



Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens

Advies wetgeving VTC nr. 2023/20 van 6 maart 2023

over

tekst	Ontwerp van decreet
van	van de Vlaamse Regering
titel	houdende de bevordering van de integriteitsbeoordeling door het openbaar bestuur en tot oprichting van een Dienst integriteitsbeoordeling voor Openbare besturen
roepnaam	(decreet casusoverleg)
datum	zoals principieel goedgekeurd op 27 januari 2023

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 mevrouw Zuhail Demir, Vlaams minister Vlaamse minister van Justitie en Handhaving, Omgeving, Energie en Toerisme van 30 januari 2023, ontvangen door de VTC op 30 januari 2023;

Gelet op de behandeling op de zitting van 6 maart 2023;

Brengt op 6 maart 2023 het volgend advies uit:

I. VOORWERP VAN DE ADVIESAANVRAAG

1. De Vlaamse minister bevoegd voor Justitie en Handhaving (hierna "de adviesvrager") verzocht om het advies van de Vlaamse Toezichtcommissie (hierna "VTC") over een ontwerp van decreet *houdende de bevordering van de integriteitsbeoordeling door het openbaar bestuur en tot oprichting van een Dienst integriteitsbeoordeling voor Openbare besturen* (hierna "het Ontwerp").

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. Vlaanderen wil vermijden dat de Vlaamse overheid en de lokale overheden ongewild georganiseerde en ondermijnende criminele activiteiten en personen zouden faciliteren.
4. Er wordt een decretaale regeling uitgewerkt die een betere informatiedeling moet toelaten tussen de verschillende beleidsniveaus om zo op gegronde wijze bv vergunningen, concessies, subsidies en overheidsopdrachten te kunnen laten weigeren, schorsen, intrekken opheffen of voorwaarden aan verbinden door het bevoegde bestuur.
5. Het decreet wil tegemoet komen aan de verzuchtingen van de openbare besturen, vooral, maar niet uitsluitend op het lokale niveau om korter op de bal te kunnen spelen als er georganiseerde criminele activiteiten vermoed worden bij bv. de aanvraag van een vergunning, concessie, subsidie,...
6. Dit ontwerp van decreet vertrekt vanuit de engagementen vastgelegd in het Vlaams Regeerakkoord 2019-2024 waarin het volgende wordt bepaald:

“We creëren een decretaal kader voor de weigering, schorsing of intrekking van (omgevings)vergunningen, subsidies, concessies en overheidsopdrachten, indien blijkt dat een burger of onderneming crimineel is, of er een ernstige risico bestaat op georganiseerde criminaliteit en ondermijning. Dit gebeurt aan de hand van een integriteitsonderzoek. We willen een geëngageerde en betrouwbare partner zijn van lokale overheden, andere deelstaten, de federale overheid en internationale partners in de strijd tegen georganiseerde criminaliteit en ondermijning. Hiervoor sluiten we de nodige samenwerkingsakkoorden. We zullen actief pleiten voor een kader inzake gegevensuitwisseling tussen overheden, zodat alle overheden hun handhavingsbevoegdheden ten volle kunnen benutten.”

7. In de beleidsnota 2019-2024 Justitie en Handhaving van minister Zuhail Demir wordt dit verder uitgewerkt:

“[...] In de strijd tegen georganiseerde misdaad heeft de veiligheidsketen, naast de reactief strafrechtelijke aanpak, dus ook behoefte aan een bestuurlijke aanpak, waarmee kan worden voorkomen dat criminele organisaties in bepaalde gemeenten voet aan de grond krijgen om van daaruit hun criminele activiteiten verder te ontplooiën. Een effectief antwoord op dit crimineel fenomeen is dan niet enkel gericht op het opsporen en vervolgen van daders, maar ook op de verstoring van de gelegenheidsstructuren en het afbreken van de economische machtsposities van deze criminele groeperingen. Criminele ondernemers en organisaties manifesteren zich op lokaal niveau op meerdere wijzen. Ze investeren in vastgoed en horeca om criminele gelden wit te wassen en om een legale dekmantel te hebben. Ze werpen zich op in het verenigingsleven, waarmee ze een sociale erkentelijkheid nastreven en zich in de bovenbouw van de samenleving innestelen. Ze huren bedrijfspanden of woningen om hun criminele activiteiten te kunnen plegen of te faciliteren (bv. cannabisplantages, labo's synthetische drugs, opslagplaatsen voor gestolen goederen, enzovoort). Ze hebben behoefte aan plaatsen voor ontmoeting (bv. de clubhuizen van criminele motorbendes) of om hun illegale goederen te helen. Enzovoort.

Aangezien regionale en lokale overheden erkenningen, vergunningen en subsidies verlenen en activiteiten ondersteunen, bijvoorbeeld via de openbare aanbesteding van infrastructuurwerken, kunnen ze het risico lopen om, onbewust en ongewild, de activiteiten van criminele ondernemers hierdoor te faciliteren. In het bijzonder om deze redenen is het daarom belangrijk dat de lokale overheden de nodige regelgevende instrumenten ter beschikking gesteld krijgen om een bestuurlijke aanpak te organiseren, op maat van de eigen veiligheidsdiagnostiek en ter aanvulling van de gerechtelijke aanpak.

Dat dit broodnodig is, maken bepaalde lokale besturen ons sinds enkele jaren duidelijk. Zij startten reeds een aantal projecten rond bestuurlijke handhaving op, omdat zij in stijgende mate te maken krijgen met grenscriminaliteit, voornamelijk vanuit Nederland. Dit gaat dan over de productie van

synthetische drugs, cannabisplantages en drugshandel in het algemeen, alsook over criminele motorbendes. De verschuiving van criminele fenomenen wordt onder andere toegeschreven aan de strengere Nederlandse bestuurlijke aanpak van criminele bendes. Het is daarom hoog tijd dat ook Vlaanderen zich wapent met een degelijke, bestuurlijke aanpak.

8. De Toelichting geeft inzake informatie-uitwisseling nog het volgende aan:

“Het ontwerp van decreet laat toe dat lokale besturen een integriteitsadvies kunnen vragen aan de DIOB op basis waarvan zij een beslissing kunnen nemen om een bepaalde bestuurshandeling te weigeren, te schorsen, in te trekken of op te heffen. De lokale besturen moeten dit integriteitsonderzoek laten uitvoeren door de DIOB, ze kunnen niet zelf alle relevante databronnen raadplegen.”

9. Over de plaats van het DIOB wordt het volgende gesteld:

“Indien niet kan aangesloten worden bij de federale DIOB (via een detachering van Vlaamse ambtenaren), zal de DIOB zich situeren binnen het Agentschap Justitie en Handhaving en zal omkleed worden met de nodige garanties m.b.t. onafhankelijkheid en integriteit.”

II. ONDERZOEK VAN DE ADVIESAANVRAAG

1. Voorafgaande toelichting

10. De VTC stelt vast dat de personen van wie gegevens worden verzameld en uitgewisseld minstens de volgende zijn:
- personen voor wie er ernstige aanwijzingen zijn dat betrokkene rechtstreeks of onrechtstreeks deelnemer is aan ernstige sanctioneerbare feiten die verband kunnen houden met een toegekend of toe te kennen recht
 -
 - en dat het minstens de volgende gegevens betreft (voor een volledig overzicht zie infra):
 - identificatiegegevens;
 - financiële gegevens;
 - administratiefrechtelijke gegevens;
 - gerechtelijke gegevens.
11. 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.

Bezorgdheden

12. Hierna wordt in detail ingegaan op de verschillende elementen van het Ontwerp. De VTC wil hier echter al aangeven dat ze zeer bezorgd is over de ontworpen regeling in het algemeen. De reden daarvoor is in de eerste plaats de zeer ruime en ook onduidelijke omschrijvingen die niet beantwoorden aan de door de AVG gevraagde proportionaliteit enerzijds en substantiële onzekerheid meebrengen voor de betrokkenen – die overigens niet op een afdoende voorspelbare manier worden omschreven in het Ontwerp, zodat de impact van het Ontwerp op het fundamentele recht op gegevensbescherming erg moeilijk te voorspellen is.

