



Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 213/2026 van 6 oktober 2026

Betreft: Advies m.b.t. een voorontwerp van wet *betreffende de georganiseerde criminaliteit* (ADV-2026-00128)

Trefwoorden: georganiseerde criminaliteit – titel 2 WVG – afscherming van identiteit – pseudonimisering – gespecialiseerde afdelingen voor risicoprofielen – veiligheidscontroles – gezondheidsgegevens – identificatie penitentiair personeel – verwerkingsverantwoordelijkheid – registers – bewaartermijnen – rechten van betrokkenen – gegevensbeschermingseffectbeoordeling

Originele versie

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, met name op artikelen 23 en 26 (hierna: WOG);

Gelet op Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (hierna: AVG);

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

Gelet op de adviesaanvraag van mevrouw Annelies Verlinden, Minister van Justitie (hierna: de aanvrager), ontvangen op 30 juli 2026;

Brengt de Autorisatie- en Adviesdienst van de Gegevensbeschermingsautoriteit (hierna: de Autoriteit) op 5 oktober 2026 het volgende advies uit:

I. Voorwerp en context van de adviesaanvraag

1. Op 30 juli 2026 verzocht de aanvrager het advies van de Autoriteit met betrekking tot een voorontwerp van wet *betreffende de georganiseerde criminaliteit* (hierna: het ontwerp).
2. Het ontwerp beoogt een ruim pakket van maatregelen in te voeren ter bestrijding van de georganiseerde criminaliteit. Het bevat onder meer bepalingen inzake de afscherming van de identiteit van bepaalde magistraten en griffiers, de hervorming van de wrakingsprocedure, de oprichting van gespecialiseerde afdelingen voor risicoprofielen in gevangenissen, de identificatie van penitentiaire personeelsleden, het varen met schepen zonder geldige nationaliteit, het bedrieglijk verhandelen van reisdocumenten en de invoering van een bijdrage in de kosten van de detentie.
3. De adviesaanvraag heeft in het bijzonder betrekking op de artikelen 23 tot en met 33 en 35 tot en met 39 van het ontwerp, op artikel 40 voor wat betreft de identificatie van de personeelsleden van de penitentiaire administratie, alsook op de artikelen 5 tot en met 11, 17 en 53 en de daarmee samenhangende bepalingen die de verwerking van persoonsgegevens van magistraten van het openbaar ministerie, onderzoeksrechters en griffiers van de onderzoeksrechter regelen.
4. Het eerste onderdeel van de adviesaanvraag betreft de mogelijkheid om aan magistraten van het openbaar ministerie, onderzoeksrechters en griffiers van de onderzoeksrechter die betrokken zijn bij onderzoeken naar bijzonder zware misdrijven een code toe te kennen die in de plaats treedt van hun identiteitsgegevens. De identiteit en de toegekende code worden opgenomen in een vertrouwelijk register bij het federaal parket. De code wordt vervolgens gebruikt in de processen-verbaal, tijdens een eventuele getuigenis en in de verdere procedure, terwijl slechts in de wettelijk bepaalde gevallen toegang kan worden verkregen tot de onderliggende identiteit.
5. Het tweede onderdeel regelt de oprichting van gespecialiseerde afdelingen voor risicoprofielen. Het ontwerp stelt de voorwaarden en procedure voor plaatsing in deze afdelingen vast, voorziet in beperkingen van de contacten en activiteiten van de betrokken gedetineerden en voert zowel bij de centrale penitentiaire administratie als in de betrokken gevangenissen registers in waarin onder meer de plaatsingsbeslissingen, de toegelaten contacten, de groepsactiviteiten en bepaalde gegevens over de medische en penitentiaire opvolging worden geregistreerd.
6. Het derde onderdeel strekt er tot slot toe bepaalde personeelsleden van de penitentiaire administratie niet langer met hun volledige naam, maar met een voornaam en een identificatienummer te laten optreden. De identiteit blijft gekoppeld aan dit nummer in het detentiebeheersysteem. Het ontwerp regelt tevens wie de achterliggende identiteit kan opvragen,

voorziet in een register van de aanvragen en in logging van de raadplegingen, en legt een vertrouwelijkheidsverplichting op aan personen die van de identiteit kennis krijgen.

7. Het onderhavige advies dient zich bijgevolg in hoofdzaak uit te spreken over de noodzakelijkheid, proportionaliteit en voorzienbaarheid van deze gegevensverwerkingen, over de afbakening van de categorieën van persoonsgegevens, betrokkenen en ontvangers, over de aanwijzing van de verwerkingsverantwoordelijken, over de maximale bewaartermijnen en over de beperkingen van de rechten van de betrokkenen. Daarbij moet rekening worden gehouden met het feit dat verschillende onderdelen van het ontwerp onder titel 2 van de WVG vallen, terwijl andere verwerkingen onder de AVG en titel 1 WVG kunnen blijven ressorteren.

II. Onderzoek ten gronde

a. Bevoegdheid van de Autoriteit en toepasselijk gegevensbeschermingskader

8. Voorafgaandelijk merkt de Autoriteit op dat de in het ontwerp geregelde gegevensverwerkingen niet allen onder hetzelfde gegevensbeschermingsrechtelijke kader vallen. Het toepasselijke kader moet worden bepaald in functie van zowel de betrokken verwerkingsverantwoordelijke als het concrete doeleinde waarvoor de verwerking plaatsvindt. In het bijzonder is titel 2 WVG van toepassing op verwerkingen door de in artikel 26, 7°, WVG bedoelde bevoegde overheden, voor zover deze worden verricht met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten, de tenuitvoerlegging van straffen of de bescherming tegen en voorkoming van gevaren voor de openbare veiligheid.
9. De penitentiaire administratie wordt in artikel 26, 7°, i), WVG uitdrukkelijk als bevoegde overheid aangemerkt voor haar wettelijke opdrachten inzake de uitvoering van vrijheidsbenemende straffen en maatregelen. Bijgevolg zullen de verwerkingen in het kader van de plaatsing en opvolging van gedetineerden in de ontworpen gespecialiseerde afdelingen voor risicoprofielen en de daarmee samenhangende veiligheidsmaatregelen in beginsel onder titel 2 WVG vallen. Hetzelfde geldt, naargelang het concrete doeleinde en de betrokken actor, voor bepaalde verwerkingen door de gerechtelijke overheden en de politiediensten. Daarentegen blijven verwerkingen die niet voor een van de in artikel 27 WVG bedoelde doeleinden worden verricht, onderworpen aan de AVG en titel 1 WVG. De kwalificatie moet derhalve per verwerking worden gemaakt en kan niet louter uit de hoedanigheid van de betrokken overheidsinstantie worden afgeleid.
10. Voor zover de Veiligheid van de Staat in het kader van de in het ontwerp bedoelde veiligheidscontroles persoonsgegevens verwerkt bij de uitvoering van haar wettelijke opdrachten, ressorteren deze verwerkingen daarentegen onder titel 3 WVG en het daarvoor geldende bijzondere toezichtskader.

