedere instelling heeft een intern meldkanaal.

Het interne meldkanaal kan door de instelling zelf worden beheerd of extern ter beschikking worden gesteld door een derde. De waarborgen voor een interne melding en de opvolging van de meldingen, vermeld in afdeling 4 en 5 van dit hoofdstuk, zijn ook van toepassing als het interne meldkanaal door een derde wordt beheerd.

§2. Het interne meldkanaal bestaat uit ten minste een persoon die bevoegd is om meldingen te ontvangen en te behandelen. Personeelsleden met een mandaat in een beslissingsorgaan of personeelsafgevaardigden kunnen geen deel uitmaken van het interne meldkanaal.

De persoon die bevoegd is om meldingen te ontvangen of te behandelen heeft daarvoor de nodige vorming gekregen.

§3. Iedere instelling werkt, na overleg met afgevaardigden van de representatieve vakorganisaties, een procedure uit om interne meldingen in te dienen, te behandelen en te beheren. Als het interne meldkanaal door een derde ter beschikking gesteld wordt, worden de afgevaardigden van de representatieve vakorganisaties op de hoogte gebracht van de inhoud van de overeenkomst met de derde.

De procedure, vermeld in het eerste lid, bevat systemen die door hun ontwerp, opzet en beheer op beveiligde wijze de geheimhouding van de informatie waarborgen en de vertrouwelijkheid beschermen van al de volgende elementen:

[1] https://overheid.vlaanderen.be/sites/default/files/media/VTC/VTC_A_W_2022_006_advies.pdf

de identiteit van de melder;
de identiteit van derden die in de melding worden genoemd;
informatie waaruit de identiteit van de melder of een derde kan blijken.

Als het meldkanaal een melding behandelt, neemt het daarbij een strikte neutraliteit in acht. Een melding kan in geen geval behandeld worden door een persoon die betrokken is of was bij de feiten waarop de melding betrekking heeft.

Alleen personeelsleden die daarvoor gemachtigd zijn, hebben toegang tot de informatie, vermeld in het tweede lid."

Artikel 9.

"§1. Personeelsleden en externen kunnen informatie over inbreuken die instellingen begaan hebben, extern melden bij de Vlaamse Ombudsdienst conform het decreet van 7 juli 1998 houdende instelling van de Vlaamse Ombudsdienst.

§2. Het externe meldkanaal, vermeld in paragraaf 1, ontvangt meldingen via systemen die door hun ontwerp, opzet en beheer op beveiligde wijze de geheimhouding van de informatie waarborgen en de vertrouwelijkheid beschermen van al de volgende elementen:

de identiteit van de melder;
de identiteit van derden die in de melding worden genoemd;
informatie waaruit de identiteit van de melder of een derde kan blijken.

Als het meldkanaal een melding behandelt, neemt het daarbij een strikte neutraliteit in acht. Een melding kan in geen geval behandeld worden door een persoon die betrokken is of was bij de feiten waarop de melding betrekking heeft.

Alleen personeelsleden die daarvoor gemachtigd zijn, hebben toegang tot de informatie, vermeld in het eerste lid."

Artikel 10.

"§1. Een personeelslid meldt informatie over inbreuken die de instelling waar het tewerkgesteld is, via het interne meldkanaal vermeld in artikel 8. Een personeelslid kan informatie over inbreuken ook rechtstreeks melden via het externe meldkanaal, vermeld in artikel 9, als het meent dat de inbreuk intern niet doeltreffend behandeld kan worden of dat er een risico op represailles bestaat.

Externen melden informatie over inbreuken die een instelling begaat, aan het externe meldkanaal, vermeld in artikel 9.

Een onderwijsinstelling kan het interne meldkanaal, vermeld in artikel 8, ook openstellen voor bepaalde of alle externen.

§2. Personeelsleden en externen die informatie over inbreuken openbaar maken komen in aanmerking voor bescherming uit hoofde van dit decreet indien is voldaan aan een van de volgende voorwaarden:
ze hebben eerst intern en extern gemeld of ze hebben meteen extern gemeld conform paragraaf 1, en er zijn geen passende maatregelen genomen binnen drie maanden nadat het meldkanaal in kwestie de melding heeft ontvangen;
ze hebben gegronde redenen om aan te nemen dat:

a) de inbreuk kan een dreigend of reëel gevaar vormen voor het algemeen belang, bijvoorbeeld wanneer er sprake is van een noodsituatie of een risico op onherstelbare schade, of b) er bestaat een risico op represailles bij externe meldingen, of het is niet waarschijnlijk dat de inbreuk doeltreffend wordt behandeld wegens de bijzondere omstandigheden van de zaak, omdat bijvoorbeeld bewijsmateriaal kan worden achtergehouden of vernietigd, of een autoriteit kan samenspannen met de pleger van de inbreuk of met iemand die bij de inbreuk is betrokken.
Deze paragraaf is niet van toepassing op gevallen waarin een personeelslid of een externe rechtstreeks informatie aan de pers verstrekt op grond van specifieke bepalingen die een stelsel voor de bescherming van de vrijheid van meningsuiting en informatie instellen."

Afdeling 4. Gemeenschappelijke bepalingen voor interne en externe meldingen

Artikel 11.

"§1. Melders kunnen schriftelijk en via de telefoon of een ander spraakberichtensysteem informatie over inbreuken melden bij de meldkanalen, vermeld in artikel 8 en 9. Ze hebben ook het recht op een fysieke ontmoeting binnen een redelijke termijn.

§2. De meldkanalen, vermeld in artikel 8 en 9, kunnen van mondelinge meldingen via een spraakberichtsysteem met gesprekopname:
een opname van het gesprek in een duurzame, opvraagbare vorm maken;
een volledig en nauwkeurig verslag laten opstellen door de personeelsleden die verantwoordelijk zijn om de melding te behandelen.

De meldkanalen, vermeld in artikel 8 en 9, stellen de melders voor de start van het gesprek op de hoogte van de mogelijkheid van het systeem om gesprekken op te nemen.

§3. De personeelsleden van de meldkanalen, vermeld in artikel 8 en 9, die verantwoordelijk zijn om de melding te behandelen, kunnen een nauwkeurig verslag opmaken van mondelinge meldingen via een spraakberichtsysteem zonder gespreksopnamefaciliteit.

§4. Als de melder toestemt, maken de meldkanalen, vermeld in artikel 8 en 9, bij een fysieke ontmoeting op verzoek van de melder:
een opname van het gesprek in een duurzame en opvraagbare vorm;
een nauwkeurig verslag van het onderhoud, dat de personeelsleden opstellen die verantwoordelijk zijn voor de behandeling van de melding.

§5. Melders kunnen de schriftelijke weergave van het gesprek, vermeld in paragraaf 2 tot en met 4, controleren, corrigeren en voor akkoord tekenen."

Artikel 12.

"§1. De meldkanalen, vermeld in artikel 8 en 9, bevestigen de ontvangst van de melding aan de melder binnen zeven dagen na de dag waarop ze de melding hebben ontvangen, als ze binnen die termijn de melding nog niet afgehandeld hebben, tenzij in één van de volgende gevallen:
de melder verzet zich uitdrukkelijk tegen het krijgen van die ontvangstmelding;
het krijgen van die ontvangstmelding brengt de bescherming van de identiteit van de melder in gevaar.

Tenzij er nieuwe wettelijke of feitelijke omstandigheden zijn die een andere opvolging rechtvaardigen, kan het externe meldkanaal, vermeld in artikel 9, bij meldingen over een instelling beslissen om in een van de volgende gevallen de melding niet in behandeling te nemen:
de inbreuk is van geringe betekenis;

de externe melding heeft betrekking op feiten die in een eerdere externe melding van de melder al zijn behandeld en de nieuwe melding bevat geen nieuwe informatie van betekenis.

In de gevallen, vermeld in het tweede lid, stuurt het externe meldkanaal, vermeld in artikel 9, de melder binnen zeven dagen nadat het de melding heeft ontvangen, naast de ontvangstmelding, vermeld in het eerste lid, de beslissing om de melding niet in behandeling te nemen en een motivatie voor die beslissing.

§2. De meldkanalen, vermeld in artikel 8 en 9, gaan de juistheid na van de informatie en nemen de gepaste maatregelen als er een vermoeden van een inbreuk is.

§3. De meldkanalen, vermeld in artikel 8 en 9, informeren de melder binnen drie maanden na de dag waarop ze de ontvangstmelding hebben verstuurd, of, als er geen ontvangstmelding naar de melder is gestuurd, binnen drie maanden nadat de periode van zeven dagen nadat de melding is gedaan, is verstreken, over de als opvolging geplande of genomen maatregelen en over de redenen daarvoor. De meldkanalen, vermeld in artikel 8 en 9, geven daarbij geen informatie vrij die afbreuk doet aan het interne onderzoek of die het onderzoek of de rechten van de betrokken persoon schaadt.

Het externe meldkanaal, vermeld in artikel 9, kan de termijn van drie maanden, vermeld in het eerste lid, verlengen tot maximaal zes maanden. In dat geval informeert het externe meldkanaal de melder schriftelijk over de verlenging van de termijn en de reden daarvoor, voor de voormelde termijn van drie maanden verstreken is.

§4. Het extern meldkanaal, vermeld in artikel 9 brengt de melder op de hoogte van het eindresultaat van de onderzoeken."

Artikel 13.

"Als een melder een melding richt aan een onbevoegd extern meldkanaal, stuurt dat onbevoegde meldkanaal, personeelslid of die onbevoegde instelling de melding zo snel mogelijk op veilige wijze door naar het bevoegde externe meldkanaal. Het onbevoegde externe meldkanaal brengt de melder onmiddellijk op de hoogte van die doorzending.
Indien het intern meldkanaal niet bevoegd is om de melding te behandelen, dan brengt het meldkanaal de melder daarvan op de hoogte."

Afdeling 5. Verwerking van gegevens

Artikel 14.