13. Zoals het nu omschreven is, lijkt de **zeer ingrijpende regeling** zich niet te beperken tot ernstige misdrijven die haar zouden kunnen rechtvaardigen. In het federale wetsontwerp¹ is er nog sprake van “ondermijnende criminaliteit”(gedefinieerd in artikel 2 van het wetsontwerp) terwijl dit Ontwerp als criterium “ernstige sanctioneerbare feiten” geeft². Het Ontwerp volgt deze aanpak niet, en neemt expliciet ook feiten waarop een louter bestuurlijke sanctie staat binnen de draagwijdte op. Dit is een enorme uitbreiding.
14. Bovendien in de federale integriteitsbeoordeling beperkt tot bepaalde sectoren op basis van een risicoanalyse, wat hier ook niet het geval is; het Ontwerp voorziet nauwelijks beperkingen voor Vlaamse instanties om integriteitsonderzoeken te lanceren . Het is volgens de VTC dan ook aangewezen het toepassen van een integriteitsbeoordeling ook te beperken wat de administratieve procedures betreft waarop ze een impact kan hebben en deze wel uitdrukkelijk op te lijsten.
15. Ook doordat er geen beperking is tot veroordeelde feiten, is er sprake van een te grote inmenging. Dit strookt niet met het vermoeden van onschuld.
16. Zoals verder wordt aangegeven zijn er nog veel andere onduidelijke elementen die teveel subjectieve beoordeling mogelijk laten.
17. Ook worden impliciete verwerkingen van bepaalde categorieën betrokkenen en gegevens van niet behandeld, zodat er geen rechtsbasis voor is. Dat geldt ook voor de - niet expliciet vermelde - dataming en profilering.
18. De bakens worden met andere woorden heel ver geplaatst, op een wijze die burgers op een onvoorspelbare manier blootstelt aan potentieel verregaande inbreuken op hun recht op gegevensbescherming, en er zijn te weinig waarborgen om de rechten en vrijheden van de betrokkenen in die context te beschermen.
19. Een ander punt van bezorgdheid is het terugvloeien van de door de bevoegde besturen en het DIOB verzamelde gegevens naar de politiediensten en de garanties rond beperkte bewaartermijnen daarbij. Meer algemeen dient een duplicatie van gegevens bij de Vlaamse en Federale diensten te worden vermeden.
20. De VTC is ook verontrust door het toevertrouwen van zo’n gevoelige verwerking aan kleine entiteiten zoals gemeenten, waarvan geweten is dat ze zeer kwetsbaar zijn waar het om de vertrouwelijkheid en veiligheid van gegevens gaat.
21. Er lijkt geen sprake te zijn van een gefundeerde risicoanalyse voor het hele project. De VTC is van oordeel dat dat zou moeten uitgevoerd worden door alle genoemde instanties samen (m.a.w. in afstemming met alle structurele partners, inclusief op federaal niveau over een haalbaar, wenselijk en evenwichtig integriteitssysteem). Als een dergelijke afstemming niet mogelijk is omdat de partijen op deze verschillende niveaus te verschillende gevoeligheden en doeleinden hebben , is het ook niet verantwoord om uitwisselingen van dergelijke gevoelige en complexe gegevens aan hen toe te vertrouwen.
22. Voor zover het project doorgang zou vinden, lijkt een (grotere) centralisatie van de verwerking (inclusief bewaring) van de persoonsgegevens meer garanties te bieden. De VTC beschouwt de verspreide bewaring van dergelijke gevoelige gegevens over een potentieel zeer groot aantal Vlaamse instanties als één van de vele cruciale pijnpunten.

¹ Kamer, 2022-2023, doc 3152/001, 8 februari 2023, wetsontwerp betreffende de gemeentelijke bestuurlijke handhaving, de instelling van een gemeentelijk integriteitsonderzoek en houdende oprichting van een Directie Integriteitsbeoordeling voor Openbare Besturen

² In het advies van de Gegevensbeschermingsautoriteit bij het wetsontwerp wordt ook het begrip “ernstige criminaliteit” besproken.

2. Kwaliteit van de regelgevende grondslag

23. De memorie van toelichting verduidelijkt de Vlaamse bevoegdheid (onderlijning VTC):

“De algemene bevoegdheid inzake openbare orde is dus federaal, ook de verregaande bevoegdheden van de burgemeester m.b.t. deze materie vinden hun grondslag in federale wetten (de strafwetten, de Nieuwe Gemeentewet, de Wet op het Politieambt, de Drugswet, de GAS-wet enz.).

*Vlaanderen heeft inzake openbare orde eerder ondersteunende bevoegdheden. Zo kan het gewest de maatschappelijke veiligheid bevorderen op het vlak van onder meer leefmilieu, ruimtelijke ordening en stads- en streekvervoer, op het vlak van veiligheid *sensu stricto* heeft het slechts beperkte bevoegdheden, in de zin dat het schorsen, intrekken en weigeren van bv. vergunningen binnen de Vlaamse materiële bevoegdheid valt en geregeld kan worden zonder een beroep te doen op impliciete bevoegdheden. Een regeling hierover in het kader van de bestrijding van georganiseerde misdaad kan op een algemeen niveau zonder dat het nodig is ieder inhoudelijk decreet aan te passen.*

[...]

Het schorsen van een door een Vlaamse administratieve rechtshandeling verleend recht op basis van een integriteitsonderzoek is een materie die nauw is verbonden met aan het Vlaamse Gewest toegewezen bevoegdheden.

[...]

De Vlaamse overheid kan op die wijze via haar eigen bevoegdheden de doelstellingen van de federale overheid op het vlak van de openbare veiligheid en de openbare orde ondersteunen. Daarvoor hoeft geen beroep te worden gedaan op artikel 10 BWHI.

Door een beroep te doen op het federale DIOB-bureau (cfr. supra) voor de behandeling van de adviesaanvragen wordt onderstreept dat het om een en dezelfde doelstelling gaat. De doelstelling qua veiligheid wordt ondersteund door een uitbreiding van de mogelijkheid tot ingrijpen via de regionale vergunningsstelsels e.a. wanneer er criminele ondermijning dreigt. [...]”

24. Specifiek over informatie-uitwisseling stelt de toelichting het volgende (onderlijning VTC):

“Wat de informatie-uitwisseling betreft, kan Vlaanderen dit regelen voor alle informatie die op Vlaams niveau wordt verzameld. Vlaanderen kan opleggen welke Vlaamse diensten informatie moeten delen, wie toegang krijgt tot deze informatie (zowel binnen de Vlaamse overheid als daarbuiten), wie deze informatie mag verwerken en dergelijke meer. Hierbij moet vanzelfsprekend rekening worden gehouden met privacywetgeving en AVG.

Vlaanderen kan voor de Vlaamse overheid ook bij decreet bepalen welke onderdelen van de Vlaamse overheid informatie van andere overheden mogen verwerken. Vlaanderen kan hetzelfde bepalen t.a.v. de lokale besturen. Vlaanderen kan bij decreet echter niet bepalen dat zij toegang moet krijgen tot de informatie van andere overheden (politie, gerechtelijke, federale fiscale info,...), noch dat die andere overheden deze informatie moeten verstrekken, noch de modaliteiten waaronder die informatie wordt/moet worden verstrekt, want dat kunnen alleen die andere overheden toestaan (bij wet, decreet ...).

Het is dus duidelijk dat de hele problematiek van de bestuurlijke handhaving van georganiseerde criminaliteit en de informatiedeling die daarbij noodzakelijk is niet op één bestuursniveau kan worden opgelost, maar dat elk bestuursniveau binnen de eigen bevoegdheden een regeling zal moeten uitwerken. Zowel Vlaanderen (of de andere deelstaten) als de federale overheid kunnen hiervoor binnen de eigen bevoegdheden een DIOB oprichten, al is het ook mogelijk om één interfederaal DIOB op te richten bij samenwerkingsakkoord. Vlaanderen wil in eerste instantie via een samenwerkingsakkoord aansluiten bij de federale DIOB, maar de Vlaamse regering krijgt bij dit decreet ook de bevoegdheid om zelf een eigen DIOB op te richten indien de andere overheden geen samenwerkingsakkoord hierover zouden willen uitwerken.

Een integriteitsbeoordeling louter op basis van Vlaamse informatie zal onvolledig zijn, maar ook een integriteitsbeoordeling op basis van louter federale informatie zal de nodige hiaten vertonen.

Het systeem staat of valt met een goede informatiedeling en hiervoor moeten dus de nodige samenwerkingsakkoorden en protocollen worden afgesloten."

25. 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.
26. De toelichting geeft expliciet aan op grond van welke rechtvaardigingsgrond in de AVG de verwerking van persoonsgegevens zal plaatsvinden, namelijk het uitvoeren van een taak van openbaar belang zoals bedoeld in artikel 6, e) van de AVG.
27. De VTC wenst in herinnering te brengen dat elke overheidsinmenging in de bescherming van de persoonlijke levenssfeer zoals gewaarborgd door artikel 8 van het EVRM³, 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 elementen⁴ van de met de overheidsinmenging gepaard gaande verwerkingen van persoonsgegevens omschreven zijn.⁵
28. Voor verwerkingen op basis van artikel 6, lid 1, e), AVG⁶, 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.
29. 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

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, transparence 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;"

de betrokkene behoorlijk en transparant is, zal het ontbreken van deze elementen zwaardere transparantiemaatregelen vragen. Er zal immers niet naar wetgeving waarin de verwerking uitdrukkelijk geregeld is, kunnen verwezen worden.