11. De Autoriteit wijst vervolgens op het noodzakelijke onderscheid tussen haar bevoegdheid om zich **in het kader van het wetgevend proces** over de ontworpen norm uit te spreken en de bevoegdheid om **achteraf toezicht uit te oefenen op concrete verwerkingen**. Artikel 4, § 2, WOG sluit het toezicht van de Autoriteit uit ten aanzien van verwerkingen door de hoven en rechtbanken en het openbaar ministerie bij de uitoefening van hun gerechtelijke taken. Deze uitzondering strekt ertoe de onafhankelijkheid van de rechterlijke macht bij de uitoefening van haar gerechtelijke functies te vrijwaren.
12. Deze toezichtsexceptie doet evenwel geen afbreuk aan de bevoegdheid van de Autoriteit om advies te verlenen over een normatieve tekst die dergelijke verwerkingen regelt. Zoals de Autoriteit reeds heeft uiteengezet in advies nr. 77/2020¹, betreft de beoordeling van een voorontwerp van wet geen controle *in concreto* op een verwerking door het openbaar ministerie of een rechtscollege, maar een advies over een handeling van de wetgever. De uitoefening van deze adviesbevoegdheid in het wetgevend proces interfereert als dusdanig niet met de onafhankelijke uitoefening van de latere taken inzake opsporing, vervolging en berechting. De Autoriteit is bijgevolg bevoegd om de in het ontwerp opgenomen wettelijke omkadering van deze verwerkingen aan de toepasselijke gegevensbeschermingsrechtelijke vereisten te toetsen.
13. Dit onderscheid is eveneens relevant voor de overige actoren waarop het ontwerp betrekking heeft. De feitelijke verwerkingen door de geïntegreerde politie vallen binnen de bevoegdheid van het Controleorgaan op de Politie Informatie (hierna: het COC), terwijl het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten (hierna: het Comité I) bevoegd is voor de onder zijn toezicht vallende verwerkingen door de inlichtingen- en veiligheidsdiensten. Voor de penitentiaire administratie werd daarentegen geen afzonderlijke toezichthoudende autoriteit aangewezen. Gelet op de residuaire bevoegdheid van de Autoriteit blijft zij derhalve bevoegd voor het toezicht op de verwerkingen van de penitentiaire administratie, ook wanneer titel 2 WVG daarop het materiële toetsingskader vormt. Het toepasselijke materiële recht en de bevoegde toezichthoudende autoriteit mogen bijgevolg niet met elkaar worden vereenzelvigd.
14. De Autoriteit stelt in dit verband vast dat de aanvrager de onderhavige adviesaanvraag uitsluitend bij de Autoriteit heeft ingediend en in het aanvraagformulier heeft aangegeven dat het ontwerp geen verwerking betreft door een van de daarin opgesomde bijzondere overheden. Uit het ontwerp en de memorie van toelichting blijkt evenwel dat bepaalde ontworpen verwerkingen rechtstreeks betrekking hebben op politiediensten en dat in het kader van de veiligheidscontroles

¹ Te raadplegen via: <https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-77-2020.pdf>.

onder meer een beroep kan worden gedaan op de geïntegreerde politie en de Veiligheid van de Staat.

15. Overeenkomstig artikel 54/1 WOG en het *Samenwerkingsprotocol tussen de Belgische federale toezichthoudende autoriteiten op het vlak van dataprotectie*² heeft de Autoriteit de adviesaanvraag daarom tevens ter kennis gebracht van het COC en het Comité I. Het samenwerkingsprotocol bepaalt immers dat wanneer een adviesaanvraag uitsluitend bij de Autoriteit wordt ingediend en uit een eerste onderzoek blijkt dat een andere toezichthoudende autoriteit mogelijk eveneens bevoegd is om advies te verlenen, de Autoriteit de aanvraag aan die autoriteit overmaakt. De aldus gevatte toezichthoudende autoriteiten beslissen vervolgens autonoom of zij, binnen hun respectieve bevoegdheden, eveneens een advies uitbrengen.
16. De onderhavige adviesverlening doet dan ook geen afbreuk aan een eventueel afzonderlijk advies van het COC of het Comité I en loopt evenmin vooruit op hun respectieve bevoegdheden inzake het toezicht op concrete toekomstige verwerkingen. De Autoriteit beperkt zich in het onderhavige advies tot de beoordeling van de door de wetgever ontworpen normatieve omkadering en gaat per voldoende homogeen verwerkingscomplex uit van het materiële kader dat daarop van toepassing is.

b. Afscherming van de identiteit van magistraten en griffiers

b.1 Doeleinde, noodzakelijkheid en aard van de beschermingsmaatregel

17. De artikelen 5 tot en met 11 van het ontwerp voeren een regeling in waarbij aan magistraten van het openbaar ministerie, onderzoeksrechters en griffiers van de onderzoeksrechter die betrokken zijn bij onderzoeken naar misdrijven bedoeld in boek II, titel 1; titel 4, hoofdstuk 1; titel 8, hoofdstukken 1, 2 en 3; en de artikelen 405 tot 409 van het Strafwetboek een code kan worden toegekend die hun identiteit in de verdere strafprocedure afschermt. De identiteit en de code worden gekoppeld in een vertrouwelijk register dat bij het federaal parket wordt bewaard. De code wordt vervolgens onder meer gebruikt in processen-verbaal en wanneer de betrokken persoon als getuige wordt gehoord.
18. Uit de memorie van toelichting blijkt dat deze maatregel ertoe strekt de ongecontroleerde verspreiding van de identificatiegegevens van de betrokken gerechtelijke actoren te beperken en hen te beschermen tegen bedreiging, intimidatie, corruptie en represailles vanwege criminele organisaties. De bestaande beschermingsmechanismen worden door de aanvrager hoofdzakelijk

² Te raadplegen via: <https://www.gegevensbeschermingsautoriteit.be/publications/samenwerkingsprotocol-tussen-de-belgische-federale-toezichthoudende-autoriteiten-op-het-vlak-van-dataprotectie.pdf>.

als reactief beschouwd, terwijl de ontworpen maatregel de blootstelling van de betrokken personen preventief moet beperken. De maatregel strekt aldus mede tot bescherming van de veiligheid van de betrokken personen, de onafhankelijkheid en sereniteit van de rechterlijke macht en de doeltreffendheid van strafrechtelijke onderzoeken. De Autoriteit is van oordeel dat deze doeleinden gerechtvaardigd zijn en dat de afscherming van identificatiegegevens in beginsel een geschikt middel kan vormen om deze te verwezenlijken.