"Ieder meldkanaal, als vermeld in artikel 8 en 9, houdt een register bij van de ontvangen meldingen.

Ieder meldkanaal, als vermeld in artikel 8 en 9, houdt al de volgende gegevens bij:
het aantal ontvangen meldingen;
het aantal onderzoeken en procedures die naar aanleiding van de meldingen zijn ingeleid en het resultaat ervan;
als dat wordt vastgesteld, de geschatte financiële schade en de bedragen die zijn teruggevorderd na onderzoeken en procedures over de gemelde inbreuken.

Meldingen worden niet langer opgeslagen dan noodzakelijk en evenredig is om te voldoen aan de vereisten die door dit decreet of door andere wetgeving zijn opgelegd."

Artikel 15.

"§1. In dit artikel wordt verstaan onder algemene verordening gegevensbescherming: verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

§2. Als die gegevens beschikbaar zijn, verwerken de meldkanalen, vermeld in artikel 8 en 9, de volgende persoonsgegevens op grond van artikel 6, eerste lid, e) van de algemene verordening gegevensbescherming bij de behandeling en registratie van meldingen:
de naam van de melder;
de contactgegevens en de functie van de melder;
de naam van de facilitator of van derden die verbonden zijn met de melder en die het slachtoffer kunnen worden van represailles in een werkgerelateerde context;
de naam en de functie van de betrokken persoon en informatie over de inbreuken van de betrokken persoon;
de naam van de getuigen;
schriftelijke meldingen;
het schriftelijke verslag van mondelinge meldingen en stemopnames, vermeld in artikel 11, §2 en §3, van dit decreet.

De meldkanalen, vermeld in artikel 8 en 9, wissen onmiddellijk andere gegevens dan de persoonsgegevens, vermeld in het eerste lid, die niet relevant zijn om de melding te behandelen.

§3. De meldkanalen, vermeld in artikel 8 en 9, maken de identiteit van de melder en alle informatie waarmee de identiteit van de melder direct of indirect achterhaald kan worden niet bekend aan anderen dan de personeelsleden die bevoegd zijn om de melding te ontvangen en op te volgen tenzij in één van de volgende gevallen:
de melder stemt daarmee in;
er is een noodzakelijke en evenredige wettelijke verplichting in het kader van een onderzoek door nationale autoriteiten of gerechtelijke procedures, om de rechten van verdediging van de melder te waarborgen.

De meldkanalen, vermeld in artikel 8 en 9, maken de identiteit van de betrokken persoon en alle informatie waarmee de identiteit van de betrokken persoon direct of indirect achterhaald kan worden, niet bekend aan anderen dan de personeelsleden die bevoegd zijn om de melding te behandelen, zolang onderzoeken naar aanleiding van de melding of openbaarmaking lopen.

§4. Vóór de meldkanalen, vermeld in artikel 8 en 9, de identiteit van de melder of de betrokken persoon bekendmaken, brengen ze de melder, respectievelijk de betrokken persoon daarvan schriftelijk op de hoogte, samen met de redenen daarvoor, tenzij die informatie de onderzoeken of gerechtelijke procedures in gevaar brengt.

§5. Met toepassing van artikel 23, lid 1, e) en h), van de algemene verordening gegevensbescherming kunnen de personeelsleden van een meldkanaal die daarvoor bevoegd zijn, bij wie een melding is ingediend, beslissen om de verplichtingen en de rechten, vermeld in artikel 12 tot en met 22 van de voormelde verordening, niet toe te passen bij de verwerking van persoonsgegevens in het kader van een onderzoek dat betrekking heeft op een welbepaalde natuurlijke persoon, als voldaan is aan de voorwaarden, vermeld in het tweede tot en met het negende lid.

De afwijkingsmogelijkheid, vermeld in het eerste lid, geldt alleen gedurende de periode waarin de betrokken persoon het voorwerp uitmaakt van een onderzoek, op voorwaarde dat het voor het goede verloop van het onderzoek noodzakelijk is of kan zijn dat de verplichtingen en de rechten, vermeld in artikel 12 tot en met 22 van de voormelde verordening, niet worden toegepast. De duur van het

onderzoek mag in voorkomend geval niet meer bedragen dan een jaar vanaf de ontvangst van een verzoek tot uitoefening van een van de rechten, vermeld in artikel 12 tot en met 22 van de voormelde verordening.

De afwijkingsmogelijkheid, vermeld in het eerste lid, heeft geen betrekking op de gegevens die losstaan van het voorwerp van het onderzoek dat de weigering of de beperking van de rechten, vermeld in het tweede lid, rechtvaardigt.

Als de betrokken persoon in het geval, vermeld in het eerste lid, tijdens de periode, vermeld in het tweede lid, een verzoek indient op basis van artikel 12 tot en met 22 van de voormelde verordening, bevestigt de bevoegde functionaris voor gegevensbescherming, de ontvangst daarvan.

De bevoegde functionaris voor gegevensbescherming, brengt de betrokken persoon schriftelijk, zo snel mogelijk en in elk geval binnen een maand vanaf de dag die volgt op de dag waarop hij het verzoek heeft ontvangen, op de hoogte van elke weigering of beperking van de rechten, vermeld in het eerste lid. Verdere informatie over de nadere redenen voor die weigering of beperking hoeft niet te worden verstrekt als dat het onderzoek zou ondermijnen, met behoud van de toepassing van het achtste lid. Als het nodig is, kan de voormelde termijn met twee maanden worden verlengd, rekening houdend met het aantal aanvragen en de complexiteit ervan. De verwerkingsverantwoordelijke, vermeld in artikel 4, 7), van de algemene verordening gegevensbescherming, brengt de betrokken persoon binnen dertig dagen vanaf de dag die volgt op de dag waarop hij het verzoek heeft ontvangen, op de hoogte van die verlenging en van de redenen voor het uitstel.

De bevoegde functionaris voor gegevensbescherming, informeert de betrokken persoon ook over de mogelijkheid om een verzoek in te dienen bij de Vlaamse toezichtcommissie voor de verwerking van persoonsgegevens conform artikel 10/5 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer, en om een beroep in rechte in te stellen.

De bevoegde functionaris voor gegevensbescherming noteert de feitelijke of juridische gronden waarop de beslissing is gebaseerd. Die informatie houdt hij ter beschikking van de Vlaamse toezichtcommissie, vermeld in artikel 10/1 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.

Nadat het onderzoek afgesloten is, worden de rechten, vermeld in artikel 13 tot en met 22 van de voormelde verordening, in voorkomend geval, conform artikel 12 van de voormelde verordening opnieuw toegepast.

Als een dossier dat persoonsgegevens als vermeld in het eerste lid, bevat, naar het Openbaar Ministerie is gestuurd en kan leiden tot activiteiten onder leiding van het Openbaar Ministerie of een onderzoeksrechter, en er onduidelijkheid is over het geheim van het onderzoek onder leiding van het Openbaar Ministerie of een onderzoeksrechter, mag de bevoegde functionaris voor gegevensbescherming, op het verzoek van de betrokken persoon overeenkomstig artikel 12 tot en met 22 van de voormelde verordening pas antwoorden nadat het Openbaar Ministerie of, in voorkomend geval, de onderzoeksrechter heeft bevestigd dat een antwoord het onderzoek niet in het gedrang brengt of kan brengen.

§5. De meldkanalen, vermeld in artikel 8 en 9, respecteren de regels met betrekking tot de verwerking en de bescherming van de persoonsgegevens in uitvoering van de algemene verordening gegevensbescherming."

Artikel 16.

"Meldkanalen, als vermeld in artikel 8 en 9, maken geen feiten openbaar die het economische, financiële of commerciële belang van een instelling kunnen schaden, tenzij dat noodzakelijk is voor de opvolging van de melding."

Artikel 34.

"In dezelfde codex[2], het laatst gewijzigd bij het decreet van 15 juli 2022, wordt aan hetzelfde hoofdstuk 3 een artikel V.230/7 toegevoegd, dat luidt als volgt:

Art. V.230/7. §1. Iedere instelling heeft een intern meldkanaal.

Het interne meldkanaal kan door de instelling zelf worden beheerd of extern ter beschikking worden gesteld door een derde. De waarborgen voor een interne melding en de opvolging van de meldingen, vermeld in hoofdstuk 4 en 5, zijn ook van toepassing als het interne meldkanaal door een derde wordt beheerd.

§2. Het interne meldkanaal bestaat uit ten minste een persoon die bevoegd is om meldingen te ontvangen en te behandelen. Personeelsleden met een mandaat in een beslissingsorgaan of personeelsafgevaardigden kunnen geen deel uitmaken van het interne meldkanaal.

De persoon die bevoegd is voor het ontvangen of behandelen van meldingen heeft daarvoor de nodige vorming gekregen.

§3. Iedere instelling werkt, na overleg met afgevaardigden van de representatieve vakorganisaties een procedure uit om interne meldingen in te dienen, te behandelen en te beheren. Als het interne meldkanaal door een derde ter beschikking gesteld wordt, worden de afgevaardigden van de representatieve vakorganisaties op de hoogte gebracht van de inhoud van de overeenkomst met de derde.

De procedure, vermeld in het eerste lid, bevat systemen die door hun ontwerp, opzet en beheer op beveiligde wijze de geheimhouding van de informatie waarborgen en de vertrouwelijkheid beschermen van de volgende elementen:
de identiteit van de melder;
de identiteit van derden die in de melding worden genoemd;
informatie waaruit de identiteit van de melder of een derde kan blijken.

Als het meldkanaal een melding behandelt, neemt het daarbij een strikte neutraliteit in acht. Een melding kan in geen geval behandeld worden door een persoon die betrokken is of was bij de feiten waarop de melding betrekking heeft.

Alleen personeelsleden die daarvoor gemachtigd zijn, hebben toegang tot de informatie, vermeld in het tweede lid.".""

Artikel 35.