30. 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.
31. 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, De VTC verwijst naar de rechtspraak van het Grondwettelijk Hof inzake delegatie door de wetgever⁷)
32. De VTC wijst erop dat er ook sprake is van persoonsgegevens als bedoeld in artikel 10 AVG, namelijk gegevens over namelijk de gegevens betreffende strafbare feiten en (mogelijk) ook artikel 9, AVG.
33. 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.
34. Artikel 21 legt de volgende maatregel op wat het unieke bestand betreft dat elke gemeente moet bijhouden: transparantie wat de geraadpleegde gegevensbronnen betreft:

*“Art. 21. Elk openbaar bestuur houdt de lijst bij van de rechtspersonen of natuurlijke personen, instanties, autoriteiten of diensten waarvan de gegevens verwerkt in het kader van het onderzoek, afkomstig zijn, evenals van de geraadpleegde gegevensbanken.
Deze lijst wordt ter beschikking gehouden van de bevoegde gegevensbeschermingsautoriteit voor de verwerking van persoonsgegevens.”*

35. Artikel 22 legt maatregelen op aan zowel de openbare besturen als het DIOB (onderlijning VTC):

“Art. 22. [...]

Bij de verwerking van deze persoonsgegevens, zijn de volgende garanties met betrekking tot de bescherming van persoonsgegevens van toepassing:

1° de categorieën van personen die toegang hebben tot de persoonsgegevens worden door de verwerkingsverantwoordelijke of, in voorkomend geval, door de verwerker aangewezen, met een beschrijving van hun functie bij verwerking van de betrokken gegevens;

2° de lijst van categorieën van personen, vermeld in 1°, wordt door de verwerkingsverantwoordelijke of, in voorkomend geval, de verwerker ter beschikking van de gegevensbeschermingsautoriteit gesteld;

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., GwH nr. 26/2023, 16 februari 2023, overw. B.74.1.

3° de aangewezen personen zijn op grond van een wettelijke of reglementaire verplichting of een gelijkwaardige contractuele bepaling verplicht om het vertrouwelijke karakter van de bedoelde gegevens te respecteren;

4° er worden passende technische en organisatorische maatregelen genomen om persoonsgegevens te beveiligen tegen accidentele of ongeoorloofde vernietiging, tegen toevallig verlies en tegen wijziging of andere ongeoorloofde verwerking van dergelijke gegevens;

5° er worden logbestanden aangelegd voor het beheersysteem en ten minste voor de volgende handelingen: verzameling, wijziging, raadpleging, communicatie, inclusief overdrachten, interconnectie en verwijdering.

Deze logbestanden worden gebruikt om vast te stellen:

a) de reden, de datum en het tijdstip van deze handelingen;

b) de categorieën personen die de persoonsgegevens hebben geraadpleegd en de identiteit van de persoon die de gegevens heeft bekeken;

c) de systemen die deze gegevens hebben meegedeeld;

d) de categorieën ontvangers van de persoonsgegevens en, indien mogelijk, de identiteit van de ontvangers van de gegevens.

De logbestanden worden drie jaar bewaard.

De bevoegde functionarissen voor gegevensbescherming zien erop toe dat dit beleid wordt gevolgd.

De Vlaamse regering kan aanvullende garanties bieden.”

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

3. Doelbinding

37. 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).

38. De volgende doeleinden worden in het Ontwerp vermeld:

- voor zowel de openbare besturen als het DIOB:

“Art. 22. Het openbaar bestuur en de DIOB verwerken de persoonsgegevens en informatie met betrekking tot natuurlijke en rechtspersonen, die worden verzameld in het kader van de toepassing van artikel 3 uitsluitend om tot een gemotiveerde integriteitsbeoordeling te komen. Het kan daartoe het rijksregisternummer en het unieke ondernemingsnummer gebruiken.”

- voor het bestand dat door elk openbaar bestuur wordt bijgehouden: dat het bedoeld is om het beheer van de integriteitsonderzoeken te verzekeren (artikel 20, §1).

39. De VTC is van oordeel dat deze doeleinden welbepaald, uitdrukkelijk omschreven en gerechtvaardigd zijn.

40. Wat de doelbinding betreft stelt artikel 8 volgende beperking:

“§ 4. Het bevoegde openbaar bestuur en de DIOB kunnen de gegevens die met toepassing van §§ 1 tot en met 3 werden verkregen enkel verwerken voor de finaliteit waarvoor de vraag werd gesteld.”

41. In de toelichting bij artikel 8 van het Ontwerp wordt volgende uitleg gegeven:

“De gegevens die hierdoor werden verkregen van deze diensten kunnen slechts worden aangewend voor de finaliteit waarvoor de vraag werd gesteld, met name het opstellen van een integriteitsbeoordeling. De mededeling, aanwending en verwerking van deze gegevens gebeurt overeenkomstig de wetgeving die op de betrokken dienst van toepassing is.”

42. In verband met de doelbinding heeft de VTC een bedenking met volgende paragraaf van artikel 8:

“§ 3. Het bevoegde openbaar bestuur en de DIOB kunnen bij de uitvoering van het integriteitsonderzoek gebruikmaken van alle publiek toegankelijke informatiebronnen.”

43. De toelichting zegt hier het volgende over:

“Het openbaar bestuur en de DIOB kunnen bij het opstellen van het advies gebruikmaken van alle publiek toegankelijke informatiebronnen. Hierbij wordt bv. gedacht aan informatie die via sociale media publiek gedeeld wordt.”

44. In tegenstelling tot wat op het eerste gezicht uit de tekst van het Ontwerp blijkt, namelijk dat het opvragen van informatie beperkt blijft tot concrete cases, wordt op basis van de toelichting (artikel 11) duidelijk dat er effectief gedacht wordt aan **datamining en profilering** (deze termen komen op zich niet voor in het Ontwerp of de toelichting):

“De verdere concrete invulling en bestaffing van de DIOB wordt overgelaten aan de Vlaamse regering. De personeelsprofielen die dienstig kunnen zijn om deze dienst te bestafferen zijn bv.:

- *Dataminers*
- *Profilers*
- *Juristen*
- *Criminologen*
- *Sociologen”*

45. De VTC wijst erop dat, voor wat persoonsgegevens betreft, het publiek maken van informatie, bijvoorbeeld op sociale media niet betekent dat de doelbinding niet moet gerespecteerd worden, aangezien het publiek maken in een welbepaalde context gebeurt.

46. Het feit dat het hier niet duidelijk is of het al dan niet om persoonsgegevens gaat, wijst er op dat deze bepaling een onvoldoende wettelijke basis biedt om persoonsgegevens op via datamining en profilering te verzamelen of te verrijken.

47. Bovendien waarschuwt de VTC ervoor dat, zo er gedacht zou worden aan *datascrapen*, waarbij een overheid haar eigen en andere burgers kan volgen op het internet, dit een instrument is dat niet zonder de gepaste strenge waarborgen kan ingezet worden in een democratische samenleving en rechtsstaat. Het Ontwerp volstaat daarvoor op dit moment niet.

48. Het aantal betrokken en persoonsgegevens die via datascrapen/datamining zouden worden verwerkt zullen veel ruimer zijn dan waarvoor hier een decretale basis wordt gecreëerd (zie infra).

4. Verantwoordelijkheid

49. 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.

50. De verwerkingsverantwoordelijken worden aangeduid in artikel 7 van het Ontwerp:

“Art. 7. Het integriteitsonderzoek wordt hetzij uitgevoerd door het bevoegde bestuur, hetzij door de DIOB.

Het onderzoek naar de integriteit wordt gevoerd onder het gezag en de verantwoordelijkheid van het openbaar bestuur of, in voorkomend geval, de DIOB. Zij zijn verantwoordelijk voor de verwerking van de persoonsgegevens die bij de integriteitsbeoordeling worden betrokken [...]”

51. Ook artikel 24 van het Ontwerp behandelt de verantwoordelijkheid, maar meer operationeel (zie onder beveiliging):

“Art. 24. De directeur van de DIOB en het orgaan van het openbaar bestuur dat bevoegd is om een beslissing zoals vermeld in artikel 3 te nemen zijn de verwerkingsverantwoordelijke voor alle persoonsgegevens en informatie die in het kader van een integriteitsonderzoek worden verzameld. [...]”

52. Het is nog niet duidelijk waar het DIOB zich zal situeren. Artikel 11 bepaalt dat er ofwel een samenwerkingsakkoord wordt gesloten ofwel een eigen DIOB wordt opgericht. De toelichting zegt hierover het volgende:

“Indien een samenwerkingsakkoord niet mogelijk is wordt op Vlaams niveau een Dienst Integriteitsbeoordeling voor Openbare Besturen opgericht. Deze dienst zal zich situeren binnen het Agentschap Justitie en Handhaving en omkleed worden met de nodige garanties m.b.t. onafhankelijkheid en integriteit. Indien blijkt dat er vanuit de federale overheid en/of de andere deelstaten gelijkaardige initiatieven genomen worden, kan deze dienst ook ingekanteld worden in een interfederale organisatie.”