19. De Autoriteit merkt evenwel op dat de in het ontwerp en de memorie van toelichting gehanteerde noties van "*anonimiteit*" en "*anonieme code*" juridisch niet correct zijn. De code kan immers aan de hand van het vertrouwelijke register opnieuw worden gekoppeld aan de identiteit van de betrokken persoon. Er is bijgevolg sprake van **pseudonimisering** in de zin van artikel 26, 5°, WVG en niet van anonimisering. De code blijft derhalve een persoonsgegeven en de betrokken verwerking blijft integraal onderworpen aan titel 2 WVG. De Autoriteit verzoekt de aanvrager om de terminologie in het ontwerp en de memorie van toelichting dienovereenkomstig aan te passen en bij voorkeur te verwijzen naar de "*afscherming van de identiteit*" en een "*beschermingscode*".
20. Het ontworpen artikel 112*undecies*/1, § 1, van het Wetboek van straffondervinding stelt als materiële voorwaarde voor de toepassing van de maatregel vast dat ernstige aanwijzingen moeten bestaan dat de onderzochte feiten een van de in paragraaf 2 opgesomde misdrijven uitmaken (zie *supra* punt 17). Artikel 112*undecies*/3 in ontwerp vereist daarnaast dat het verzoekschrift de "*bijzondere redenering*" vermeldt die de toekenning van de code wettigen. De memorie van toelichting verduidelijkt dat elk verzoek individueel wordt beoordeeld, rekening houdend met de specifieke omstandigheden van het onderzoek en de daadwerkelijk gelopen risico's. Deze laatste vereiste blijkt evenwel niet met dezelfde duidelijkheid uit de normatieve tekst van het ontwerp.
21. Gelet op het preventieve karakter van de maatregel acht de Autoriteit het niet noodzakelijk dat reeds een concrete of gematerialiseerde bedreiging ten aanzien van de betrokken magistraat of griffier wordt aangetoond. De loutere omstandigheid dat het onderzoek betrekking heeft op een van de in artikel 112*undecies*/1, § 2, in ontwerp opgesomde misdrijven kan evenwel evenmin volstaan. De wet moet vereisen dat uit concrete en geïndividualiseerde omstandigheden eigen aan het dossier, de aard of context van het onderzoek, de rol van de betrokkene of het bestaande dreigingsbeeld redelijkerwijze blijkt dat de bekendmaking van diens identiteit een reëel risico kan doen ontstaan voor zijn veiligheid of integriteit, dan wel voor het goede verloop van het onderzoek. De in de memorie van toelichting beschreven individuele risicobeoordeling moet derhalve uitdrukkelijk in het ontwerp zelf worden verankerd.
22. De memorie van toelichting vermeldt voorts uitdrukkelijk dat geen bijzondere subsidiariteitsvoorwaarde wordt opgelegd, omdat de toekenning van een code niet automatisch

gebeurt en de Beschermingscommissie tussenkomt om het dossier te beoordelen. De Autoriteit merkt op dat het facultatieve karakter van een maatregel en de tussenkomst van een beoordelingsorgaan op zichzelf de naleving van de beginselen van noodzakelijkheid en evenredigheid niet waarborgen. De Beschermingscommissie moet bij haar beoordeling tevens nagaan of de afscherming in het concrete geval noodzakelijk en evenredig is en niet verder gaat dan hetgeen voor het nagestreefde beschermingsdoeleinde vereist is. Deze beoordelingsvereiste moet minstens uitdrukkelijk uit de wettelijke regeling blijken. Artikel 28 WVG vereist immers dat de verwerkte persoonsgegevens toereikend en ter zake dienend zijn en niet bovenmatig in verhouding tot het betrokken doeleinde.

23. De Autoriteit neemt voor het overige wel positief akte van het feit dat de maatregel niet automatisch wordt toegepast, dat een schriftelijk en gemotiveerd verzoekschrift vereist is, dat de beslissing wordt genomen door de Beschermingscommissie en gemotiveerd moet zijn, en dat in geval van uiterst dringende noodzakelijkheid een door de voorzitter toegekende code zo snel mogelijk door de voltallige Commissie moet worden gevalideerd. Deze procedurele waarborgen zijn relevant voor de proportionaliteit van de verwerking. Het feit dat tegen de beslissing van de Beschermingscommissie geen rechtsmiddel openstaat, onderstreept evenwel bijkomend het belang van voldoende nauwkeurige wettelijke beoordelingscriteria.
24. Tot slot is de Autoriteit van oordeel dat artikel 112 *undecies*/1 in ontwerp op voldoende bepaalde wijze de actieve geldigheidsduur van de beschermingscode vaststelt: deze loopt gedurende het onderzoek en tot een rechterlijke beslissing in kracht van gewijsde is getreden. Volgens de memorie van toelichting wordt in beginsel voor elk afzonderlijk onderzoek een andere code toegekend, teneinde te voorkomen dat de herhaalde toepassing van dezelfde code uiteindelijk zelf tot identificatie leidt. Na afloop van het dossier wordt de code niet langer actief gebruikt, maar blijft zij voorkomen in de processen-verbaal, het strafdossier en de rechterlijke beslissing. De Autoriteit neemt hiervan akte. De aldus vastgestelde gebruiksduur moet evenwel worden onderscheiden van de bewaartermijn van de onderliggende koppeling tussen de code en de identiteit in het vertrouwelijke register, waarop hierna wordt teruggekomen.

b.2 Categorieën van persoonsgegevens en behandeling van het verzoek

25. Artikel 112 *undecies*/2 in ontwerp definieert de "identiteit" als "*alle gegevens of handelingen die rechtstreeks of onrechtstreeks tot identificatie*" van de betrokken magistraat, onderzoeksrechter of griffier kunnen leiden. De Autoriteit begrijpt dat, gelet op het beperkte aantal magistraten binnen bepaalde rechtsgebieden en specialisaties, ook indirecte informatie de doeltreffendheid van de beschermingsmaatregel kan ondermijnen. De gekozen definitie is evenwel dermate ruim

dat zij geen bruikbare afbakening vormt van de persoonsgegevens die in het kader van de ontworpen regeling mogen worden verwerkt.

26. Het ontwerp moet bijgevolg een duidelijk onderscheid maken tussen, enerzijds, de rechtstreeks of onrechtstreeks identificerende persoonsgegevens die moeten worden afgeschermd en, anderzijds, de procedurele of operationele maatregelen die moeten verhinderen dat de identiteit door een handeling of de concrete omstandigheden van het onderzoek alsnog bekend wordt. Dit is in het bijzonder noodzakelijk omdat artikel 112*undecies*/4 in ontwerp bepaalt dat de "*identiteit*" van de betrokkene in het vertrouwelijke register wordt opgenomen. De ruime definitie van artikel 112*undecies*/2 in ontwerp mag er niet toe leiden dat zonder verdere afbakening alle mogelijke indirect identificerende informatie in dat register wordt geregistreerd.
27. Artikel 112*undecies*/3 in ontwerp bepaalt concreter dat het verzoekschrift onder meer de naam, voornaam en het Rijksregisternummer van de betrokken persoon, het notitienummer van het strafdossier en de bijzondere redenen voor de toekenning van een code bevat. Gelet op het belang van een ondubbelzinnige koppeling tussen de beschermingscode en de juiste gerechtelijke actor kan de verwerking van een uniek identificatienummer in deze bijzonder gevoelige context in beginsel worden verantwoord, onverminderd de voorwaarden die krachtens de Rijksregisterwet voor het gebruik van het Rijksregisternummer gelden. De gegevens die onder de "*bijzondere redener*" worden opgenomen, moeten evenwel beperkt blijven tot hetgeen noodzakelijk is om de Beschermingscommissie in staat te stellen de voorwaarden voor de toekenning van de code te beoordelen.
28. De Autoriteit stelt daarnaast vast dat artikel 112*undecies*/3 in ontwerp bepaalt dat de voorzitter van de Beschermingscommissie andere personen dan de in artikel 111ter, § 1, tweede lid, van het Wetboek van straffordering bedoelde leden kan uitnodigen wanneer zij "*een belang hebben bij de bevoegdheden bedoeld in het eerste lid*". De draagwijdte van deze formulering is onduidelijk. Artikel 111ter, § 1, eerste lid, van het Wetboek van Straffordering heeft immers betrekking op de bevoegdheden van de Beschermingscommissie inzake het toekennen, wijzigen en intrekken van beschermingsmaatregelen en financiële hulpmaatregelen in het kader van de bestaande beschermingsregeling, terwijl de ontworpen bepaling louter betrekking heeft op de mogelijkheid voor de korpschef van de betrokken magistraat om, bij een met redenen omkleed verzoekschrift, de Beschermingscommissie te verzoeken een beschermingscode toe te kennen. Indien wordt beoogd de voorzitter toe te laten bijkomende personen uit te nodigen wier deelname noodzakelijk is voor de beoordeling van dat verzoek, moet dit uitdrukkelijk en nauwkeurig in de ontworpen bepaling worden vermeld. Gelet op de gevoelige persoonsgegevens en strafdossiergegevens waartoe deze personen in voorkomend geval toegang kunnen krijgen, moet hun deelname bovendien worden beperkt tot de gevallen waarin zij noodzakelijk is voor de beoordeling van het