"In dezelfde codex, het laatst gewijzigd bij het decreet van 15 juli 2022, wordt aan hetzelfde hoofdstuk 3 een artikel V.230/8 toegevoegd, dat luidt als volgt:

[2] Codex Hoger Onderwijs van 11 oktober 2013

Art. V.230/8. §1. Personeelsleden en externen kunnen informatie over inbreuken die instellingen begaan hebben, extern melden conform deel 4, titel 4.

§2. Het externe meldkanaal, vermeld in paragraaf 1, ontvangt meldingen via systemen die door hun ontwerp, opzet en beheer op beveiligde wijze de geheimhouding van de informatie waarborgen en de vertrouwelijkheid beschermen van al de volgende elementen:
de identiteit van de melder;
de identiteit van derden die in de melding worden genoemd;
informatie waaruit de identiteit van de melder of een derde kan blijken.

Als het meldkanaal een melding behandelt, neemt het daarbij een strikte neutraliteit in acht. Een melding kan in geen geval behandeld worden door een persoon die betrokken is of was bij de feiten waarop de melding betrekking heeft.

Alleen personeelsleden die daarvoor gemachtigd zijn, hebben toegang tot de informatie, vermeld in het eerste lid.”.”

Artikel 36.

“In dezelfde codex, het laatst gewijzigd bij het decreet van 15 juli 2022, wordt aan hetzelfde hoofdstuk 3 een artikel V.230/9 toegevoegd, dat luidt als volgt:

“Art. V.230/9. §1. Personeelsleden melden informatie over inbreuken in de instelling waar ze tewerkgesteld zijn, via het interne meldkanaal vermeld in artikel V.230/7. Personeelsleden kunnen informatie over inbreuken ook rechtstreeks melden via het externe meldkanaal, vermeld in artikel V.230/8, als ze menen dat de inbreuk intern niet doeltreffend behandeld kan worden of dat er een risico op represailles bestaat.

Externen melden informatie over inbreuken die een instelling begaat, aan het externe meldkanaal, vermeld in artikel V.230/8.

Een instelling kan het interne meldkanaal, vermeld in artikel V.230/7 ook openstellen voor bepaalde of alle externen.

§2. Personeelsleden en externen die informatie over inbreuken openbaar maken komen in aanmerking voor bescherming uit hoofde van dit decreet indien is voldaan aan een van de volgende voorwaarden:
ze hebben eerst intern en extern gemeld of ze hebben meteen extern gemeld conform paragraaf 1, en er zijn geen passende maatregelen genomen binnen drie maanden nadat het meldkanaal in kwestie de melding heeft ontvangen;
ze hebben gegronde redenen om aan te nemen dat:
a) de inbreuk kan een dreigend of reëel gevaar vormen voor het algemeen belang, bijvoorbeeld wanneer er sprake is van een noodsituatie of een risico op onherstelbare schade, of er bestaat een risico op represailles bij externe meldingen, of het is niet waarschijnlijk dat de inbreuk doeltreffend wordt behandeld wegens de bijzondere omstandigheden van de zaak, omdat bijvoorbeeld bewijsmateriaal kan worden achtergehouden of vernietigd, of een autoriteit kan samenspannen met de pleger van de inbreuk of met iemand die bij de inbreuk is betrokken.

Deze paragraaf is niet van toepassing op gevallen waarin een personeelslid of een externe rechtstreeks informatie aan de pers verstrekt op grond van specifieke bepalingen die een stelsel voor de bescherming van de vrijheid van meningsuiting en informatie instellen.”.”

Artikel 37.

"In dezelfde codex, het laatst gewijzigd bij het decreet van 15 juli 2022, wordt in titel 3/1, ingevoegd bij artikel 25, een hoofdstuk 4 ingevoegd, dat luidt als volgt:

"Hoofdstuk 4. Gemeenschappelijke bepalingen voor interne en externe meldingen"."

Artikel 38.

"In dezelfde codex, het laatst gewijzigd bij het decreet van 15 juli 2022, wordt aan hoofdstuk 4, ingevoegd bij artikel 37, een artikel V.230/10 toegevoegd, dat luidt als volgt:

"Art. V.230/10. §1. Melders kunnen schriftelijk en via de telefoon of een ander spraakberichtensysteem informatie over inbreuken melden bij de meldkanalen, vermeld in artikel V.230/7 en V.230/8. Ze hebben ook het recht op een fysieke ontmoeting binnen een redelijke termijn.

§2. De meldkanalen, vermeld in artikel V.230/7 en V.230/8, kunnen van mondelinge meldingen via een spraakberichtsysteem met gesprekopname:
een opname van het gesprek in een duurzame, opvraagbare vorm maken;
een volledig en nauwkeurig verslag laten opstellen door de personeelsleden die verantwoordelijk zijn om de melding te behandelen.

De meldkanalen, vermeld in artikel V.230/7 en V.230/8, stellen de melders voor de start van het gesprek op de hoogte van de mogelijkheid van het systeem om gesprekken op te nemen.

§3. De personeelsleden van de meldkanalen, vermeld in artikel V.230/7 en V.230/8, die verantwoordelijk zijn om de melding te behandelen, kunnen een nauwkeurig verslag opmaken van mondelinge meldingen via een spraakberichtsysteem zonder gespreksopnamefaciliteit.

§4. Als de melder toestemt, maken de meldkanalen, vermeld in artikel V.230/7 en V.230/8, bij een fysieke ontmoeting op verzoek van de melder:
een opname van het gesprek in een duurzame en opvraagbare vorm;
een nauwkeurig verslag van het onderhoud, dat de personeelsleden opstellen die verantwoordelijk zijn voor de behandeling van de melding.

§5. Melders kunnen de schriftelijke weergave van het gesprek, vermeld in paragraaf 2 tot en met 4, controleren, corrigeren en voor akkoord tekenen."."

Artikel 39.

"In dezelfde codex, het laatst gewijzigd bij het decreet van 15 juli 2022, wordt aan hetzelfde hoofdstuk 4 een artikel V.230/11 toegevoegd, dat luidt als volgt:

"Art. V.230/11. §1. De meldkanalen, vermeld in artikel V.230/7 en V.230/8, bevestigen de ontvangst van de melding aan de melder binnen zeven dagen na de dag waarop ze de melding hebben ontvangen, als ze binnen die termijn de melding nog niet afgehandeld hebben, tenzij in één van de volgende gevallen:
de melder verzet zich uitdrukkelijk tegen het krijgen van die ontvangstmelding;
het krijgen van die ontvangstmelding brengt de bescherming van de identiteit van de melder in gevaar.

Tenzij er nieuwe wettelijke of feitelijke omstandigheden zijn die een andere opvolging rechtvaardigen, kan het externe meldkanaal, vermeld in artikel V.230/8, bij meldingen over een instelling beslissen om in een van de volgende gevallen de melding niet in behandeling te nemen:
de inbreuk is van geringe betekenis;
de externe melding heeft betrekking op feiten die in een eerdere externe melding van de melder al zijn behandeld en de nieuwe melding bevat geen nieuwe informatie van betekenis.

In de gevallen, vermeld in het tweede lid, stuurt het externe meldkanaal, vermeld in artikel V.230/8, de melder binnen zeven dagen nadat het de melding heeft ontvangen, naast de ontvangstmelding, vermeld in het eerste lid, de beslissing om de melding niet in behandeling te nemen en een motivatie voor die beslissing.

§2. De meldkanalen, vermeld in artikel V.230/7 en V.230/8, gaan de juistheid na van de informatie en nemen de gepaste maatregelen als er een vermoeden van een inbreuk is.

§3. De meldkanalen, vermeld in artikel V.230/7 en V.230/8, informeren de melder binnen drie maanden na de dag waarop ze de ontvangstmelding hebben verstuurd, of, als er geen ontvangstmelding naar de melder is gestuurd, binnen drie maanden nadat de periode van zeven dagen nadat de melding is gedaan, is verstreken, over de als opvolging geplande of genomen maatregelen en over de redenen daarvoor. De meldkanalen, vermeld in artikel V.230/7 en V.230/8, geven daarbij geen informatie vrij die afbreuk doet aan het interne onderzoek of die het onderzoek of de rechten van de betrokken persoon schaadt.

Het externe meldkanaal, vermeld in artikel V.230/8, kan de termijn van drie maanden, vermeld in het eerste lid, verlengen tot maximaal zes maanden. In dat geval informeert het externe meldkanaal, vermeld in artikel V.230/8, de melder schriftelijk over de verlenging van de termijn en de reden daarvoor, voor de voormelde termijn van drie maanden verstreken is.

§4. Het externe meldkanaal, vermeld in artikel V.230/8, brengt de melder op de hoogte van het eindresultaat van de onderzoeken.”.”

Artikel 40.

“In dezelfde codex, het laatst gewijzigd bij het decreet van 15 juli 2022, wordt aan hetzelfde hoofdstuk 4 een artikel V.230/12 toegevoegd, dat luidt als volgt:

“Art. V.230/12. Als een melder een melding richt aan een onbevoegd extern meldpunt, stuurt dat onbevoegde externe meldkanaal de melding zo snel mogelijk op veilige wijze door naar het bevoegde meldkanaal. Het onbevoegde externe meldkanaal brengt de melder onmiddellijk op de hoogte van die doorzending.

Indien het intern meldkanaal niet bevoegd is om de melding te behandelen, dan brengt het meldkanaal de melder daarvan op de hoogte.”. “

Artikel 41.

“In dezelfde codex, het laatst gewijzigd bij het decreet van 15 juli 2022, wordt in titel 3/1, ingevoegd bij artikel 25, een hoofdstuk 5 ingevoegd, dat luidt als volgt:

“Hoofdstuk 5. Verwerking van gegevens”.”

Artikel 42.

"In dezelfde codex, het laatst gewijzigd bij het decreet van 15 juli 2022, wordt aan hoofdstuk 5, ingevoegd bij artikel 41, een artikel V.230/13 toegevoegd, dat luidt als volgt:

"Art. V.230/13. Ieder meldkanaal, vermeld in artikel V.230/7 en V.230/8, houdt een register bij van de ontvangen meldingen.