53. De VTC behandelt de adviesvraag verder vanuit de aanname dat er een Vlaams DIOB wordt opgericht.

54. Wat de openbare besturen betreft, wordt de verantwoordelijkheid verder gespecificeerd in artikel 20 van het Ontwerp:

“Art. 20. § 1. Elk openbaar bestuur houdt één enkel bestand bij van de natuurlijke personen of rechtspersonen die het voorwerp uitmaken of hebben uitgemaakt van een integriteitsonderzoek. Afhankelijk van het betrokken bestuursniveau is de leidend ambtenaar van de dienst die het integriteitsonderzoek heeft gevoerd, de bestendige deputatie of de algemeen directeur, verantwoordelijk voor de verwerking van dit bestand. [...]”

55. De AVG als ook het e-govdecreet legt de aanstelling van een functionaris voor de gegevensbescherming (artikel 37 AVG)⁸ op. Gezien de verschillende gegevensstromen (zie verder), zou de rol (niet de aanstelling) van de **functionaris** voor de gegevensbescherming best verankerd worden in de regelgeving voor wat de hier bedoelde verwerkingen betreft zodat verzekerd wordt dat die telkens een advies kan geven.

56. De decreetgever, de Vlaamse Regering en de verwerkingsverantwoordelijken moeten nagaan of het uitvoeren van een **gegevensbeschermingseffectenbeoordeling** (GEB - artikel 35 AVG)⁹ voor de verschillende gegevensstromen al dan niet noodzakelijk is.

⁸ Zie:

- Info op website van de federale Gegevensbeschermingsautoriteit:

<https://www.gegevensbeschermingsautoriteit.be/professioneel/avg/functionaris-voor-gegevensbescherming>

- Aanbeveling nr. 04/2017 van de Commissie voor de bescherming van de persoonlijke levenssfeer (hierna “CBPL”)

(<https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-04-2017.pdf>)

- Richtlijnen Groep 29 (WP 243) (http://vtc.corve.be/docs/WP29_DPO.pdf)

⁹ 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>)

57. De VTC meent alvast dat het uitvoeren van een GEB verplicht zal zijn gelet op **de lijst van de VTC**¹⁰ met verwerkingen waarvoor een Vlaamse bestuursinstantie een GEB moet uitvoeren conform artikel 35.4 van de AVG. De VTC verwijst in dit kader naar de volgende punten:

3) wanneer er op systematische wijze bijzondere categorieën van persoonsgegevens in de zin van artikel 9 van de AVG, evenals persoonsgegevens met betrekking tot strafrechtelijke veroordelingen of strafbare feiten zoals omschreven in artikel 10 van de AVG of gegevens van zeer persoonlijke aard (zoals financiële gegevens en gegevens over inkomen en vermogen, werkloosheid, betrokkenheid van jeugdzorg of maatschappelijk werk, gegevens omtrent huishoudelijke en privé-activiteiten, locatiegegevens) worden uitgewisseld tussen meerdere verwerkingsverantwoordelijken. GEVOELIGE GEGEVENS [criteria 4 en 5]¹²;

6) wanneer er sprake is van zwarte lijsten: verwerkingen waarbij persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten, gegevens over onrechtmatig of hinderlijk gedrag of gegevens over slecht betalingsgedrag worden verwerkt met het oogmerk om besluiten mogelijk te maken waaraan voor de betrokkenen rechtsgevolgen zijn verbonden of die hen anderszins in aanmerkelijke mate treffen (zwarte lijsten of waarschuwingslijsten, zoals bijvoorbeeld zwarte lijsten die betrekking hebben op onrechtmatig gedrag van werknemers, bijvoorbeeld in de zorg ,of van hinderlijk gedrag van huurders van sociale woningen. ZWARTE LIJSTEN [criteria 4, 6, 7, 8];

15) wanneer er op grote schaal gegevens ingezameld worden bij derden¹⁹ teneinde de economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen van natuurlijke personen te analyseren of voorspellen; INZAMELEN OM TE PROFILEREN [criteria 1 en 5]

16) wanneer er sprake is van grootschalige verwerkingen van persoonsgegevens waarbij op systematische wijze via geautomatiseerde verwerking gedrag van natuurlijke personen geobserveerd, verzameld, vastgelegd of beïnvloed wordt, inclusief voor overheidsadvertentie- , overheidsmarketing of overheidsdienstverleningsdoeleinden. OBSERVATIE OM TE PROFILEREN [criteria 1 en 5];

17) wanneer er sprake is van matching of samenvoeging van datasets, bijvoorbeeld datasets die voortkomen uit twee of meer gegevensverwerkingen die voor verschillende doeleinden zijn uitgevoerd en/of door verschillende verwerkingsverantwoordelijken zijn uitgevoerd op een wijze die de redelijke verwachtingen van de betrokkene zou overschrijden²³. BIG DATA ANALYTICS (onder andere) [criterium 6].

Bij deze verwerking moet er een gegevensbeschermingseffectbeoordeling worden uitgevoerd als aan al de volgende voorwaarden is voldaan: (a) de koppeling of de verdere of latere verwerking is grootschalig; (b) minstens sommige data worden verwerkt voor doeleinden die verschillen van die van de oorspronkelijke verwerking; (c) er worden algoritmes gebruikt die niet begrijpelijk zijn voor de betrokkenen;

19) wanneer er sprake is van grootschalige verwerkingen van (bijzondere) persoonsgegevens en/of stelselmatige monitoring in het kader van fraudebestrijding. FRAUDEBESTRIJDING [criteria 3, 4, 5 (en 9)]

11) wanneer persoonsgegevens ingezameld worden bij andere Vlaamse of andere bestuursinstanties of derden om vervolgens in aanmerking te worden genomen bij de beslissing om een welbepaalde dienstverlening met een natuurlijke persoon te weigeren of stop te zetten. GEEN DIENSTVERLENING [criteria 6 en 9];

58. 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 verplicht¹¹.

¹⁰ Beslissing VTC nr. O/2020/01 van 14 januari 2020 betreffende Aannee van de lijst met verwerkingen waarvoor een Gegevensbeschermingseffectbeoordeling dient te worden uitgevoerd conform artikel 35.4 van de Algemene Verordening Gegevensbescherming door Vlaamse bestuursinstanties
https://overheid.vlaanderen.be/sites/default/files/media/VTC/O_2020_01_DPIA_lijsten_v1_voor_web.pdf

¹¹ 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."

5. Minimale gegevensverwerking

59. 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.
60. De **categorieën betrokkenen** zijn:
- (natuurlijke) personen voor wie er ernstige aanwijzingen zijn dat ze rechtstreeks of onrechtstreeks deelnemer zijn aan ernstige sanctioneerbare feiten die verband kunnen houden met een toegekend of toe te kennen recht dat via een Vlaamse administratieve bestuurshandeling wordt verleend en dat de betrokkene misbruikt, zal misbruiken of laat misbruiken;
 - een derde die tegenover de persoon hiervoor vermeld de acto of de iure een dominante positie heeft en sanctioneerbare feiten heeft gepleegd (artikel 5);
 - de vermoedelijke lastgever van de eerst vermelde betrokkene (stromanconstructie);
 - in de mate dat datamining en profilering worden ingezet: potentieel elke burger.
61. “Sanctioneerbare feiten” wordt gedefinieerd als feiten waarvoor een strafrechtelijke of bestuurlijke sanctie kan worden opgelegd. In de toelichting wordt aangegeven dat er wat “sanctioneerbare feiten”, betreft, niet wordt gewerkt met een limitatieve lijst. Er worden wel voorbeelden gegeven: terrorisme, witwassen en heling, georganiseerde misdaad, illegale handel in drugs- en dopingproducten, illegale wapenhandel, mensensmokkel en -handel, exploitatie van prostitutie, hormonenhandel, illegale handel in menselijke organen en weefsels, ernstige fiscale fraude, ernstige sociale fraude, verduistering en corruptie, ernstige milieucriminaliteit, valsmunterij, namaak van goederen, diefstal, afpersing, informaticabedrog, ernstige voedsel- en geneesmiddelencriminaliteit.
62. De VTC wijst op de sterke tegenstrijdigheid tussen de gegeven voorbeelden (die allemaal beschouwd kunnen worden als ernstige criminaliteit) en de tekst van het Ontwerp (die toepassing op verhoudingsgewijs triviale feiten toelaat). Op basis van de voorbeelden lijkt de verwijzing naar een bestuurlijke sanctie te kunnen worden weggelaten. Dit zou de groep betrokkenen dan verduidelijken en sterk beperken, conform het principe van minimale gegevensverwerking. Als het toch nodig zou zijn die term te behouden, dan beveelt de VTC aan te verantwoorden waarom een substantiële inbreuk op de gegevensbescherming verantwoord kan worden bij louter bestuurlijk gesanctioneerde feiten.
63. Er wordt ook geen limitatieve lijst van bestuurshandelingen opgenomen. In de toelichting worden wel weer voorbeelden gegeven: erkenningen, toelatingen, toestemmingen, subsidies, machtigingen, vergunningen, concessies, licenties, attesten, ontheffingen, vrijstellingen, beroepskaarten. Dit is opnieuw heel ruim, en bovendien spreekt de tekst van het Ontwerp nergens over ‘bestuurshandelingen’, maar over “een recht dat op basis van Vlaamse regelgeving via een administratieve rechtshandeling wordt verleend”. Elk dergelijk recht kan aanleiding geven tot een mogelijke integriteitstoets, hetgeen een zeer open draagwijdte is.
64. Het moeilijkst te interpreteren criterium is de aanwezigheid van “ernstige aanwijzingen”. Dit heeft zowel betrekking op het bepalen van de categorie betrokkenen als op het bepalen welke persoonsgegevens zullen verwerkt worden.
65. Er wordt in dit kader wel gesteld dat een eerdere loutere strafrechtelijke of bestuurlijke sanctionering niet volstaat, maar er moeten concrete aanwijzingen zijn dat het recht waarvan sprake misbruikt wordt, of zal worden.
- “Op die manier wordt het risico dat de sociale integratie bemoeilijkt zou kunnen worden uitgesloten. Enkel wanneer er aanwijzingen zijn dat het recht wordt misbruikt voor criminele doeleinden, m.a.w. als er indicaties zijn dat er van sociale integratie geen sprake is, kan dit leiden tot het ontzeggen van het recht.”*
66. Verder wordt er in artikel 5 van het Ontwerp verduidelijkt dat er uit de gemotiveerde integriteitsbeoordeling moet blijken dat er een aanwijsbaar ernstig risico, gebaseerd op feiten, omstandigheden of redelijke vermoedens, bestaat dat het recht, toegekend via de administratieve rechtshandeling, wordt misbruikt of zal worden misbruikt
67. Artikel 19 van het Ontwerp somt de **categorieën van persoonsgegevens** op:

“Art. 19. Bij het uitvoeren van een integriteitsonderzoek, het opstellen van een advies voor de integriteitsbeoordeling en de integriteitsbeoordeling is de verwerking van persoonsgegevens beperkt tot de volgende categorieën:

- a) De naam, voornamen, het adres, de geboortedatum, de geboorteplaats, de woon- en verblijfplaats of de plaats van vestiging van de betrokkene;
- b) De naam, voornamen, het adres, de geboortedatum, de geboorteplaats, de woon- en verblijfplaats of de plaats van vestiging van degene door wie de betrokkene zich laat vertegenwoordigen;
- c) Het Rijksregisternummer van de in a) en b) bedoelde personen;
- d) Het nummer van een officieel identificatiedocument, uitgereikt door een overheid;
- e) Financiële, administratiefrechtelijke en gerechtelijke gegevens.”

68. Artikel 20 voegt daar nog aan toe voor het bestand dat bijgehouden wordt door elk openbaar bestuur (zie hiervoor):

“§ 2. Het bestand bevat, behalve de in artikel 19 vermelde persoonsgegevens, nog de volgende informatie:

1° de naam, maatschappelijke zetel en het ondernemingsnummer van de rechtspersonen die het voorwerp uitmaken van een integriteitsonderzoek;

2° de gegevens waarop de beslissing als vermeld in artikel 3, is gesteund ;

3° de met redenen omklede beslissing van het openbaar bestuur met betrekking tot de beslissing als vermeld in artikel 3. “

69. De VTC wijst er op dat de categorieën heel ruim zijn en dat mogelijk (ook) volgende persoonsgegevens worden verwerkt:

- het begunstigd zijn van een recht en welk recht dat is;
- het aanwijsbaar ernstig risico op misbruik van het recht;
- de ernst van de feiten;
- de relatie van de houder of aanvrager van het recht tot de feiten;
- andere elementen uit de adviesvraag aan de DIOB
- andere elementen uit het integriteitsonderzoek (door openbaar bestuur of DIOB);
- andere persoonsgegevens in de gemotiveerde integriteitsbeoordeling (door openbaar bestuur of DIOB);
- andere persoonsgegevens in het advies van het DIOB;
- audio- en beeldopnames, ...

70. De VTC kan gezien de ruime en mogelijk onvolledige omschrijving geen uitspraak doen over de proportionaliteit van de gegevensverwerking op dit punt.

71. Wat de **ontvangers** betreft, dit zijn:

- **voor het dossier dat door een openbaar bestuur of de DIOB wordt aangelegd om tot een integriteitsbeoordeling te komen** (artikel 23):

“Dit dossier is enkel toegankelijk of kan enkel geraadpleegd worden door de leden die door de directeur van de DIOB of het orgaan van het openbaar bestuur dat bevoegd is om een beslissing zoals vermeld in artikel 3 te nemen, worden aangewezen op basis van de nood om er kennis van te nemen.”

72. De VTC leest dat de personeelsleden geen toegang hebben tot het dossier en dat de toegang dus zeer beperkt is, wat zeer positief is. Anderzijds wordt de personeelsleden wel een geheimhoudingsplicht opgelegd. De VTC gaat ervan uit dat een gelijkaardige bepaling voor de personeelsleden ontbreekt. Het resultaat van dat onderzoek zal in elk geval in concreto moeten worden gemotiveerd en dan zal er toch informatie vrijkomen. **Ze adviseert om dit te verduidelijken.**

- een hele reeks federale en gewestelijke overheidsdiensten aan wie het openbaar bestuur en de DIOB verzoeken tot mededeling van persoonsgegevens en informatie kunnen richten (artikel 8, §1 van het Ontwerp) of moeten doorgeven (artikel 18, §2):

73. De VTC merkt op dat de gegevens uit een integriteitsonderzoek hierdoor wellicht niet louter voor de doeleinden van het integriteitsonderzoek zullen worden gebruikt, aangezien ze worden doorgegeven aan ontvangers die een ander en veel breder mandaat hebben. De resultaten van een integriteitsonderzoek kunnen dus voor zeer afwijkende doeleinden worden gebruikt, wat de potentiële impact en gevoeligheid van het systeem sterkt vergroot.
74. De VTC herinnert eraan dat bij het opvragen van gegevens ook (persoons)gegevens worden meegegeven. De vragen moeten volgens artikel 8, §1, tweede lid trouwens ook gemotiveerd zijn, wat ook informatie over de betrokkenen zal inhouden.
75. In het laatste punt p) staat vermeld: elke dienst door de Vlaamse Regering aangeduid. Hiervoor adviseert de VTC dat er **minstens criteria** worden bepaald (zie hiervoor over de delegatiebevoegdheid).
76. Voor zover de vermelde diensten behoren tot de Vlaamse Overheid moeten ze op de informatievraag ingaan volgens artikel 8, §1, derde lid.
77. De VTC wijst erop dat de ontvanger van een verzoek gehouden is aan de principes van de AVG en de wettigheid en proportionaliteit van de vraag zal moeten onderzoeken.
78. De toelichting vermeldt hoe de raadpleging van de Vlaamse Diensten zal gebeuren:

“De ontsluiting van de gegevens bij deze instanties kan bevoegdheidsmatig relatief eenvoudig gerealiseerd worden voor de diensten op het niveau van de Vlaamse overheid, zoals bv. inspectiediensten, beboetingsinstanties en diensten die bevoegd zijn inzake het verlenen van de zaken vermeld in artikel 3. Er zal een koppeling worden gemaakt met het Vlaams bestuurlijk sanctieregister¹², dat zijn rechtsgrond heeft in het Kaderdecreet Bestuurlijke Handhaving van 22 maart 2019 en dat momenteel uitgebouwd wordt, evenals met een toekomstig Vlaams bestuurlijk maatregelenregister. Deze Vlaamse diensten zijn verplicht om aan een informatieverzoek door een openbaar bestuur te voldoen, zij moeten de gevraagde informatie medelen (rekening houdend met de voorwaarden in paragraaf 4).”

79. Wat het verkrijgen van informatie van de federale diensten betreft, geeft de toelichting volgende uitleg:

“Belangrijker dan de ontsluiting van informatie van de eigen Vlaamse diensten is in deze context evenwel de informatie die zich op federaal niveau bevindt. De toegang tot bepaalde federale informatie is noodzakelijk om een goed onderbouwde, volledige integriteitsbeoordeling te kunnen

¹² De VTC herinnert aan wat ze gesteld heeft in haar advies VTC/A/W/2022/082 in verband met het bestuurlijk sanctieregister (vet VTC):

“Hiermee wordt meteen de basis gelegd voor het uitwerken van een toekomstige Vlaamse Kruispuntbank Handhaving, die het mogelijk zal maken om handavingsinformatie, opgenomen in het Digitaal Archief, het bestuurlijk sanctieregister en het maatregelenregister, te kruisen met handavingsinformatie van andere bestuursniveau's en andere (niet aan eigenlijke handavingsprocessen gerelateerde) overheidsinformatie, zoals gegevens over vergunningen, subsidieaanvragen e.d.”