concrete verzoek. Hun toegang moet worden beperkt tot de informatie die voor die deelname strikt noodzakelijk is en hun vertrouwelijkheidsverplichtingen moeten ondubbelzinnig worden vastgesteld.

29. Om dezelfde reden moet de mogelijkheid voor de Beschermingscommissie om het volledige strafdossier te raadplegen restrictief worden toegepast. De raadpleging van de relevante stukken moet het uitgangspunt vormen. Toegang tot het volledige strafdossier kan slechts worden verantwoord indien de Commissie zonder die ruimere toegang niet met kennis van zaken kan beoordelen of aan de voorwaarden voor de beschermingsmaatregel is voldaan. De reden voor een dergelijke ruimere raadpleging moet in voorkomend geval controleerbaar worden gedocumenteerd.

b.3 Verwerkingsverantwoordelijkheid en vertrouwelijk register

30. De Autoriteit stelt vast dat het ontwerp niet uitdrukkelijk bepaalt wie als verwerkingsverantwoordelijke optreedt voor de behandeling van de verzoekschriften door de Beschermingscommissie en voor het in artikel 112*undecies*/4 in ontwerp bedoelde vertrouwelijke register. Laatstgenoemde bepaling vermeldt dat de voorzitter van de Beschermingscommissie de identiteit en de code optekent en dat het register bij het federaal parket wordt bewaard. De enkele aanwijzing van de natuurlijke persoon die deze materiële handeling verricht, volstaat evenwel niet om de verwerkingsverantwoordelijkheid te regelen.
31. Artikel 26, 8°, WVG definieert de verwerkingsverantwoordelijke als de bevoegde overheid die de doeleinden en middelen van de verwerking vaststelt en bepaalt dat, wanneer deze elementen bij of krachtens een wet worden vastgesteld, de door die norm aangewezen entiteit als verwerkingsverantwoordelijke optreedt. De aanvrager moet bijgevolg nagaan of de verantwoordelijkheid voor de onderscheiden verwerkingen reeds ondubbelzinnig uit het bestaande wettelijke kader voortvloeit. Indien dit niet het geval is, moet het ontwerp de betrokken verwerkingsverantwoordelijke of verwerkingsverantwoordelijken uitdrukkelijk en functioneel aanwijzen en hun respectieve verantwoordelijkheden afbakenen.
32. Artikel 112*undecies*/4 bepaalt dat de identiteit en de code in het vertrouwelijke register worden opgenomen, maar stelt niet nauwkeurig vast welke categorieën van persoonsgegevens dit register verder bevat. Nochtans zal voor het beheer ervan minstens informatie nodig kunnen zijn over de betrokken strafzaak, de datum van toekenning, de geldigheidsduur of status van de code en de eventuele beëindiging ervan. Krachtens artikel 33 WVG moet de wettelijke grondslag minstens de doeleinden en de categorieën van persoonsgegevens van de verwerking vaststellen. Het ontwerp moet de categorieën van gegevens die daadwerkelijk in het vertrouwelijke register mogen worden

opgenomen dan ook nauwkeuriger bepalen en beperken tot hetgeen noodzakelijk is voor het beheer van de identiteit-codekoppeling en de wettelijk toegelaten gevallen van kennisname van de identiteit.

33. De Autoriteit neemt daarentegen positief akte van de bijzonder beperkte toegangsregeling van artikel 112undecies/4. Voor magistraten van het openbaar ministerie en onderzoeksrechters kan de volledige identiteit slechts worden geraadpleegd door de federale procureur en de bevoegde magistraat wanneer tegen de beschermde persoon een strafonderzoek wordt gevoerd; voor griffiers geldt een vergelijkbare regeling ten aanzien van de magistraten die het betrokken strafonderzoek voeren. De toegang is aldus gekoppeld aan een concreet en wettelijk omschreven doeleinde.

b.4 Bewaartermijn en beveiliging

34. Het ontwerp stelt evenwel geen maximale bewaartermijn vast voor de identiteit-codekoppeling in het vertrouwelijke register. Het feit dat artikel 112undecies/1 de periode bepaalt gedurende welke de code actief wordt gebruikt, verhelpt deze lacune niet. Volgens de memorie van toelichting blijft de beschermingscode immers ook na de definitieve beëindiging van het dossier in de processen-verbaal, het dossier en de rechterlijke beslissing opgenomen en wordt de achterliggende identiteit niet aan de partijen vrijgegeven. Een zekere verdere beschikbaarheid van de koppeling kan bijgevolg noodzakelijk zijn om de verantwoordingsplicht en de wettelijk voorziene mogelijkheden tot latere identificatie te waarborgen, maar rechtvaardigt geen bewaring voor onbepaalde duur.
35. Artikel 30 WVG bepaalt uitdrukkelijk dat de wet een maximale bewaartermijn moet vaststellen. Zij kan daarbij voorzien in een eerste bewaartermijn waarna aan de hand van wettelijke noodzakelijkheids- en proportionaliteitscriteria wordt beoordeeld of verdere bewaring nodig is, maar ook in dat geval moet een absolute maximale bewaartermijn worden vastgesteld. Het ontwerp moet derhalve een maximale termijn bepalen voor de bewaring van de identiteit-codekoppeling, waarbij rekening kan worden gehouden met de noodzaak om de identiteit nog te kunnen achterhalen in het kader van de wettelijk bepaalde gerechtelijke, tuchtrechtelijke of andere procedures. Het aanvangspunt en het uiterste einde van die termijn moeten objectief bepaalbaar zijn.
36. Dezelfde oefening moet worden gemaakt voor de persoonsgegevens die voorkomen in het verzoekschrift, de stukken die voor de beoordeling ervan aan de Beschermingscommissie worden meegedeeld en de beslissing van de Commissie. Het einde van de actieve geldigheidsduur van de code betekent niet noodzakelijk dat al deze gegevens gedurende dezelfde termijn moeten worden

bewaard. De bewaartermijnen moeten worden vastgesteld in functie van hun respectieve doeleinden en mogen niet langer lopen dan daarvoor noodzakelijk is.