Ieder meldkanaal, vermeld in artikel V.230/7 en V.230/8, houdt al de volgende gegevens bij:
het aantal ontvangen meldingen;
het aantal onderzoeken en procedures die naar aanleiding van de meldingen zijn ingeleid en het resultaat ervan;
als dat wordt vastgesteld, de geschatte financiële schade en de bedragen die zijn teruggevorderd na onderzoeken en procedures over de gemelde inbreuken.

Meldingen worden niet langer opgeslagen dan noodzakelijk en evenredig is om te voldoen aan de vereisten die door deze codex of door andere wetgeving zijn opgelegd."."

Artikel 43.

"In dezelfde codex, het laatst gewijzigd bij het decreet van 15 juli 2022, wordt aan hetzelfde hoofdstuk 5 een artikel V.230/14 toegevoegd, dat luidt als volgt:

"Art. V.230/14. §1. In dit artikel wordt verstaan onder algemene verordening gegevensbescherming: verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

§2. Als die gegevens beschikbaar zijn, verwerken de meldkanalen, vermeld in artikel V.230/7 en V.230/8, de volgende persoonsgegevens op grond van artikel 6, eerste lid, e) van de algemene verordening gegevensbescherming bij de behandeling en registratie van meldingen:
de naam van de melder;
de contactgegevens en de functie van de melder;
de naam van de facilitator of van derden die verbonden zijn met de melder en die het slachtoffer kunnen worden van represailles in een werkgerelateerde context;
de naam en de functie van de betrokken persoon en informatie over de inbreuken van de betrokken persoon;
de naam van de getuigen;
schriftelijke meldingen;
het schriftelijke verslag van mondelinge meldingen en stemopnames, vermeld in artikel V.230/10, §2 en §3, van deze codex.

De meldkanalen, vermeld in artikel V.230/7 en V.230/8, wissen onmiddellijk andere gegevens dan de persoonsgegevens, vermeld in het eerste lid, die niet relevant zijn om de melding te behandelen.

§3. De meldkanalen, vermeld in artikel V.230/7 en V.230/8, maken de identiteit van de melder en alle informatie waarmee de identiteit van de melder direct of indirect achterhaald kan worden, niet bekend aan anderen dan de personeelsleden die bevoegd zijn om de melding te ontvangen en op te volgen tenzij in één van de volgende gevallen:
de melder stemt daarmee in;

er is een noodzakelijke en evenredige wettelijke verplichting in het kader van een onderzoek door nationale autoriteiten of gerechtelijke procedures, om de rechten van verdediging van de melder te waarborgen.

De meldkanalen, vermeld in artikel V.230/7 en V.230/8, maken de identiteit van de betrokken persoon en alle informatie waarmee de identiteit van de betrokken persoon direct of indirect achterhaald kan worden, niet bekend aan anderen dan de personeelsleden die bevoegd zijn om de melding te behandelen, zolang onderzoeken naar aanleiding van de melding of openbaarmaking lopen.

§4. Vóór de meldkanalen, vermeld in artikel V.230/7 en V.230/8, de identiteit van de melder of de betrokken persoon bekendmaken, brengen ze de melder, respectievelijk de betrokken persoon daarvan schriftelijk op de hoogte, samen met de redenen daarvoor, tenzij die informatie de onderzoeken of gerechtelijke procedures in gevaar brengt.

§. Met toepassing van artikel 23, lid 1, e) en h), van de algemene verordening gegevensbescherming kunnen de personeelsleden van een meldkanaal die daarvoor bevoegd zijn, bij wie een melding is ingediend, beslissen om de verplichtingen en de rechten, vermeld in artikel 12 tot en met 22 van de voormelde verordening, niet toe te passen bij de verwerking van persoonsgegevens in het kader van een onderzoek dat betrekking heeft op een welbepaalde natuurlijke persoon, als voldaan is aan de voorwaarden, vermeld in het tweede tot en met het negende lid.

De afwijkingsmogelijkheid, vermeld in het eerste lid, geldt alleen gedurende de periode waarin de betrokken persoon het voorwerp uitmaakt van een onderzoek, op voorwaarde dat het voor het goede verloop van het onderzoek noodzakelijk is of kan zijn dat de verplichtingen en de rechten, vermeld in artikel 12 tot en met 22 van de voormelde verordening, niet worden toegepast. De duur van het onderzoek mag in voorkomend geval niet meer bedragen dan een jaar vanaf de ontvangst van een verzoek tot uitoefening van een van de rechten, vermeld in artikel 12 tot en met 22 van de voormelde verordening.

De afwijkingsmogelijkheid, vermeld in het eerste lid, heeft geen betrekking op de gegevens die losstaan van het voorwerp van het onderzoek dat de weigering of de beperking van de rechten, vermeld in het tweede lid, rechtvaardigt.

Als de betrokken persoon in het geval, vermeld in het eerste lid, tijdens de periode, vermeld in het tweede lid, een verzoek indient op basis van artikel 12 tot en met 22 van de voormelde verordening, bevestigt de bevoegde functionaris voor gegevensbescherming, de ontvangst daarvan.

De bevoegde functionaris voor gegevensbescherming, brengt de betrokken persoon schriftelijk, zo snel mogelijk en in elk geval binnen een maand vanaf de dag die volgt op de dag waarop hij het verzoek heeft ontvangen, op de hoogte van elke weigering of beperking van de rechten, vermeld in het eerste lid. Verdere informatie over de nadere redenen voor die weigering of beperking hoeft niet te worden verstrekt als dat het onderzoek zou ondermijnen, met behoud van de toepassing van het achtste lid. Als het nodig is, kan de voormelde termijn met twee maanden worden verlengd, rekening houdend met het aantal aanvragen en de complexiteit ervan. De verwerkingsverantwoordelijke, bedoeld in artikel 4, 7), van de algemene verordening gegevensbescherming, brengt de betrokken persoon binnen dertig dagen vanaf de dag die volgt op de dag waarop hij het verzoek heeft ontvangen, op de hoogte van die verlenging en van de redenen voor het uitstel.

De bevoegde functionaris voor gegevensbescherming, informeert de betrokken persoon ook over de mogelijkheid om een verzoek in te dienen bij de Vlaamse toezichtcommissie voor de verwerking van persoonsgegevens conform artikel 10/5 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer, en om een beroep in rechte in te stellen.

De bevoegde functionaris voor gegevensbescherming, noteert de feitelijke of juridische gronden waarop de beslissing is gebaseerd. Die informatie houdt hij ter beschikking van de Vlaamse

toezichtcommissie, vermeld in artikel 10/1 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.

Nadat het onderzoek afgesloten is, worden de rechten, vermeld in artikel 13 tot en met 22 van de voormelde verordening, in voorkomend geval, conform artikel 12 van de voormelde verordening opnieuw toegepast.

Als een dossier dat persoonsgegevens als vermeld in het eerste lid, bevat, naar het Openbaar Ministerie is gestuurd en kan leiden tot activiteiten onder leiding van het Openbaar Ministerie of een onderzoeksrechter, en er onduidelijkheid is over het geheim van het onderzoek onder leiding van het Openbaar Ministerie of een onderzoeksrechter, mag de bevoegde functionaris voor gegevensbescherming, op het verzoek van de betrokken persoon overeenkomstig artikel 12 tot en met 22 van de voormelde verordening pas antwoorden nadat het Openbaar Ministerie of, in voorkomend geval, de onderzoeksrechter heeft bevestigd dat een antwoord het onderzoek niet in het gedrang brengt of kan brengen.

§5. De meldkanalen, vermeld in artikel V.230/7 en V.230/6, respecteren de regels met betrekking tot de verwerking en de bescherming van de persoonsgegevens in uitvoering van de algemene verordening gegevensbescherming.”.”

Artikel 44.

“In dezelfde codex, het laatst gewijzigd bij het decreet van 15 juli 2022, wordt aan hetzelfde hoofdstuk 5 een artikel V.230/15 toegevoegd, dat luidt als volgt:

“Art. V.230/15. Meldkanalen, als vermeld in artikel V.230/7 en V.230/8, maken geen feiten openbaar die het economische, financiële of commerciële belang van een instelling kunnen schaden, tenzij dat noodzakelijk is voor de opvolging van de melding.”.”

De VTC wil voorafgaand aan de bespreking van de specifieke ontwerpbepalingen **enkele algemene opmerkingen maken:**

Relatie met het melden van inbreuken op de GDPR

9. De VTC adviseert om verduidelijkingen aan te brengen inzake de verhouding met andere meldingsprocedures en klachtenprocedures waarbij een persoon aangeeft dat er in de werkomgeving een wettelijke of reglementaire bepaling niet wordt nageleefd.

10. De VTC wijst erop dat de AVG zelf een procedure bevat om inbreuken op de AVG te melden. Die meldingen moeten gedaan worden door de verwerkingsverantwoordelijke (de instantie zelf, in de praktijk de leidinggevende ervan). De functionaris voor gegevensbescherming wordt hierbij normaal gezien betrokken. Dit geldt voor inbreuken op de beveiliging, die meestal een schending zullen vormen van artikel 32, AVG. De VTC ontvangt en behandelt die meldingen.

11. Het is echter mogelijk dat een medewerker al dan niet functionaris een inbreuk vaststelt en de verantwoordelijke niet geneigd is om die te melden. Het lijkt de VTC dan aangewezen dat de functionaris of een andere werknemer die dat vaststelt beschermd wordt als die de melding zelf doet en dat die melding bij de VTC terecht komt.

12. De VTC behandelt ook klachten en informele meldingen die van werknemers kunnen uitgaan over mogelijke inbreuken op de AVG (al dan niet m.b.t. de beveiliging). De VTC zou het positief vinden dat de klagers en melders van de bescherming van de klokkenluidersregeling zouden kunnen gebruik maken, maar ook hier bij voorkeur in eerste instantie via een melding bij de VTC.