22. In eerste instantie uit de VTC hier haar bezorgdheid dat er een gegevensuitwisseling (“kruisen”) mogelijk wordt gemaakt waar **te weinig beperkingen** aan worden gesteld. Verder in de tekst (minstens waar het de registers betreft) wordt er opgedragen aan de Vlaamse Regering om dit verder uit te werken, maar hier ontbreken verwijzingen naar beperkingen van noodzakelijkheid en evenredigheid. Zo lijkt de gegevensuitwisseling beleidsdomeinoverschrijdend te zijn wat tegen het **specialiteitsbeginsel van de overheidsbevoegdheid** lijkt in te gaan. Er is ook sprake van andere bestuursniveaus. De Memorie van Toelichting verwijst naar het Regeerakkoord 2019-2024 waarin het volgende staat:

“Het bestuurlijk sanctieregister wordt uitgerold als een Kruispuntbank Handhaving waar de relevante actoren inzake bestuurlijke politie toegang toe hebben met inachtneming van de wetgeving inzake gegevensbescherming.”

maken. Belangrijke strafrechtelijke, gerechtelijke en financiële informatie wordt bijgehouden op het federale niveau. Er wordt hier o.a. gedacht aan informatie die in handen is van de geïntegreerde politie, het centraal strafregister, ECRIS (European Criminal Records Information System), de inlichtingen- en veiligheidsdiensten, de cel voor financiële informatieverwerking, de Algemene Administraties van de Fiscaliteit, de Bijzondere Belastinginspectie en de Douane en Accijnzen van de FOD Financiën, de sociale inspectiediensten, de economische inspectie, de Dienst Vreemdelingenzaken, het Federaal Agentschap voor de Veiligheid van de Voedselketen en het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten.
Om toegang tot deze informatie te krijgen moeten er de nodige samenwerkingsakkoorden en protocollen met de federale overheid afgesloten worden."

80. Artikel 8, §5 bepaalt het volgende:

"§ 5. De Vlaamse regering sluit een samenwerkingsakkoord tussen de Staat, de gemeenschappen en de gewesten, bedoeld bij artikel 92bis, § 1, van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen, af met betrekking tot de mededeling van persoonsgegevens en informatie door
a) de instanties, vermeld in § 1, a) tot en met k);
b) de gerechtelijke overheden, vermeld in § 2."

- **gerechtelijke overheden aan wie het openbaar bestuur en de DIOB verzoeken tot mededeling van persoonsgegevens en informatie kunnen richten** (artikel 8, §2 van het Ontwerp)
- **de bevoegde medewerkers van het andere bevoegde openbaar bestuur** (artikel 3, § 3):

"§ 3. Een openbaar bestuur kan de beslissingen, vermeld in de §§ 1 en 2 enkel nemen met betrekking tot de rechten die het door zijn eigen administratieve rechtshandelingen kan verlenen of heeft verleend.

Als uit het integriteitsonderzoek overeenkomstig hoofdstuk 3, blijkt dat er een beslissing nodig is van een ander bevoegd openbaar bestuur, kan het openbare bestuur aan het andere openbaar bestuur vragen om de beslissingen vermeld in de §§ 1 en 2 te nemen. In dat geval maakt het openbaar bestuur de integriteitsbeoordeling, de elementen uit het integriteitsonderzoek waarop de integriteitsbeoordeling is gesteund en, desgevallend, het advies van het DIOB waarop het is gesteund over aan het bevoegde openbaar bestuur. "

- **buitenlandse en binnenlandse equivalente instellingen** (artikel 15):

"§ 2. De DIOB kan met deze instellingen en netwerken samenwerken overeenkomstig de verdragsrechtelijke, supranationale, wettelijke en decretale regels op het gebied van:

- 1° de uitwisseling van informatie in het kader van de adviesverlening over integriteitsbeoordelingen ;*
- 2° de uitwisseling van goede praktijken over het uitbrengen van integriteitsbeoordelingen;*
- 3° thematische vorming over integriteitsbeoordelingen .*

§ 3. De uitwisseling van operationele informatie in het kader van de adviesbehandeling is slechts mogelijk voor de landen en onder de voorwaarden die worden bepaald door de Vlaamse regering."

- **nutsbedrijven en distributienetbeheerders** (artikel 16):

"Art. 16. §1. De DIOB en een openbaar bestuur kunnen met de nutsbedrijven en distributienetbeheerders een protocol afsluiten om nuttige gegevens te kunnen inwinnen in het kader van het uitvoeren van integriteitsbeoordelingen. Deze gegevens kunnen enkel ingewonnen worden voor zover dit noodzakelijk is voor het betreffende integriteitsonderzoek.
De nutsbedrijven of de distributienetbeheerders moeten de gegevens binnen een termijn van 14 dagen na ontvangst van de aanvraag bezorgen."

81. Met de tweede paragraaf van artikel 16 lijkt een voldoende wettelijke basis te worden gegeven Het betreft geen systematische mededeling van persoonsgegevens gezien de vermelding “voor het betreffende integriteitsonderzoek”. Het is evenwel positief dat in een protocol afspraken en waarborgen worden opgenomen.
82. In het Ontwerp wordt specifiek de **mededeling** geregeld van gegevens. De VTC wijst erop dat er rekening zal moeten gehouden worden met artikel 8 van het Vlaams e-govdecreet van 18 juli 2008, dat aan Vlaamse instanties de verplichting oplegt om protocollen af te sluiten voor de mededeling van persoonsgegevens aan andere overheden. Dit geldt dus niet alleen voor de mededelingen van de Vlaamse inspectiediensten aan die van de andere Gewesten, maar ook voor de mededelingen door alle andere Vlaamse instanties aan de Vlaamse inspectiediensten (voor zover die niet al gemachtigd werden) en aan de inspectiediensten van de andere Gewesten.
83. Bovendien kunnen bepaalde mededelingen ook onderworpen zijn aan artikel 20 van de WVG of artikel 46 van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid[1] en de artikelen 5 en 8 van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen die een machtigingsvereiste instellen van de minister bevoegd voor Binnenlandse Zaken voor het gebruik van het rijksregisternummer.
84. De VTC wijst erop dat optioneel advies aan haar kan gevraagd worden over een ontwerpprotocol.
85. In de toelichting bij artikel 14 over de adviesverlening door het DIOB wordt volgende uitleg gegeven:

“De haalbaarheid van deze termijn hangt voornamelijk af van de mate waarin er informatiebronnen geraadpleegd kunnen worden. Hoe meer informatiebronnen inschuiven in een nog te ontwikkelen kruispuntbank hoe vlotter en sneller de adviesverlening kan verlopen. De efficiëntie en effectiviteit van het ganse systeem staat of valt met de beschikbaarheid van data. Niet alleen op het Vlaamse niveau moeten hiervoor de nodige afspraken worden gemaakt, maar het is onontbeerlijk dat er ook met het federale niveau de nodige samenwerkingsakkoorden worden gesloten. Zonder toegang tot strafrechtelijke, politionele, fiscale en andere belangrijke gegevens die zich op het federale niveau bevinden, dreigt de integriteitsbeoordeling zijn relevantie te verliezen. Vlaanderen beschikt namelijk maar over een beperkt aantal gegevens die dienstig zijn voor een integriteitsonderzoek, het gaat hier bv. over gegevens m.b.t. administratieve sancties en maatregelen, subsidiedossiers, vergunningenregisters,...”

Als de integriteitsbeoordeling louter gebaseerd wordt op Vlaamse gegevens, kan er t.a.v. de betrokkene een heel verkeerd en vooral onvolledig beeld ontstaan, waardoor er beslissingen genomen worden o.b.v. onvolledige informatie en waardoor de betrokkene bv. in zijn rechten geschonden kan worden.”

86. De VTC merkt op dat het Ontwerp niets bepaalt over een **kruispuntbank** en dat het ook niet duidelijk is of er sprake is van een echte kruispuntbank conform het principe van dienstenintegratie of een gewone databank. Dit heeft gevolgen voor de proportionaliteitsbeoordeling met inbegrip van de bepaling van de bewaartermijn.
87. 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.
88. Wat de **bewaartermijnen** betreft, merkt de VTC op dat die vastgelegd wordt voor het ene bestand dat elke gemeente moet hebben (artikel 20, §2):

“De gegevens van het bestand worden gedurende drie jaar bewaard, te rekenen vanaf de datum waarop het integriteitsonderzoek werd afgerond. Eens deze termijn is verstreken, worden zij hetzij vernietigd, hetzij geanonimiseerd. De gegevens als bedoeld in punt 2 van het tweede lid worden onmiddellijk vernietigd nadat alle beroepsmiddelen uitgeput zijn en de beslissing definitief is.”*

** waarschijnlijk wordt punt 2° van de tweede paragraaf bedoeld: de gegevens waarop de beslissing als vermeld in artikel 3, is gesteund.*

89. Er worden verder bepalingen opgenomen die verder de archivering en vernietiging bepalen:

Het dossier dat door de DIOB wordt aangelegd, wordt na het versturen van het gemotiveerde advies naar de verzoekende overheid onverwijld gearchiveerd door de DIOB (artikel 23, §2).