37. Gelet op het bijzondere beschermingsdoeleinde van het register is de beveiliging ervan bovendien van wezenlijk belang. Een ongeoorloofde koppeling tussen de code en de identiteit zou niet alleen een inbreuk op de bescherming van persoonsgegevens vormen, maar rechtstreeks het veiligheidsrisico verwezenlijken dat het ontwerp beoogt te voorkomen. De strafbaarstelling van de ongeoorloofde raadpleging of bekendmaking waarin artikel 53 van het ontwerp voorziet, vormt een relevante waarborg, maar heeft in essentie een repressief karakter en kan passende preventieve technische en organisatorische maatregelen niet vervangen.
38. De verwerking moet bijgevolg worden georganiseerd volgens een strikt *need-to-know*-beginsel, met een passende scheiding tussen de identificatiegegevens en de overige dossiergegevens, sterke authenticatie en toegangscontrole en een volledige logging van iedere raadpleging en bekendmaking. Artikel 56 WVG verplicht reeds tot het bijhouden van logbestanden die onder meer toelaten de reden, de datum en het tijdstip van een raadpleging of bekendmaking, alsook zo mogelijk de identiteit van de gebruiker en de ontvanger, te achterhalen. Artikel 60 WVG vereist daarnaast passende technische en organisatorische maatregelen die zijn afgestemd op het risico. Gelet op de bijzondere gevoeligheid van het register moet de praktische beveiligingsarchitectuur bovendien uitdrukkelijk aan bod komen in de gegevensbeschermingseffectbeoordeling.

b.5 Gebruik van de code en latere onthulling van de identiteit

39. Artikel 112undecies/5 in ontwerp bepaalt dat processen-verbaal opgesteld door politie- of opsporingsdiensten geen enkel element mogen bevatten dat de veiligheid en de afscherming van de identiteit van de betrokken persoon in het gedrang kan brengen en voorziet dat de onder code handelende magistraat of onderzoeksrechter alle maatregelen kan nemen om de eigen identiteit of die van de griffier (van de onderzoeksrechter) verborgen te houden. De Autoriteit onderschrijft het daarmee nagestreefde doeleinde. Er moet evenwel worden verzekerd dat de afscherming niet leidt tot een verlies van de traceerbaarheid van de proceshandelingen. Wanneer identificerende vermeldingen uit een document worden verwijderd of afgeschermd, moeten de betrokken handeling, de gebruikte code en, waar nodig, de wijziging zelf binnen de beveiligde omgeving controleerbaar blijven. Dit is noodzakelijk zowel voor de integriteit van het strafdossier als voor de eventuele latere toepassing van de wettelijk geregelde mogelijkheden tot identificatie.
40. De artikelen 112undecies/6 en 112undecies/7, die respectievelijk het optreden als getuige onder code en de onthulling van de identiteit in geval van strafvervolgning tegen de beschermde persoon regelen, zijn voldoende nauw verbonden met het beschermingsdoeleinde en beperken de

bekendmaking van de werkelijke identiteit tot specifiek omschreven omstandigheden. Vanuit het oogpunt van de bescherming van persoonsgegevens geven deze bepalingen als dusdanig geen aanleiding tot bijzondere opmerkingen.

41. Artikel 17 van het ontwerp voorziet daarnaast in een bijzondere procedure wanneer de afscherming van de identiteit van een onderzoeksrechter de daadwerkelijke uitoefening van het wrakingsrecht onmogelijk zou maken. De Autoriteit neemt positief akte van deze waarborg, waarbij de kamer van inbeschuldigingstelling, op verzoek van de stafhouder, de afscherming van de identiteit kan opheffen. Zij stelt evenwel vast dat de verzoeker daartoe reeds in zijn wrakingsakte, op basis van concrete elementen, aannemelijk moet maken dat de afscherming hem verhindert zijn wrakingsrecht uit te oefenen. Niet alle in artikel 828 van het Gerechtelijk Wetboek bedoelde wrakingsgronden kunnen evenwel worden vastgesteld zonder kennis van de identiteit van de betrokken onderzoeksrechter. Terwijl bepaalde gronden kunnen blijken uit diens concrete optreden of proceshandelingen, houden andere gronden rechtstreeks verband met zijn persoon, zoals een persoonlijk belang, verwantschap, eerdere betrokkenheid of een belangenconflict. In die laatste gevallen kan de afgeschermd identiteit precies de informatie vormen die noodzakelijk is om het bestaan van een mogelijke wrakingsgrond te kunnen vaststellen. De Autoriteit beveelt daarom aan om minstens in de memorie van toelichting nader te verduidelijken welke concrete situaties met het ontworpen artikel 835*bis* van het Gerechtelijk Wetboek worden beoogd en hoe de vereiste van "*concrete elementen*" moet worden toegepast wanneer de mogelijke wrakingsgrond zelf afhankelijk is van de identiteit van de onderzoeksrechter. Daarbij moet worden verzekerd dat van de verzoeker niet wordt verlangd dat hij reeds het bestaan van een persoonsgebonden wrakingsgrond aannemelijk maakt wanneer hij die grond redelijkerwijs slechts kan vaststellen nadat de identiteit van de onderzoeksrechter bekend is. Desgevallend verdient het aanbeveling dit ook in de ontworpen bepaling zelf te verduidelijken, bijvoorbeeld door te bepalen dat het volstaat dat de verzoeker concrete elementen aanvoert waaruit blijkt dat kennis van de identiteit redelijkerwijs noodzakelijk is om het bestaan van een in artikel 828 bedoelde wrakingsgrond te kunnen beoordelen.
42. Onder voorbehoud van de voorgaande opmerkingen geeft de ontworpen afscherming van de identiteit van magistraten van het openbaar ministerie, onderzoeksrechters en griffiers van de onderzoeksrechter als dusdanig geen aanleiding tot fundamenteel bezwaar. Het beschermingsdoeleinde is gerechtvaardigd en het ontwerp bevat reeds verschillende relevante procedurele waarborgen. Een aanpassing is evenwel vereist wat betreft de materiële voorwaarden voor de toekenning van de code, de kwalificatie als pseudonimisering, de afbakening van de verwerkte gegevens, de deelname van derden aan de Beschermingscommissie, de verwerkingsverantwoordelijkheid, de inhoud en maximale bewaartermijn van het vertrouwelijke register en de beveiliging en traceerbaarheid van de identiteit-codekoppeling.