13. Het moet duidelijk zijn dat dergelijke meldingen in eerste instantie bij de VTC moeten terechtkomen, die de gespecialiseerde instantie is, dit zonder de andere kanalen uit te sluiten.

De problematiek van de bescherming van persoonsgegevens als de melder de vermeende inbreuk openbaar maakt

14. Het Ontwerp voorziet in artikel 10 § 2 en in artikel 36 dat een nieuw artikel V. 230/9 § 2 toevoegt aan de Codex Hoger Onderwijs van het Ontwerp :

> *"Personeelsleden en externen die informatie over inbreuken openbaar maken komen in aanmerking voor bescherming uit hoofde van dit decreet indien is voldaan aan een van de volgende voorwaarden:*
> *1° ze hebben eerst intern en extern gemeld of ze hebben meteen extern gemeld conform paragraaf 1, en er zijn geen passende maatregelen genomen binnen drie maanden nadat het meldkanaal in kwestie de melding heeft ontvangen;*
> *2° ze hebben gegronde redenen om aan te nemen dat:*
> *a) de inbreuk kan een dreigend of reëel gevaar vormen voor het algemeen belang, bijvoorbeeld wanneer er sprake is van een noodsituatie of een risico op onherstelbare schade, of b) er bestaat een risico op represailles bij externe meldingen, of het is niet waarschijnlijk dat de inbreuk doeltreffend wordt behandeld wegens de bijzondere omstandigheden van de zaak, omdat bijvoorbeeld bewijsmateriaal kan worden achtergehouden of vernietigd, of een autoriteit kan samenspannen met de pleger van de inbreuk of met iemand die bij de inbreuk is betrokken.*
> *Deze paragraaf is niet van toepassing op gevallen waarin een personeelslid of een externe rechtstreeks informatie aan de pers verstrekt op grond van specifieke bepalingen die een stelsel voor de bescherming van de vrijheid van meningsuiting en informatie instellen."*

15. Op basis van deze bepaling kan een melder dus niet alleen de feiten maar ook de identiteit van de betrokken personen openbaar maken en de bescherming krijgen waarin het decreet voorziet. Het openbaar maken brengt natuurlijk mee dat ook gegevens van de betrokken persoon en andere personen in de openbaarheid worden gebracht terwijl er nog geen onderzoek werd gevoerd. De VTC beveelt aan dat de al opgenomen transparantiebepalingen over de klokkenluidersprocedure en de bescherming van de randvoorwaarden (bv. proportionaliteit) die bij deze openbaarmaking horen, worden verduidelijkt in richtlijnen. De VTC doet ook opmerken dat "openbaar maken" een ruime betekenis heeft en ter kennis brengen van het publiek betekent.

II. ONDERZOEK VAN DE ADVIESAANVRAAG

1. Voorafgaande toelichting

16. De VTC stelt vast dat de personen van wie gegevens worden verzameld en uitgewisseld de volgende zijn: melder, derden, facilitator, betrokkene, getuigen;

en dat het minstens de volgende gegevens lijkt te betreffen : identificatie – en contactgegevens, stemopnames.

17. Het betreft informatie over natuurlijke personen met onder meer identificatiegegevens en dus gaat het om de verwerking van informatie over geïdentificeerde natuurlijke personen, zijnde persoonsgegevens zoals bedoeld in de AVG. De VTC gaat daarom na in hoeverre het Ontwerp en de bestaande decreten in lijn liggen met de principes van het gegevensbeschermingsrecht.

2. Kwaliteit van de regelgevende grondslag

18. Het komt de stellers van het Ontwerp toe om erover te waken dat – en dit ook voor de bestaande wet- en regelgeving - elke verwerking die in onderhavige context zal plaatsvinden een rechtvaardigingsgrond vindt in artikel 6 AVG.

19. Het Ontwerp of de memorie vermelden niet expliciet op grond van welke rechtvaardigingsgrond in de AVG de verwerking van persoonsgegevens zal plaatsvinden. De VTC gaat ervan uit dat de verwerking gebeurt in het kader van het uitoefenen van een taak van algemeen belang. De decreetgever zou dit wel zelf moeten aangegeven in het Ontwerp of de memorie.

20. De VTC wenst in herinnering te brengen dat elke overheidsinmenging in de bescherming van de persoonlijke levenssfeer zoals gewaarborgd door artikel 8 van het EVRM[3], artikel 7 van het Handvest van de Grondrechten van de Europese Unie samengelezen met artikel 52.1 van het Handvest en artikel 22 van de Grondwet moet worden voorgeschreven in een 'voldoende precieze wettelijke bepaling' die beantwoordt aan een dwingende maatschappelijke behoefte en evenredig is met de nagestreefde doelstelling. In een dergelijke precieze wettelijke bepaling moeten de essentiële elementen[4] van de met de overheidsinmenging gepaard gaande verwerkingen van persoonsgegevens omschreven zijn. [5]

21. Voor verwerkingen op basis van artikel 6, lid 1, e), AVG[6], die niet zozeer betrekking hebben op het privé-leven, maar eerder enkel op de bescherming van persoonsgegevens, moet het doeleinde voldoende duidelijk blijken uit de taak van algemeen belang of voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend door unierecht of lidstatelijk recht. Andere elementen van de verwerking die al duidelijk (eventueel impliciet) blijken uit de bestaande wetgeving moeten niet per se herhaald worden. De VTC vindt het niettemin een goede praktijk om dat wel te doen om een uniform kader te creëren waarop verschillende uitvoeringsbesluiten kunnen steunen. Bovendien maakt dit het veel gemakkelijker om de verwerkingen van persoonsgegevens te toetsen aan de AVG, zowel voor de toezichthouder als voor de betrokkenen. Er is dus een onderscheid te maken tussen de legaliteitstoets (eisen waaraan de wettelijke basis moet voldoen om geldig te zijn) en de conformiteitstoets aan de AVG.

22. Aangezien met de vermelding van de essentiële elementen ook minstens gedeeltelijk tegemoetgekomen wordt aan artikel 5, 1, a), AVG, dat bepaalt dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene behoorlijk en transparant is, zal het ontbreken van deze elementen zwaardere

---

[3] Europees Verdrag voor de Rechten van de Mens en de Fundamentele Vrijheden.

[4] Artikel 6, AVG vermeldt de volgende elementen:

- het doel van de verwerking;
- de types of categorieën van te verwerken persoonsgegevens; Deze gegevens moeten bovendien beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt („minimale gegevensverwerking");
- de betrokkenen;
- de entiteiten waaraan en doeleinden waarvoor de persoonsgegevens mogen worden verstrekt;
- de opslagperioden;
- de aanduiding van de verwerkingsverantwoordelijke(n).

[5] EHRM, arrest *Rotaru c. Roumania*, 4 mei 2000; GWH 23 april 2015, arrest nr. 44/2015, 63; GWH 5 oktober 2017, arrest nr. 100/2017, 17; GWH 15 maart 2018, arrest nr. 29/2018, 26; GwH 14 januari 2021, arrest nr. 2/2021, overw. B.22.1.e.e.; GwH 18 november 2021, arrest nr. 158/2021, overw. B.6; GwH 9 december 2021, B.53.1-B.53.2; R.v.St, adv. 68.936/AV van 7 april 2021 over een voorontwerp van wet *betreffende maatregelen van bestuurlijke politie tijdens een epidemische noodsituatie*, Parl.St. Kamer, 2020-2021, doc. nr. 551951/001, 94-98; SCHRAM, F., *Privacy & persoonsgegevens. Handboek*, Brussel, Politeia, 2019, 75-98, 111-116; DEGRAVE, E., "*L'é-gouvernement et la protection de la vie privée – Légalité, transparance et contrôle*" , Collection du CRIDS, Larcier, Brussel, 2014, p. 161 e.v.

[6] "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;"

transparantiemaatregelen vragen. Er zal immers niet naar wetgeving waarin de verwerking uitdrukkelijk geregeld is, kunnen verwezen worden.

23. De opstellers van de wettelijke en reglementaire teksten zullen moeten inschatten of de beoogde verwerking een meer uitgewerkte rechtsgrond nodig heeft. Daarbij moet in eerste instantie gekeken worden naar de graad van inmenging van de overheid in het privé-leven.

24. Hierbij moet er op gelet worden dat in een eventueel uitvoeringsbesluit (mits delegatie aan de Vlaamse Regering) verdere modaliteiten kunnen worden bepaald, maar dat de essentie in het decreet zelf moet worden opgenomen, wat nu nog niet het geval is. De VTC verwijst naar de rechtspraak van het Grondwettelijk Hof inzake delegatie door de wetgever[7].

25. De VTC wijst erop dat er mogelijk ook sprake is van persoonsgegevens als bedoeld in artikel 9.1, AVG, namelijk de stem als biometrisch gegeven (hier wel niet bedoeld voor identificatie, maar (ongewenste) identificatie is mogelijk – zie infra) en zoals bedoeld in artikel 10 AVG, namelijk de gegevens die verwerkt worden in eventuele gerechtelijke of administratiefrechtelijke procedures (artikel 19 en 49 van het Ontwerp).

26. Voor gegevens als bedoeld in artikel 9. 1, AVG is een bijzondere rechtvaardigingsgrond vereist.

27. Bijzondere categorieën van persoonsgegevens in de zin van de artikelen 9 en 10 AVG behoeven strengere beveiligingsmaatregelen. De VTC wijst op de toepasselijkheid van de artikelen 9 en 10, §2, WVG die aangeven welke bijkomende veiligheidsmaatregelen moeten voorzien worden:

- de categorieën van personen aanwijzen die de persoonsgegevens kunnen raadplegen, waarbij hun hoedanigheid ten opzichte van de verwerking van de betrokken gegevens nauwkeurig moet worden omschreven;
- de lijst van de aldus aangewezen categorieën van personen ter beschikking houden van de bevoegde toezichthoudende autoriteit voor gegevensbescherming;
- ervoor zorgen dat de aangewezen personen door een wettelijke of statutaire verplichting, of door een evenwaardige contractuele bepaling ertoe gehouden zijn het vertrouwelijke karakter van de betrokken gegevens in acht te nemen.