De gearchiveerde gegevens zijn enkel toegankelijk voor de directeur van de DIOB, op basis van een specifieke motivering in het kader van de verdediging in rechte of een belangrijke missie van openbaar belang en voor de gerechtelijke overheden in het kader van de opsporing en vervolging van misdrijven.

Na de termijn van drie jaar na archivering wordt dit dossier vernietigd, met uitzondering van het aan de verzoekende overheid verzonden gemotiveerde advies, dat na zes jaar wordt vernietigd. De termijnen worden niet gemotiveerd, zodat de VTC ze niet kan beoordelen.

Het dossier dat door een openbaar bestuur wordt aangelegd, wordt door het openbaar bestuur gearchiveerd onmiddellijk nadat het openbaar bestuur een beslissing zoals vermeld in artikel 3 heeft genomen of heeft besloten dat er geen aanleiding is om een dergelijke beslissing te nemen (artikel 23, §3)

De gearchiveerde gegevens zijn enkel toegankelijk voor het orgaan van het openbaar bestuur dat bevoegd is om een beslissing zoals vermeld in artikel 3 te nemen, op basis van een specifieke motivering in het kader van de verdediging in rechte of een belangrijke missie van openbaar belang en voor de gerechtelijke overheden in het kader van de opsporing en vervolging van misdrijven.

Het dossier wordt vernietigd na een termijn van zes jaar na archivering.

90. De VTC heeft bij de archiverings- en vernietigingsbepalingen geen opmerkingen. Zie evenwel ook verder onder beveiliging.

6. Juistheid

91. Persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd (artikel 5, 1, d), AVG).
92. Het Ontwerp bevat geen bepalingen hierover. De VTC beveelt aan om die op te nemen, eventueel door te verwijzen naar bestaande regelingen.

7. Rechten van de betrokkenen en transparantie

93. 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.
94. De VTC is van oordeel dat het aanbevolen is om het Ontwerp aan te vullen met de verplichting om de **vermeldingen** zoals bedoeld in randnummer 81, op te nemen in de communicatie met de burger 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.
95. De eisen die aan het integriteitsonderzoek en de integriteitsbeoordeling worden gesteld (artikel 6 van het Ontwerp) houden ook transparantievereisten in:

“Art. 6. Het integriteitsonderzoek en de integriteitsbeoordeling voldoen aan volgende voorwaarden:

- a) ze mogen **niet discriminatoir** zijn;*
- b) ze zijn duidelijk, ondubbelzinnig en objectief;*
- c) ze gebeuren op een **transparante** wijze.”*

96. Anderzijds worden er ook beperkingen opgelegd qua transparantie. In artikel 9 dat specifiek over de integriteitsbeoordeling gaat, wordt bepaald dat noch het advies van de DIOB, noch de integriteitsbeoordeling van het openbaar bestuur gegevens mogen vermelden waarvan de mededeling schade zou kunnen toebrengen aan bijvoorbeeld de verdediging van de onschendbaarheid van het nationaal grondgebied, de inwendige veiligheid van de Staat, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het geheim van een lopend strafrechtelijk of bestuurlijk opsporingsonderzoek of het geheim van het gerechtelijk onderzoek,...
97. Daarbij wordt als laatste punt 13) ook de bescherming van privacy van derden vernoemd.
98. De VTC neemt er akte van dat het Ontwerp **afwijkingen op de AVG-rechten** invoert:
99. Artikel 25 en 26 van het ontwerp lijken (zonder dat expliciet te vermelden) een beroep te doen op de uitzonderingsmogelijkheid op de rechten van de betrokkenen die artikel 23, AVG, biedt:

“Art. 25. §1. Onverminderd de artikelen 14 en 16 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en in afwijking van de artikelen 14, 15, 16, 17 en 18 van de Verordening (EU) 2016/679 en voor zover artikel 14, § 5, b), c) of d) in het specifiek geval niet kan worden ingeroepen, kunnen de rechten van de betrokkenen worden overgedragen, beperkt of uitgesloten voor zover de toepassing ervan de goede uitvoering van het integriteitsonderzoek en het opstellen van de integriteitsbeoordeling zou schaden.

De in het eerste lid vermelde afwijkingen gelden minstens gedurende de periode waarin de betrokkene het voorwerp uitmaakt van een integriteitsonderzoek of de daarmee verband houdende voorbereidende werkzaamheden uitgevoerd door het openbaar bestuur en maximum tot het ogenblik waarop een beslissing zoals vermeld in artikel 3 wordt genomen.

§ 2. De beperkingen van de rechten van betrokkene, voorzien in dit artikel, doen geen afbreuk aan de specifieke rechten die aan betrokkene zijn toegekend door of krachtens de wet in het kader van bepaalde geschilprocedures of administratieve procedures.

***Art. 26.** Het verzoek om de rechten uit te oefenen zoals bedoeld in de artikelen 14, 15, 16, 17, 18 en 21 van Verordening (EU) 2016/679, met betrekking tot de verwerking van persoonsgegevens door de DIOB en het orgaan van het openbaar bestuur dat bevoegd is om een beslissing zoals vermeld in artikel 3 te nemen, wordt gericht aan de functionaris van de gegevensbescherming bij het openbaar bestuur of de DIOB.*

De functionaris van de gegevensbescherming geeft aan de verzoeker een ontvangstmelding af.

De functionaris van de gegevensbescherming informeert betrokkene schriftelijk, onverwijld en in elk geval binnen de maand waarin het verzoek werd ontvangen, over elke weigering of beperking van het recht zoals bedoeld in het vorig lid, evenals over de redenen van deze weigering of beperking. De informatie met betrekking tot de weigering of de beperking mogen worden weggelaten indien het meedelen ervan de goede uitvoering van het integriteitsonderzoek en het opstellen van de integriteitsbeoordeling zou schaden. De functionaris van de gegevensbescherming vermeldt de feitelijke of juridische redenen waarop zijn beslissing berust. Deze inlichtingen worden ter beschikking gesteld van de bevoegde gegevensbeschermingsautoriteit voor de verwerking van persoonsgegevens.

Naar gelang de complexiteit van de verzoeken en het aantal verzoeken kan de in het derde lid vermelde termijn, indien nodig, worden verlengd met twee maanden. Binnen de maand na ontvangst van het verzoek, informeert de functionaris van de gegevensbescherming betrokkene over deze verlenging en de reden van het uitstel.

De functionaris van de gegevensbescherming brengt betrokkene op de hoogte van de mogelijkheid om klacht in te dienen bij de bevoegde gegevensbeschermingsautoriteit voor de verwerking van persoonsgegevens en om een beroep in rechte in te stellen.”

100. De toelichting verduidelijkt dat de betrokkene uiteraard het recht behoudt om zich te beroepen op de gewone administratieve geschil- en beroepsprocedures en dat zijn bestuurlijk dossier dus beschikbaar blijft.
101. Voor de uitoefening van de rechten door de betrokkene stelt de toelichting dat gedurende de periode waarin het advies wordt opgesteld, en tot op het ogenblik dat het advies aan de verzoekende overheid is verzonden, de rechten van betrokkenen worden uitgesloten. Dit is de fase van analyse van verzamelde gegevens en een toegang tot gegevens in deze fase zou het niet mogelijk maken om de missie van openbaar belang uit te voeren die aan het openbaar bestuur dan wel de DIOB is toegekend. Wanneer deze fase is afgesloten, kan de betrokkene via de functionaris van de gegevensbescherming bij het openbaar bestuur, desgevallend de DIOB zijn recht op toegang, rectificatie en uitwissing uitoefenen.
102. De VTC stelt vast dat deze regeling afwijkt van de regeling die in andere ontwerpen die ze geadviseerd heeft werd opgenomen¹³. Op basis van de uitzonderingsregel mogelijk gemaakt door artikel 23, AVG kan de betrokkene beroep doen op een verificatieprocedure¹⁴, net in de gevoelige fase. Bovendien is het de verwerkingsverantwoordelijke die per verzoek moet oordelen of er op de uitzondering wordt beroep gedaan en heeft de functionaris voor gegevensbescherming nooit beslissingsmacht, enkel een adviesbevoegdheid.
103. Mogelijk is het de bedoeling om af te stemmen met de in ontwerp zijnde federale regeling waarbij ook geen gebruik wordt gemaakt van de verificatieprocedure (maar wel meer transparantie naar de betrokkene bij het begin van het onderzoek wordt voorzien). De VTC wijst er evenwel op dat het e-govdecreet in ieder geval een verificatieprocedure voorziet waarin de VTC een rol speelt. De VTC beveelt aan om de regeling van het Ontwerp te herbekijken.