43. Artikel 23 van het ontwerp geeft vanuit gegevensbeschermingsrechtelijk oogpunt als dusdanig geen aanleiding tot bijzondere opmerkingen.
44. Artikel 24 van het ontwerp wijzigt daarnaast de informatieverstrekking in het kader van het bestaande individuele bijzondere veiligheidsregime door voortaan het openbaar ministerie als adviesverlenende instantie aan te wijzen. Uit de memorie van toelichting blijkt dat informatie van politiediensten die aanleiding kan geven tot een dergelijke plaatsing via het openbaar ministerie aan de penitentiaire administratie kan worden meegedeeld. De opmerkingen in de punten 46 tot en met 49 inzake de kwaliteit, actualiteit en herkomst van de meegedeelde gegevens zijn *mutatis mutandis* ook op deze verwerking van toepassing, met dien verstande dat het bijzondere regime van artikel 45 WVG moet worden geëerbiedigd voor zover de meegedeelde gegevens rechtstreeks of onrechtstreeks afkomstig zijn van een in titel 3 WVG bedoelde overheid.

c. Gespecialiseerde afdelingen voor risicoprofielen

c.1 Plaatsingscriteria en gegevenskwaliteit

45. De artikelen 25 tot en met 38 van het ontwerp voeren een nieuw regime in voor de plaatsing van bepaalde gedetineerden in gespecialiseerde afdelingen voor risicoprofielen. Het ontworpen artikel 118/1 van de basiswet van 12 januari 2005 *betreffende het gevangeniswezen en de rechtspositie van de gedetineerden* (hierna: de basiswet van 12 januari 2005) koppelt deze plaatsing aan het bestaan van ernstige en actuele aanwijzingen dat de gedetineerde een leidende of deelnemende rol speelt in een criminele organisatie en een ernstige en voortdurende bedreiging voor de veiligheid vormt, vanuit de gevangenis criminele activiteiten leidt of voortzet die een dergelijke bedreiging vormen, dan wel vanuit de gevangenis door intimidatie, bedreiging, geweld of corruptie de uitoefening van een openbaar ambt of de werking van een openbare dienst ernstig ontwricht of in het gedrang brengt. Volgens de memorie van toelichting moeten deze criteria worden gestaafd door concrete en nog actuele elementen, waaronder nauwkeurige informatie afkomstig van externe partners.
46. Gelet op het nagestreefde doeleinde — het voorkomen dat georganiseerde criminaliteit vanuit de gevangenis wordt voortgezet en het beschermen van de interne en externe veiligheid — geven deze criteria als dusdanig geen aanleiding tot principiële opmerkingen. Zij zijn bovendien voldoende gericht om te vermijden dat de enkele band met een criminele organisatie automatisch tot plaatsing aanleiding geeft. De Autoriteit benadrukt niettemin dat de plaatsing een bijzonder ingrijpende maatregel vormt, zodat de persoonsgegevens waarop zij steunt juist, actueel,

betrouwbaar en rechtstreeks relevant moeten zijn voor de beoordeling van de in het ontworpen artikel 118/1 vastgestelde criteria.

47. Deze vereiste is des te belangrijker nu uit de memorie van toelichting blijkt dat informatie van politiediensten via het openbaar ministerie aan de penitentiaire administratie kan worden meegedeeld en dat de directeur-generaal zijn beslissing tot plaatsing of hernieuwing volledig op het advies van het openbaar ministerie zal baseren. Artikel 32 WVG vereist in dit verband dat persoonsgegevens die op feiten zijn gebaseerd zoveel mogelijk worden onderscheiden van persoonsgegevens die op persoonlijke beoordelingen berusten en dat bij een doorgifte de nodige aanvullende informatie wordt verstrekt om de juistheid, volledigheid, betrouwbaarheid en actualiteit van de gegevens te kunnen beoordelen.
48. Het advies van het openbaar ministerie moet derhalve op een wijze worden opgesteld die de directeur-generaal toelaat te onderscheiden welke elementen betrekking hebben op vastgestelde feiten, vermoedens, inlichtingen of beoordelingen, wat de herkomst en datum van de relevante informatie is en in welke mate zij actueel en betrouwbaar wordt geacht. Daarbij hoeft niet noodzakelijk alle onderliggende informatie integraal aan de penitentiaire administratie te worden meegedeeld, maar moeten voldoende concrete elementen worden verstrekt om de wettelijke plaatsingscriteria op controleerbare wijze te kunnen beoordelen. Indien de onderliggende informatie later wordt gecorrigeerd, geactualiseerd of als onjuist wordt aangemerkt, moet dit onverwijld worden meegedeeld aan de instantie die deze gegevens verder verwerkt, overeenkomstig artikel 32, § 3, WVG.
49. Voor zover het advies van het openbaar ministerie informatie bevat die rechtstreeks of onrechtstreeks afkomstig is van een inlichtingen- of veiligheidsdienst, moet bovendien rekening worden gehouden met het specifieke regime van artikel 45 WVG. Titel 2 WVG laat immers niet toe dat de ontvangst van dergelijke gegevens door de penitentiaire administratie de bijzondere regels inzake toegang, mededeling en bescherming van gegevens afkomstig van titel 3-overheden neutraliseert. Dit aspect moet in de operationele gegevensstromen uitdrukkelijk worden onderscheiden.
50. Artikel 118/4 in ontwerp voorziet voorts in een automatisch voorlopig regime zodra aan de gedetineerde wordt meegedeeld dat de procedure tot mogelijke plaatsing is gestart. Gedurende deze fase wordt de betrokkene onder meer uitgesloten van gemeenschappelijke activiteiten, bezoek en telefonisch contact en wordt zijn briefwisseling systematisch gecontroleerd. Volgens de memorie van toelichting worden deze maatregelen automatisch en stelselmatig toegepast en staat daartegen geen afzonderlijk beroep open. Hoewel de opportuniteit van dit regime als dusdanig buiten het specifieke gegevensbeschermingsrechtelijke onderzoek valt, versterkt de automatische

koppeling tussen de ontvangen informatie en deze onmiddellijke gevolgen het belang van de juistheid, actualiteit en betrouwbaarheid van de gegevens waarop de opstart van de procedure berust.