28. Wat de vertrouwelijkheidsverplichtingen betreft, heeft het Ontwerp een verplichting tot vertrouwelijke behandeling opgenomen. Zie de bespreking hiervan in het luik beveiliging van dit advies.

29. Andere maatregelen kunnen geformuleerd worden op basis van een gegevensbeschermingseffectbeoordeling (zie verder).

3. Doelbinding

30. Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt (artikel 5, 1, b), AVG).

31. De doeleinden van de gegevensverwerking worden niet expliciet in het Ontwerp vermeld, maar zijn eruit af te leiden: het ontvangen en de behandeling van meldingen van klokkenluiders.

[7] bv. GwH nr. 166/2011, 10 november 2011, overw. B.43.3 e.v., GwH nr. 158/2021, 18 november 2021, overw. B.8.4.2.

32. De doeleinden zijn dan ook welbepaald en transparant. Verder zijn de doeleinden die worden nagestreefd nuttig en noodzakelijk, rekening houdend met het algemeen belang. Er is een evenwicht tussen het belang van de betrokkenen om hun rechten en vrijheden te vrijwaren en het algemeen belang om tot een verwerking van gegevens over te gaan.

33. De VTC is van oordeel dat de doeleinden welbepaald, uitdrukkelijk omschreven en gerechtvaardigd zijn.

4. Verantwoordelijkheid

34. Artikel 4.7) AVG bepaalt dat voor de verwerkingen waarvan de regelgeving het doel en de middelen vastlegt, de **verwerkingsverantwoordelijke** diegene is die daarin als dusdanig wordt aangewezen.

35. Het Ontwerp bevat geen specifieke en expliciete bepalingen. Het is nochtans van belang dat de betrokkenen perfect weten tot wie zich te richten met het oog op het uitoefenen en afdwingen van de hen door de AVG toegekende rechten. Dit wordt dus bij voorkeur in de decreten opgenomen.

36. Er is weliswaar opgenomen in artikelen 15 en 43 van het Ontwerp dat de meldkanalen persoonsgegevens verwerken, maar de VTC beveelt aan om uitdrukkelijk op te nemen wie de verwerkingsverantwoordelijke is zodat de betrokkenen ook duidelijk weten tot wie ze zich dienen te richten.

37. De decreetgever, de Vlaamse Regering en de verwerkingsverantwoordelijken moeten nagaan of het uitvoeren van een **gegevensbeschermingseffectenbeoordeling** (GEB - artikel 35 AVG)[8] voor de verschillende gegevensstromen al dan niet noodzakelijk is.

38. De VTC gaat ervan uit dat de verwerkingen in deze context niet grootschalig zullen zijn, maar dat door het grote risico voor de melder en diegenen die al dan niet terecht vermeld worden in een meldingsdossier een GEB voor de verschillende verwerkingen zo niet verplicht, ten zeerste aangewezen is.

39. De VTC wijst erop dat een GEB aan de VTC kan worden voorgelegd voor advies. Bij een hoog risico is de consultatie van de VTC verplicht[9].

5. Minimale gegevensverwerking

40. Conform artikel 5.1, c), AVG, moeten de persoonsgegevens toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.

41. De **categorieën betrokkenen** zijn melder, derden, facilitator, betrokkene, getuigen en de **categorieën gegevens** :

- de naam van de melder;
- de contactgegevens en de functie van de melder;

---

[8] Voor meer uitleg over en model van GEB, zie:

- https://overheid.vlaanderen.be/vlaamse-toezichtcommissie-dpia

- Info op website van de federale Gegevensbeschermingsautoriteit: https://www.gegevensbeschermingsautoriteit.be/professioneel/avg/effectbeoordeling-geb

- Aanbeveling CBPL nr. 01/2018 (https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-01-2008.pdf)

- Richtlijnen Groep 29 (WP 248) (https://www.gegevensbeschermingsautoriteit.be/publications/handleiding-gegevensbeschermingseffectbeoordeling.pdf)

[9] Artikel 36, AVG bepaalt dit als volgt: "Wanneer uit een gegevensbeschermingseffectbeoordeling krachtens artikel 35 blijkt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken, raadpleegt de verwerkingsverantwoordelijke voorafgaand aan de verwerking de toezichthoudende autoriteit."

- de naam van de facilitator of van derden die verbonden zijn met de melder en die het slachtoffer kunnen worden van represailles in een werkgerelateerde context;

- de naam en de functie van de betrokken persoon en informatie over de inbreuken van de betrokken persoon;

- de naam van de getuigen;

- schriftelijke meldingen;

- het schriftelijke verslag van mondelinge meldingen en stemopnames, vermeld in artikel 11, §2 en §3, van dit decreet.

42. De VTC stelt vast dat wat de voorliggende regeling betreft, de categorieën van gegevens eerder algemeen zijn aangeduid met verwijzingen naar documenten in plaats van naar gegevenscategorieën, namelijk de inhoud van schriftelijke meldingen of van het schriftelijke verslag van mondelinge meldingen. De VTC begrijpt dat voor de bedoelde meldingen moeilijk beperkingen kunnen worden gesteld. Voor wat er geregistreerd wordt in de registers (artikel 14 en 42 dat een nieuw artikel V.230/13 invoert in de Codex Hoger Onderwijs van het Ontwerp) kan dit echter wel.

43. De VTC beoordeelt het positief dat het Ontwerp een bepaling bevat (artikel 15 § 2 en 43 dat een nieuw artikel V.230/14 invoert in de Codex Hoger Onderwijs) die oplegt dat de meldingskanalen onmiddellijk andere gegevens wissen dan de gegevens, vermeld in het eerste lid, die niet relevant zijn om de melding te behandelen. De VTC vraagt zich wel af hoe dit gerealiseerd zal worden.

44. De paragrafen 3 en 4 van het nieuwe artikel 15 en 43 dat een nieuw artikel V.230/14 invoert in de Codex Hoger Onderwijs bevatten regels met betrekking tot de bescherming van de identiteit van de betrokkenen (onderlijning VTC):

"§3. De meldkanalen, vermeld in artikel 8 en 9, maken de identiteit van de melder en alle informatie waarmee de identiteit van de melder direct of indirect achterhaald kan worden niet bekend aan anderen dan de personeelsleden die bevoegd zijn om de melding te ontvangen en op te volgen tenzij in één van de volgende gevallen:

a. de melder stemt daarmee in;

b. er is een noodzakelijke en evenredige wettelijke verplichting in het kader van een onderzoek door nationale autoriteiten of gerechtelijke procedures, om de rechten van verdediging van de melder te waarborgen.

De meldkanalen, vermeld in artikel 8 en 9, maken de identiteit van de betrokken persoon en alle informatie waarmee de identiteit van de betrokken persoon direct of indirect achterhaald kan worden, niet bekend aan anderen dan de personeelsleden die bevoegd zijn om de melding te behandelen, zolang onderzoeken naar aanleiding van de melding of openbaarmaking lopen.

§4. Vóór de meldkanalen, vermeld in artikel 8 en 9, de identiteit van de melder of de betrokken persoon bekendmaken, brengen ze de melder, respectievelijk de betrokken persoon daarvan schriftelijk op de hoogte, samen met de redenen daarvoor, tenzij die informatie de onderzoeken of gerechtelijke procedures in gevaar brengt."

45. De VTC is van oordeel dat er voldaan kan worden aan het principe van minimale gegevensverwerking als de persoonsgegevens in de registers tot het noodzakelijke worden beperkt.

46. Wat de instanties die toegang hebben betreft: het interne meldkanaal van de instelling of het personeelslid aangewezen door de regeringscommissaris.

47. Artikel 8 § 3 van het Ontwerp voorziet dat iedere instelling, na overleg met afgevaardigden van de representatieve vakorganisaties, een procedure uitwerkt om interne meldingen in te dienen, te behandelen en te beheren en artikel 24, dat wijzigingen aanbrengt aan artikel IV.104 van de Codex van het Ontwerp voorziet dat het college van commissarissen een procedure uitwerkt om externe meldingen van klokkenluiders te ontvangen en op te volgen. De VTC is echter van mening dat deze procedure beter opgenomen wordt in het decreet, minstens in een

uitvoeringsbesluit omdat het duidelijk moet zijn, ook voor de melders en de betrokkenen, dat de delegatie telkens een zeer beperkt aantal personen mag betreffen.

48. Door artikel 15 en 43 van het Ontwerp wordt uitvoering gegeven aan artikel 16/2 van de Klokkenluidersrichtlijn, wanneer onder andere gesteld wordt dat de identiteit van de melder bekend kan gemaakt worden aan anderen dan de personeelsleden die de melding ontvangen en opvolgen, als die daarmee instemt. De motivering hiervoor is dat de bekendmaking van de identiteit van de melder het onderzoek naar de melding vaak zal vergemakkelijken.

49. De VTC stelt vast dat er in het Ontwerp geen sprake is van systematische mededeling van persoonsgegevens aan andere overheidsinstanties. Er werd alleen een regeling opgenomen voor het geval een melding foutief zou geadresseerd worden.

50. 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.

51. Wat de **bewaartermijn** betreft, merkt de VTC op dat die niet vastgelegd wordt. Het moet evenwel duidelijk zijn hoelang de verwerkingsverantwoordelijke mag bijhouden. Hiervoor moet enerzijds gekeken worden naar de eventueel toepasselijke archiefwetgeving en anderzijds een proportionaliteitsafweging te worden gemaakt.

52. In het licht van artikel 6.3 van de AVG, adviseert de VTC om in het Ontwerp de maximale bewaartermijn(en) van de met het oog op de onderscheiden doeleinden voor deze verwerking van persoonsgegevens te voorzien, of toch minstens criteria op te nemen die toelaten deze bewaartermijn(en) te bepalen.

6. Juistheid

53. Persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd (artikel 5, 1, d), AVG).

54. Het Ontwerp bevat geen bepalingen hierover. De VTC beveelt aan dat de verwerkingsverantwoordelijke hiertoe de nodige maatregelen neemt.