8. Vertrouwelijkheid

104. Er wordt een bijzondere aandacht besteed aan de vertrouwelijkheid: artikel 17 en 18 stellen een strafrechtelijk gesanctioneerd beroepsgeheim in:

***“Art. 17.** De personeelsleden van het openbaar bestuur of de DIOB die belast zijn met het integriteitsonderzoek zijn voor de handelingen die ze stellen in uitvoering van dat onderzoek gehouden aan het beroepsgeheim zoals bedoeld artikel 458 van de Strafwet. Hij die dit beroepsgeheim schendt, wordt gesanctioneerd met de straffen voorzien in artikel 458 van de Strafwet.*

***Art. 18.** § 1. Buiten het geval waarin ze worden opgeroepen om in rechte te getuigen in strafzaken, of voor een parlementaire onderzoekscommissie, zijn de volgende personen gebonden door het beroepsgeheim en mogen ze aan geen enkele persoon of autoriteit gegevens bekendmaken waarvan zij bij de uitoefening van de bevoegdheden krachtens dit decreet, in kennis werden gesteld:*

- *de personeelsleden van de DIOB;*
- *de leden van het orgaan van het openbaar bestuur dat bevoegd is om een beslissing zoals vermeld in artikel 3 te nemen en alle personeelsleden van het openbaar bestuur die kennis krijgen van persoonsgegevens en informatie die werd verzameld met het oog op het uitvoeren van integriteitsbeoordelingen.*

De geheimhoudingsplicht blijft bestaan zelfs wanneer ze de DIOB of het openbaar bestuur hebben verlaten of de medewerking hebben stopgezet.

§ 2. In afwijking van paragraaf 1 en onverminderd artikel 8, §2 deelt de DIOB:

1) op eigen initiatief alle gegevens mee waarover het beschikt in het kader van extremisme, van terrorisme en van de financiering van terrorisme, aan de Veiligheid van de Staat, de Algemene Dienst inlichting en veiligheid van de Krijgsmachten en de Cel voor financiële informatieverwerking;

¹³ Zie bijvoorbeeld VTC/A/W/2020/36

https://overheid.vlaanderen.be/sites/default/files/media/VTC/VTC_A_W_2020_36_advies.pdf

¹⁴ <https://overheid.vlaanderen.be/verificaties-bij-onderzoeken-inspectiediensten>

2) op verzoek van de inlichtingen- en veiligheidsdiensten, de Cel voor financiële informatieverwerking en het Coördinatieorgaan voor de dreigingsanalyse, alle gegevens aan hen mee die nuttig zijn voor de uitvoering van hun opdrachten;

3) op verzoek van de gerechtelijke overheden, in het kader van het opsporings-, gerechtelijk of strafuitvoeringsonderzoek, hen de gevraagde gegevens mee.

§ 3. Artikel 29 van het Wetboek van Strafvordering is niet van toepassing op

a) de leden en organen van het openbaar bestuur die betrokken zijn bij het integriteitsonderzoek en de integriteitsbeoordeling,

b) de personeelsleden van de DIOB, binnen de uitoefening van de opdrachten van de DIOB.

Het eerste lid geldt enkel voor de sanctioneerbare feiten die in het integriteitsonderzoek of de integriteitsbeoordeling betrokken zijn.

§ 4. *Inbreuken op de eerste paragraaf worden bestraft met een gevangenisstraf van een jaar tot drie jaar en een geldboete van honderd euro tot duizend euro of met een van die straffen alleen. De bepalingen van boek I van het Strafwetboek, met inbegrip van hoofdstuk VII en artikel 85, zijn van toepassing op inbreuken op dit artikel.*

105. De VTC beoordeelt de invoering van de geheimhoudingsplicht – al is ze al verplicht - positief. De VTC wijst er wel op dat een beroepsgeheim in principe geen uitwisseling toelaat tussen personeelsleden ook al zijn er meerdere mensen belast met een integriteitsonderzoek

9. Beveiligingsmaatregelen

106. 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.

107. De VTC wijst erop dat aangezien het gegevens zoals bedoeld in artikel 10, AVG, betreft en de gegevens niet duidelijk afgebakend zijn en het mogelijk delicate gegevens/ bijzondere categorieën van persoonsgegevens betreft een bijzondere aandacht vereist is inzake informatieveiligheid.

108. Artikel 24 van het Ontwerp bevat verplichtingen inzake beveiliging, met een opdracht aan de Vlaamse Regering:

“Art. 24. [...].

De directeur van de DIOB en het orgaan van het openbaar bestuur dat bevoegd is om een beslissing zoals vermeld in artikel 3 te nemen, neemt de gepaste technische en organisatorische maatregelen om te verzekeren dat de toegang tot de gegevens en de verwerkingsmogelijkheden beperkt worden tot wat de personen nodig hebben voor de uitoefening van hun functie of voor de noden van de dienst.

Hij neemt daarenboven de gepaste technische of organisatorische maatregelen om de persoonsgegevens te beschermen tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging of iedere andere niet-toegelaten verwerking van deze gegevens. De Vlaamse regering bepaalt daartoe de nadere modaliteiten.

109. De VTC herhaalt haar bezorgdheid over het feit dat het Ontwerp voorziet dat de persoonsgegevens die werden gebruikt bij een integriteitsonderzoek minstens deels worden bewaard bij de betrokken openbare besturen. Het gaat om een zeer ruime groep entiteiten, die ook kleinere (lokale) instanties omvat met soms slechts beperkte kennis en middelen om een gepast veiligheidsniveau te verzekeren. Dit is **bijzonder riskant** bij verwerkingen die in principe gericht zouden moeten zijn op het achterhalen van ernstige criminele feiten (zoals blijkt uit de voorbeelden van geïsoleerde feiten die de opstellers van het Ontwerp opgeven). Het lijkt sterk aangewezen om bij dit soort gevoelige

gegevens minstens te voorzien in het verplichte gebruik van een centrale en sterk beveiligde infrastructuur, eerder dan volledig te rekenen op de capaciteiten van de betrokken entiteiten.

110. 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.
111. Voor de concrete uitwerking hiervan wijst de VTC op de aanbeveling¹⁵ ter voorkoming van gegevenslekken en op de referentiemaatregelen¹⁶ die bij elke verwerking van persoonsgegevens in acht zouden moeten worden genomen. De VTC benadrukt ook het belang van een behoorlijk gebruikers- en toegangsbeheer¹⁷ en een logging van de toegangen zodat de functionaris en de toezichthouders kunnen controleren wie wanneer toegang had tot welke gegevens, wat zijn/haar acties waren en waarom¹⁸.
112. Zoals geciteerd in luik II.2 van dit advies, worden er uitgebreide verplichtingen inzake logging opgelegd.
113. Voor zover er gedacht wordt aan het gebruik van cloudtoepassingen, verwijst de VTC naar haar adviezen en aanbevelingen daarover¹⁹.
114. In geval beroep wordt gedaan op een verwerker dan wijst de VTC op volgende vereisten:
- sluiten van een verwerkersovereenkomst;
 - aanstellen van een DPO door de verwerker;
 - aanwijzen van categorieën personen die toegang hebben en lijst bijhouden.
115. 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 gebeuren²⁰.

¹⁵ Aanbeveling CBPL nr. 01/2013

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

¹⁶ 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>)

¹⁷ Zie ook Aanbeveling CBPL nr. 01/2008

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

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

¹⁸ *Audit trailing of beveiligd controlespoor.*

¹⁹ <https://overheid.vlaanderen.be/vlaamse-toezichtcommissie-cloud>

²⁰ Dit kan eventueel ook in een ministerieel besluit of een omzendbrief.

III. BESLUIT

116. De VTC ziet dat de adviesvrager een inspanning heeft gedaan om de gegevensverwerking goed te kaderen. Ze is evenwel van oordeel dat het voorgelegde voorontwerp op verschillende punten te vaag is en op die manier **onvoldoende waarborgen** biedt wat de bescherming van de persoonsgegevens van de betrokkenen betreft.
117. Naast deze algemene tekortkoming, die hoe dan ook geremedieerd moet worden, adviseert de VTC dat volgende elementen bijkomend worden geïmplementeerd :
- herbekijken of administratiefrechtelijke veroordelingen in rekening moeten worden genomen gezien het doel van de gegevensverwerking ('criminaliteitsredenen');
 - datamining en profilering: uitdrukkelijk uitsluiten of de vereiste waarborgen inbouwen;
 - de categorieën persoonsgegevens nader bepalen, bij voorkeur in het decreet zelf;
 - de toegang door de personeelsleden te verduidelijken/beperken;
 - de bewaartermijn van 3 jaar verantwoorden;
 - de regeling van de uitzondering op de rechten van de betrokkenen herbekijken;
 - bekijken op welke wijze een gepast beveiligingsniveau verzekerd kan worden eventueel via centralisatie;
 - de juistheid van de persoonsgegevens garanderen;
 - de regeling inzake verificaties herwerken;
 - de VTC na twee jaar na de inwerkingtreding van het decreet een evaluatierapport bezorgen.

Hans Graux,
Voorzitter VTC

Getekend door: Hans Graux (Signature)
Getekend op: 2023-03-09 10:41:48 +01:00
Reden: Ik keur dit document goed