c.2 Veiligheidscontroles van bezoekers en telefonische contacten

51. Het ontworpen artikel 118/2, 2° en 3°, van de basiswet van 12 januari 2005 bepaalt dat iedere persoon die de gedetineerde wenst te bezoeken of met hem telefonisch contact wenst te onderhouden vooraf aan een veiligheidscontrole wordt onderworpen. Op basis van het resultaat daarvan kan de directeur-generaal het contact weigeren wanneer geïndividualiseerde aanwijzingen bestaan dat het bezoek of het telefonisch contact de handhaving van de veiligheid ernstig in gevaar kan brengen. Indien het resultaat van de controle niet binnen de wettelijke termijn wordt ontvangen, wordt het contact toegestaan.
52. De Autoriteit stelt vast dat het ontwerp het bestaan en de gevolgen van deze veiligheidscontrole regelt, maar de verwerking van persoonsgegevens die eraan voorafgaat vrijwel volledig ongeregeld laat. Het ontwerp bepaalt met name niet welke overheid de veiligheidscontrole aanvraagt en uitvoert, welke overheden of gegevensbronnen mogen worden geraadpleegd, welke categorieën van persoonsgegevens daarbij mogen worden verwerkt, volgens welke criteria het veiligheidsrisico wordt beoordeeld, welke gegevens of resultaten aan de directeur-generaal mogen worden meegedeeld en gedurende welke termijn deze informatie wordt bewaard.
53. Deze lacune kan niet uitsluitend door de memorie van toelichting worden opgevangen. Daarin wordt vermeld dat de penitentiaire administratie gebruik kan maken van de informatie waarover zij zelf beschikt en van informatie verkregen door het bevragen van "externe partners", waaronder de geïntegreerde politie, het openbaar ministerie en de Veiligheid van de Staat. Een dergelijke open verwijzing naar externe partners biedt, gelet op de aard van de betrokken gegevens, onvoldoende voorzienbaarheid. Voor de verwerking onder titel 2 WVG vereist artikel 33 WVG dat de wettelijke of reglementaire grondslag minstens de doeleinden en de categorieën van verwerkte persoonsgegevens regelt.
54. De ontworpen regeling moet bijgevolg minstens vaststellen of voldoende nauwkeurig bepaalbaar maken:
 - welke (categorieën van) overheden of diensten aan de veiligheidscontrole kunnen bijdragen;
 - welke actor voor welk onderdeel van de veiligheidscontrole als verwerkingsverantwoordelijke optreedt en welk gegevensbeschermingsrechtelijk kader op de betrokken verwerking van toepassing is;
 - welke categorieën van gegevens daarbij mogen worden geraadpleegd of uitgewisseld;

- welke concrete veiligheidsrisico's worden onderzocht;
 - welke informatie aan de directeur-generaal mag worden meegedeeld;
 - welke maximale bewaartermijnen van toepassing zijn;
 - op welke wijze onjuiste of achterhaalde informatie wordt gecorrigeerd en hoe een nieuwe beoordeling kan plaatsvinden.
55. De omstandigheid dat de veiligheidscontrole betrekking heeft op bezoekers en telefonische contactpersonen en niet op de gedetineerde zelf, sluit de toepassing van titel 2 WVG niet uit. Artikel 31 WVG vermeldt immers uitdrukkelijk, naast verdachten en veroordeelden, andere personen die bij een strafbaar feit betrokken zijn, waaronder personen die contact hebben of banden onderhouden met verdachten of veroordeelden. Voor zover de penitentiaire administratie de persoonsgegevens van deze contactpersonen verwerkt in het kader van haar wettelijke opdrachten inzake de uitvoering van vrijheidsbenemende straffen en maatregelen en met het oog op de in artikel 27 WVG bedoelde veiligheidsdoeleinden, ressorteert deze verwerking onder titel 2 WVG.
56. Dit neemt niet weg dat de betrokkenen zich in een wezenlijk andere positie bevinden dan de gedetineerde. Zij zijn niet wegens hun eigen gedrag aan het betrokken detentieregime onderworpen. De enkele familiale, persoonlijke of professionele band met een gedetineerde mag bijgevolg niet leiden tot een ongedifferentieerde verwerking van alle persoonsgegevens die bij de geraadpleegde bevoegde overheden beschikbaar zijn. De veiligheidscontrole moet derhalve beperkt blijven tot de gegevens die noodzakelijk en relevant zijn om te beoordelen of het concrete bezoek of telefonisch contact een ernstig gevaar voor de veiligheid kan vormen. Dit geldt des te meer wanneer de betrokken contactpersoon een minderjarige of een andere kwetsbare persoon is.
57. Vanuit het beginsel van minimale gegevensverwerking verdient het bovendien de voorkeur dat de veiligheidscontrole in beginsel resulteert in een doelgebonden beoordeling van het concrete veiligheidsrisico, zonder dat alle onderliggende ruwe gegevens systematisch aan de penitentiaire administratie worden overgemaakt. De mededeling kan bijvoorbeeld worden beperkt tot het resultaat van de controle, de relevante risicofactoren, de geldigheidsduur van de beoordeling en de feitelijke elementen die noodzakelijk zijn om een eventuele weigeringsbeslissing te motiveren. Indien de mededeling van bijkomende onderliggende gegevens noodzakelijk is, moet zij afzonderlijk aan de beginselen van noodzakelijkheid, proportionaliteit en doelbinding worden getoetst.
58. Het ontwerp bepaalt dat een toelating later kan worden ingetrokken wanneer nieuwe informatie aantoont dat het contact een ernstig gevaar vormt. Omgekeerd moet ook worden voorzien in een

passende herbeoordeling wanneer de informatie die tot een weigering heeft geleid niet langer actueel blijkt, wordt gecorrigeerd of haar relevantie heeft verloren. De veiligheidscontrole mag niet leiden tot een statisch risicolabel dat gedurende de volledige plaatsingsperiode blijft doorwerken ongeacht latere wijzigingen.

c.3 Psycho-medische gegevens

59. Het ontwerp voorziet in een intensieve medische en psychiatrische opvolging van de in de gespecialiseerde afdeling geplaatste gedetineerde. Twee maanden vóór het verstrijken van de plaatsingsbeslissing moet de gevangenisdirecteur bovendien een verslag over het verloop van de plaatsing en een psycho-medisch advies aan de directeur-generaal bezorgen. Deze documenten worden vervolgens integraal aan het openbaar ministerie overgemaakt met het oog op een geactualiseerd advies over de eventuele hernieuwing van de plaatsing.
60. De Autoriteit erkent dat de mentale en fysieke gezondheidstoestand van de gedetineerde relevant kan zijn voor de beoordeling van de gevolgen en de voortzetting van een bijzonder restrictief detentieregime. Gezondheidsgegevens behoren evenwel tot de bijzondere categorieën van persoonsgegevens bedoeld in artikel 34 WVG en mogen slechts worden verwerkt wanneer dit strikt noodzakelijk is en passende waarborgen worden geboden.
61. Het ontwerp moet daarom verduidelijken welke informatie het psycho-medisch advies mag bevatten en voor welk precies doeleinde zij aan de directeur-generaal en vervolgens aan het openbaar ministerie wordt meegedeeld. Uit de memorie van toelichting blijkt dat het advies betrekking moet hebben op de verenigbaarheid van de mentale gezondheid van de gedetineerde met de verdere plaatsing in de gespecialiseerde afdeling. In zoverre dit het beoogde doeleinde vormt, moet de verwerking daartoe worden beperkt. Het is niet noodzakelijk dat het volledige medisch of psychiatrisch dossier wordt meegedeeld; een functioneel advies dat beperkt is tot de voor de beslissing noodzakelijke conclusies en elementen verdient de voorkeur.
62. Een soortgelijke opmerking geldt voor het ontworpen artikel 118/6 van de basiswet van 12 januari 2005. Deze bepaling laat toe dat de gevangenispsychiater, op eigen initiatief of op verzoek, informatie aan de directeur-generaal verstrekt met het oog op een eventuele versoepeling van de maatregelen. De memorie van toelichting voegt daaraan toe dat informatie afkomstig van de psychiater vervolgens door de directeur-generaal aan het openbaar ministerie zal worden overgemaakt met het oog op diens advies. Die verdere mededeling volgt niet uitdrukkelijk uit het ontworpen artikel 118/6 zelf. Gelet op de bijzondere gevoeligheid van gezondheidsgegevens kan de memorie van toelichting hiervoor niet als zelfstandige rechtsgrond dienen. Indien deze mededeling wordt behouden, moet zij uitdrukkelijk in de wet worden geregeld.