7. Rechten van de betrokkenen en transparantie

55. De VTC neemt er akte van dat artikel 15 en artikel 43 van het Ontwerp afwijkingen op de **AVG-rechten** invoeren :

Artikel 15

"Met toepassing van artikel 23, lid 1, e) en h), van de algemene verordening gegevensbescherming kunnen de personeelsleden van een meldkanaal die daarvoor bevoegd zijn, bij wie een melding is ingediend, beslissen om de verplichtingen en de rechten, vermeld in artikel 12 tot en met 22 van de voormelde verordening, niet toe te passen bij de verwerking van persoonsgegevens in het kader van een onderzoek dat betrekking heeft op een welbepaalde natuurlijke persoon, als voldaan is aan de voorwaarden, vermeld in het tweede tot en met het negende lid.
De afwijkingsmogelijkheid, vermeld in het eerste lid, geldt alleen gedurende de periode waarin de betrokken persoon het voorwerp uitmaakt van een onderzoek, op voorwaarde dat het voor het goede verloop van het onderzoek noodzakelijk is of kan zijn dat de verplichtingen en de rechten, vermeld in artikel 12 tot en met 22 van de voormelde verordening, niet worden toegepast. De duur van het onderzoek mag in voorkomend geval niet meer bedragen dan een jaar vanaf de ontvangst van een verzoek tot uitoefening van een van de rechten, vermeld in artikel 12 tot en met 22 van de voormelde verordening.
De afwijkingsmogelijkheid, vermeld in het eerste lid, heeft geen betrekking op de gegevens die losstaan van het voorwerp van het onderzoek dat de weigering of de beperking van de rechten, vermeld in het tweede lid, rechtvaardigt.

Als de betrokken persoon in het geval, vermeld in het eerste lid, tijdens de periode, vermeld in het tweede lid, een verzoek indient op basis van artikel 12 tot en met 22 van de voormelde verordening, bevestigt de bevoegde functionaris voor gegevensbescherming, de ontvangst daarvan.
De bevoegde functionaris voor gegevensbescherming, brengt de betrokken persoon schriftelijk, zo snel mogelijk en in elk geval binnen een maand vanaf de dag die volgt op de dag waarop hij het verzoek heeft ontvangen, op de hoogte van elke weigering of beperking van de rechten, vermeld in het eerste lid. Verdere informatie over de nadere redenen voor die weigering of beperking hoeft niet te worden verstrekt als dat het onderzoek zou ondermijnen, met behoud van de toepassing van het achtste lid.
Als het nodig is, kan de voormelde termijn met twee maanden worden verlengd, rekening houdend met het aantal aanvragen en de complexiteit ervan. De verwerkingsverantwoordelijke, vermeld in artikel 4, 7), van de algemene verordening gegevensbescherming, brengt de betrokken persoon binnen dertig dagen vanaf de dag die volgt op de dag waarop hij het verzoek heeft ontvangen, op de hoogte van die verlenging en van de redenen voor het uitstel.
De bevoegde functionaris voor gegevensbescherming, informeert de betrokken persoon ook over de mogelijkheid om een verzoek in te dienen bij de Vlaamse toezichtcommissie voor de verwerking van persoonsgegevens conform artikel 10/5 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer, en om een beroep in rechte in te stellen.
De bevoegde functionaris voor gegevensbescherming noteert de feitelijke of juridische gronden waarop de beslissing is gebaseerd. Die informatie houdt hij ter beschikking van de Vlaamse toezichtcommissie, vermeld in artikel 10/1 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.
Nadat het onderzoek afgesloten is, worden de rechten, vermeld in artikel 13 tot en met 22 van de voormelde verordening, in voorkomend geval, conform artikel 12 van de voormelde verordening opnieuw toegepast.
Als een dossier dat persoonsgegevens als vermeld in het eerste lid, bevat, naar het Openbaar Ministerie is gestuurd en kan leiden tot activiteiten onder leiding van het Openbaar Ministerie of een onderzoeksrechter, en er onduidelijkheid is over het geheim van het onderzoek onder leiding van het Openbaar Ministerie of een onderzoeksrechter, mag de bevoegde functionaris voor gegevensbescherming, op het verzoek van de betrokken persoon overeenkomstig artikel 12 tot en met 22 van de voormelde verordening pas antwoorden nadat het Openbaar Ministerie of, in voorkomend geval, de onderzoeksrechter heeft bevestigd dat een antwoord het onderzoek niet in het gedrang brengt of kan brengen."

Artikel 43

"Met toepassing van artikel 23, lid 1, e) en h), van de algemene verordening gegevensbescherming kunnen de personeelsleden van een meldkanaal die daarvoor bevoegd zijn, bij wie een melding is ingediend, beslissen om de verplichtingen en de rechten, vermeld in artikel 12 tot en met 22 van de voormelde verordening, niet toe te passen bij de verwerking van persoonsgegevens in het kader van een onderzoek dat betrekking heeft op een welbepaalde natuurlijke persoon, als voldaan is aan de voorwaarden, vermeld in het tweede tot en met het negende lid.
De afwijkingsmogelijkheid, vermeld in het eerste lid, geldt alleen gedurende de periode waarin de betrokken persoon het voorwerp uitmaakt van een onderzoek, op voorwaarde dat het voor het goede verloop van het onderzoek noodzakelijk is of kan zijn dat de verplichtingen en de rechten, vermeld in artikel 12 tot en met 22 van de voormelde verordening, niet worden toegepast. De duur van het onderzoek mag in voorkomend geval niet meer bedragen dan een jaar vanaf de ontvangst van een verzoek tot uitoefening van een van de rechten, vermeld in artikel 12 tot en met 22 van de voormelde verordening.
De afwijkingsmogelijkheid, vermeld in het eerste lid, heeft geen betrekking op de gegevens die losstaan van het voorwerp van het onderzoek dat de weigering of de beperking van de rechten, vermeld in het tweede lid, rechtvaardigt.
Als de betrokken persoon in het geval, vermeld in het eerste lid, tijdens de periode, vermeld in het tweede lid, een verzoek indient op basis van artikel 12 tot en met 22 van de voormelde verordening, bevestigt de bevoegde functionaris voor gegevensbescherming, de ontvangst daarvan.

De bevoegde functionaris voor gegevensbescherming, brengt de betrokken persoon schriftelijk, zo snel mogelijk en in elk geval binnen een maand vanaf de dag die volgt op de dag waarop hij het verzoek heeft ontvangen, op de hoogte van elke weigering of beperking van de rechten, vermeld in het eerste lid. Verdere informatie over de nadere redenen voor die weigering of beperking hoeft niet te worden verstrekt als dat het onderzoek zou ondermijnen, met behoud van de toepassing van het achtste lid.
Als het nodig is, kan de voormelde termijn met twee maanden worden verlengd, rekening houdend met het aantal aanvragen en de complexiteit ervan. De verwerkingsverantwoordelijke, bedoeld in artikel 4, 7), van de algemene verordening gegevensbescherming, brengt de betrokken persoon binnen dertig dagen vanaf de dag die volgt op de dag waarop hij het verzoek heeft ontvangen, op de hoogte van die verlenging en van de redenen voor het uitstel.
De bevoegde functionaris voor gegevensbescherming, informeert de betrokken persoon ook over de mogelijkheid om een verzoek in te dienen bij de Vlaamse toezichtcommissie voor de verwerking van persoonsgegevens conform artikel 10/5 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer, en om een beroep in rechte in te stellen.
De bevoegde functionaris voor gegevensbescherming, noteert de feitelijke of juridische gronden waarop de beslissing is gebaseerd. Die informatie houdt hij ter beschikking van de Vlaamse toezichtcommissie, vermeld in artikel 10/1 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.
Nadat het onderzoek afgesloten is, worden de rechten, vermeld in artikel 13 tot en met 22 van de voormelde verordening, in voorkomend geval, conform artikel 12 van de voormelde verordening opnieuw toegepast.
Als een dossier dat persoonsgegevens als vermeld in het eerste lid, bevat, naar het Openbaar Ministerie is gestuurd en kan leiden tot activiteiten onder leiding van het Openbaar Ministerie of een onderzoeksrechter, en er onduidelijkheid is over het geheim van het onderzoek onder leiding van het Openbaar Ministerie of een onderzoeksrechter, mag de bevoegde functionaris voor gegevensbescherming, op het verzoek van de betrokken persoon overeenkomstig artikel 12 tot en met 22 van de voormelde verordening pas antwoorden nadat het Openbaar Ministerie of, in voorkomend geval, de onderzoeksrechter heeft bevestigd dat een antwoord het onderzoek niet in het gedrang brengt of kan brengen."

56. Deze afwijking wordt in de memorie niet verantwoord.

57. Het moet duidelijk zijn dat de beperking van de rechten niet van toepassing mag zijn op de rechten van de melder zelf, die in principe op de hoogte is van het onderzoek en waarvoor dus geen geheimhouding en inkorting van de rechten vereist is. Uit de formulering van het Ontwerp blijkt dit niet zo duidelijk: "bij de verwerking van persoonsgegevens in het kader van een onderzoek dat betrekking heeft op een welbepaalde natuurlijke persoon".

58. De VTC herhaalt wat ze al in verschillende adviezen heeft gemeld over de procedure van toepassing bij het beperken van de rechten van betrokkenen:

59. Deze paragraaf is geschreven op basis van een standaardbepaling die met het AVGdecreet werd opgenomen in diverse Vlaamse regelgeving, onder andere voor Audit Vlaanderen, na de inwerkingtreding van de AVG en in die bepaling wordt onder meer het volgende gesteld: "Art. 9. Met toepassing van artikel 23, lid 1, a), c), d) en i), van de algemene verordening gegevensbescherming kunnen de diensten, voorzieningen en gesubsidieerde organisaties, vermeld in artikel 3, en de gemeenten, beslissen om de verplichtingen en de rechten, vermeld in artikel 12 tot en met 21 van de voormelde verordening, niet toe te passen bij de verwerking van persoonsgegevens in het kader van dit decreet als voldaan is aan de voorwaarden, vermeld in het tweede tot en met het zevende lid."

60. De federale Gegevensbeschermingsautoriteit[10] werd niet geraadpleegd bij de totstandkoming van het AVG-decreet, maar wel om advies gevraagd bij een Ontwerp van besluit van de Vlaamse Regering dat gelijkaardige bepalingen bevat[11].

61. De Autoriteit bekritiseerde de formulering waarbij de rechten van de betrokkene "niet worden toegepast" (hier "niet toe te passen"), terwijl enkel een beperking van de reikwijdte mogelijk is volgens de AVG. De VTC sluit zich aan bij deze opmerking en verwijst naar het volledige advies van de Autoriteit.

62. De VTC herinnert de decreetgever aan haar opmerking gemaakt in haar advies A/W/2019/16 (randnummer 27), inzake de tegenstrijdige bepaling in artikel 10/5 van het e-govdecreet wat de taken van de VTC betreft.

63. De VTC beveelt aan om deze afwijking omstandig te motiveren in de memorie.

64. Artikel 12 AVG bepaalt dat de verwerkingsverantwoordelijke passende maatregelen neemt opdat de betrokkene de in de artikelen 13 en 14, AVG bedoelde informatie en de in de artikelen 15 tot en met 22 en artikel 34, AVG bedoelde communicatie in verband met de verwerking in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt.

65. Aangezien artikelen 17 en 46 al bepaalde vermeldingen op de website van de dienst die de Vlaamse Regering aanwijst, oplegt inzake de klokkenluidersprocedure, is het volgens de VTC aangewezen om die vermeldingen aan te vullen met de verplichte vermeldingen op grond van de AVG zodat de betrokkenen goed geïnformeerd worden over de verwerking van hun persoonsgegevens en het voor de betrokkenen duidelijk is wat hun rechten zijn en tot wie zij zich moeten richten voor de uitoefening van hun rechten. Alle verantwoordelijken moeten hiervoor de nodige maatregelen nemen.

8. Beveiligingsmaatregelen

66. Artikel 32 AVG verplicht de verwerkingsverantwoordelijke om gepaste technische en organisatorische maatregelen te treffen die nodig zijn voor de bescherming van de persoonsgegevens. Deze maatregelen moeten een passend beveiligingsniveau verzekeren rekening houdend, enerzijds, met de stand van de techniek ter zake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen gegevens en de potentiële risico's.

67. De VTC wijst erop dat aangezien de gegevens niet duidelijk afgebakend zijn, er het risico is voor represailles en het mogelijk persoonsgegevens als bedoeld in artikel 10, AVG betreft, een bijzondere aandacht vereist is inzake informatieveiligheid.

68. De VTC beoordeelt het positief dat in het Ontwerp het principe van gegevensbescherming door ontwerp (artikel 25, AVG) wordt toegepast, met name in de artikelen 9 en 34 :

"(…) via systemen die door hun ontwerp, opzet en beheer op beveiligde wijze de geheimhouding van de informatie waarborgen en de vertrouwelijkheid beschermen van al de volgende elementen:
1° de identiteit van de melder;
2° de identiteit van derden die in de melding worden genoemd;
3° informatie waaruit de identiteit van de melder of een derde kan blijken."

[10] De toenmalige VTC evenmin

[11] Advies nr. 88/2018 van 26 september 2018 betreffende het ontwerp van besluit van de Vlaamse Regering houdende aanpassing van de besluiten van de Vlaamse Regering aan de verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming) (CO-A2018-079)

69. De VTC beveelt wel aan om deze verplichting uit te breiden naar elke (en zeker de externe) communicatie in verband met het dossier.

70. Het waarborgen van de anonimiteit bij anonieme meldingen moet zeker ook voldoende aandacht krijgen.

71. In het Ontwerp wordt ook al rekening gehouden met de mogelijkheid van het verkeerd of onveilig versturen van een melding in artikel 13 (onderlijning VTC):

> *"Als een melder een melding richt aan een onbevoegd extern meldkanaal, stuurt dat onbevoegde meldkanaal, personeelslid of die onbevoegde instelling de melding zo snel mogelijk op veilige wijze door naar het bevoegde externe meldkanaal. Het onbevoegde externe meldkanaal brengt de melder onmiddellijk op de hoogte van die doorzending.*
> *Indien het intern meldkanaal niet bevoegd is om de melding te behandelen, dan brengt het meldkanaal de melder daarvan op de hoogte."*

72. Bovendien moet er rekening gehouden worden met de mogelijkheid dat bij een melding via de telefoon of een ander spraakberichtensysteem het gesprek opgenomen wordt, wat het risico op identificatie vergroot. "een opname van het gesprek in een duurzame, opvraagbare vorm maken".

73. De VTC beveelt aan om de opnames onmiddellijk vervormd te maken.

74. Krachtens artikel 124 van de Wet betreffende de elektronische communicatie (WEC) mag niemand met opzet kennisnemen van het bestaan van informatie van alle aard die via elektronische weg is verstuurd en die niet persoonlijk voor hem bestemd is tenzij hij toestemming heeft gekregen van alle andere, direct of indirect betrokken personen.

75. Er zou een uitzondering kunnen voorzien worden conform artikel 125 van de vermelde wet[12], maar de VTC adviseert om toestemming te vragen aan de betrokkene.

76. Artikel 32, AVG wijst op een aantal voorbeeldmaatregelen om, waar passend, een op het risico afgestemd beveiligingsniveau te waarborgen:

- de pseudonimisering en versleuteling van persoonsgegevens;
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

77. Voor de concrete uitwerking hiervan wijst de VTC op de aanbeveling[13] ter voorkoming van gegevenslekken en op de referentiemaatregelen[14] die bij elke verwerking van persoonsgegevens in acht zouden moeten worden genomen. De VTC benadrukt ook het belang van een behoorlijk gebruikers- en toegangsbeheer[15] en een logging van de toegangen

---

[12] "Art. 125. § 1. De bepalingen van artikel 124 van deze wet en de artikel en 259bis en 314bis van het Strafwetboek zijn niet van toepassing: 1° wanneer de wet het stellen van de bedoelde handelingen toestaat of oplegt; [...]."

[13] Aanbeveling CBPL nr. 01/2013

(https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-01-2013.pdf)

[14] Referentiemaatregelen CBPL voor de beveiliging van elke verwerking van persoonsgegevens, Versie 1.0 (https://www.gegevensbeschermingsautoriteit.be/publications/nota-inzake-de-beveiliging-van-persoonsgegevens.pdf)

[15] Zie ook Aanbeveling CBPL nr. 01/2008

(https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-01-2008.pdf)

Verschillende instanties kunnen hiervoor aangepaste technologische oplossingen bieden (zoals bijvoorbeeld de Kruispuntbank van de Sociale zekerheid).

zodat de functionaris en de toezichthouders kunnen controleren wie wanneer toegang had tot welke gegevens, wat zijn/haar acties waren en waarom[16].

78. Voor zover er gedacht wordt aan het gebruik van cloudtoepassingen, verwijst de VTC naar haar adviezen en aanbevelingen daarover[17].

79. In principe moet de specificering van maatregelen niet in de wetgeving worden opgenomen. Wanneer de decreetgever of in een later stadium (mits delegatie), de Vlaamse Regering echter vermoedt dat de gepaste maatregelen niet gerealiseerd zullen worden zonder dit aan de betrokken instanties expliciet op te leggen, dan moet dat wel gebeuren[18].

III. BESLUIT

80. De VTC is van oordeel dat het voorgelegde voorontwerp voldoende waarborgen zou kunnen bieden wat de bescherming van de persoonsgegevens van de betrokkenen betreft, op voorwaarde dat daarin volgende elementen bijkomend worden geïmplementeerd, inzonderheid:

- verduidelijkingen aanbrengen in verband met andere bestaande meldings- en klachtenprocedures (luik "algemene opmerkingen")
- transparantiebepalingen en bescherming van de randvoorwaarden verduidelijken in richtlijnen (luik "algemene opmerkingen")
- de rechtvaardigingsgrond toevoegen aan het Ontwerp of de memorie (luik 2);
- de rechtvaardigingrond bij toepassing van artikel 9.1. en 10 AVG motiveren in de memorie (luik 2);
- de verwerkingsverantwoordelijke bepalen en expliciet benoemen in het Ontwerp (luik 4)
- een gegevensbeschermingseffectenbeoordeling uitvoeren (luik 4);
- de categorieën gegevens specifiëren (luik 5);
- de procedure om interne meldingen in te dienen, te behandelen en te beheren opnemen in het Ontwerp of minstens in een uitvoeringsbesluit (luik 5);
- de bewaartermijn bepalen, minstens criteria opnemen in het Ontwerp die toelaten om de bewaartermijn te bepalen (luik 5);
- de nodige maatregelen nemen voor de juistheid van de gegevens (luik 6);
- afwijkingen op de AVG – rechten omstandig motiveren in de memorie (luik 7);
- specifiëren dat de rechten van de melder niet beperkt worden (luik 7);
- de vermeldingen op de website aanvullen met de verplichte vermeldingen op grond van de AVG (luik 7);
- gegevensbescherming door ontwerp uitbreiden naar elke communicatie in het dossier (luik 8);
- opnames van meldingen vervormd maken (luik 8);
- toestemming vragen aan de betrokkene conform artikel 124 WEC (luik 8).

Hans Graux,
Voorzitter VTC

Getekend door:Hans Graux (Signature)
Getekend op:2022-11-30 11:34:29 +01:0
Reden:Ik keur dit document goed

[16] *Audit trailing* of *beveiligd controlespoor*.

[17] https://overheid.vlaanderen.be/vlaamse-toezichtcommissie-cloud

[18] Dit kan eventueel ook in een ministerieel besluit of een omzendbrief.