c.4 Verwerkingsverantwoordelijkheid en bewaartermijnen

63. Het ontworpen artikel 118/5 van de basiswet van 12 januari 2005 voorziet in twee registers. Een eerste register wordt bijgehouden bij de centrale penitentiaire administratie en bevat de beslissingen inzake plaatsing, groepsactiviteiten, bezoek en telefonische contacten. Daarnaast wordt in iedere gevangenis met een gespecialiseerde afdeling een lokaal register bijgehouden met gegevens over de geplaatste gedetineerde, toegestane contacten, activiteiten en de medische en penitentiaire opvolging. De FOD Justitie wordt uitdrukkelijk aangewezen als verwerkingsverantwoordelijke voor de persoonsgegevens die in het kader van het bijhouden van deze registers worden verwerkt.
64. De Autoriteit neemt akte van de uitdrukkelijke aanwijzing van de FOD Justitie als verwerkingsverantwoordelijke voor het bijhouden van beide registers. Voor het centrale register geeft deze aanwijzing geen aanleiding tot bijzondere opmerkingen. Wat het register van de gevangenis betreft, moet evenwel worden verduidelijkt hoe de verantwoordelijkheden tussen de FOD Justitie en de betrokken penitentiaire inrichting worden verdeeld. Het enkele feit dat dit register lokaal wordt bijgehouden, volstaat niet om de penitentiaire inrichting als afzonderlijke of gezamenlijke verwerkingsverantwoordelijke aan te merken. Overeenkomstig artikel 26, 8°, en artikel 52 WVG is daarvoor vereist dat zij, alleen of samen met de FOD Justitie, de doeleinden en de wezenlijke middelen van de verwerking bepaalt. Indien de betrokken gevangenis uitsluitend als interne dienst van de FOD Justitie handelt binnen de wettelijk en centraal vastgestelde krijtlijnen, kan de FOD Justitie als enige verwerkingsverantwoordelijke worden aangemerkt. Indien aan de gevangenisdirectie daarentegen een eigen beslissingsbevoegdheid toekomt inzake wezenlijke aspecten van de verwerking, moet de aanwijzing van de verwerkingsverantwoordelijke daarmee in overeenstemming worden gebracht en moeten, in voorkomend geval, de respectieve verantwoordelijkheden overeenkomstig artikel 52 WVG worden vastgesteld.
65. De ontworpen bepaling vertoont daarnaast verschillende interne inconsistenties die moeten worden weggewerkt.
66. Zo bepaalt artikel 118/5, § 1, in ontwerp dat in het centrale register alle plaatsingsbeslissingen en beslissingen betreffende groepsactiviteiten, toegelaten bezoeken en telefonische contacten worden opgenomen. De opsomming van de persoonsgegevens die krachtens paragraaf 4 in dit register worden verwerkt, vermeldt evenwel uitsluitend identificatiegegevens van de gedetineerde, van de personen die aan een veiligheidscontrole werden onderworpen en van de medegedetineerden met wie groepsactiviteiten al dan niet zijn toegestaan. De inhoud, datum,

geldigheidsduur, status en motivering van de in paragraaf 1 bedoelde beslissingen worden niet als gegevenscategorieën vermeld.

67. Ook de doeleinden van het centrale register moeten worden aangevuld. Paragraaf 4 vermeldt uitsluitend het mogelijk maken van toezicht en controle en het opstellen van geanonimiseerde statistieken. Indien het register eveneens bedoeld is om de plaatsings- en regimebeslissingen operationeel te beheren, uit te voeren of op te volgen, moet dit doeleinde uitdrukkelijk worden vermeld.
68. Een soortgelijke discrepantie bestaat voor het lokale register. Daarin moeten volgens paragraaf 2 onder meer de toegelaten activiteiten en ieder bezoek van de arts, arts-psychiater en directeur worden geregistreerd. In de gegevensopsomming van paragraaf 5 worden daarentegen identificatiegegevens en eventuele opmerkingen van de arts en de arts-psychiater en opmerkingen van de gedetineerde over zijn gezondheidstoestand en situatie vermeld, zonder dat alle in paragraaf 2 bedoelde operationele gegevens duidelijk worden hernomen. De verschillende paragrafen moeten met elkaar in overeenstemming worden gebracht, zodat de categorieën van persoonsgegevens en doeleinden ondubbelzinnig uit de norm blijken.
69. Bijzondere aandacht verdient de opname van medische en psychiatrische opmerkingen en van opmerkingen van de gedetineerde over zijn gezondheidstoestand in het lokale register. Het registreren van het feit dat en het tijdstip waarop de wettelijk vereiste medische opvolging heeft plaatsgevonden kan noodzakelijk zijn om toe te zien op de naleving van de wettelijke verplichtingen. Daaruit volgt evenwel niet dat inhoudelijke medische of psychiatrische informatie in hetzelfde operationele register moet worden opgenomen.
70. In beginsel moeten inhoudelijke gezondheidsgegevens worden verwerkt binnen het daarvoor bestemde medische dossier en onder de daarbij horende specifieke toegangsbescherming. Indien de aanvrager van oordeel is dat bepaalde inhoudelijke gezondheidsgegevens noodzakelijkerwijs in het lokale register moeten worden opgenomen, moet artikel 118/5 in ontwerp de betrokken categorieën aanzienlijk nauwkeuriger afbakenen en het specifieke doeleinde, evenals de toepasselijke bewaartermijn bepalen. Overeenkomstig artikel 34, § 2, WVG moet bovendien een lijst worden opgesteld van de categorieën van personen die tot deze gegevens toegang hebben, met vermelding van hun hoedanigheid, en moeten zij aan een passende vertrouwelijkheidsverplichting zijn onderworpen.
71. Artikel 118/5, § 3, in ontwerp kent toegang toe aan de "*personen of instanties die belast zijn met het toezicht en de controle van de gevangenen of van de uitvoering van de straf of vrijheidsbenemende maatregel*". Deze formulering omvat potentieel verschillende actoren met

uiteenlopende wettelijke opdrachten. Zij mag niet aldus worden gelezen dat iedere instantie die op enige wijze toezicht uitoefent automatisch toegang krijgt tot alle gegevens in beide registers. De categorieën van ontvangers moeten nader worden bepaald of minstens ondubbelzinnig bepaalbaar zijn op basis van hun wettelijke bevoegdheden. De toegang moet bovendien per actor en per gegevenscategorie worden beperkt tot hetgeen voor diens concrete taak noodzakelijk is.

72. Het ontwerp stelt ten slotte geen maximale bewaartermijn vast voor de persoonsgegevens in beide registers. Dit vormt een wezenlijke lacune. Artikel 30 WVG bepaalt uitdrukkelijk dat de formele norm een maximale bewaartermijn moet vaststellen en dat de gegevens na afloop daarvan moeten worden gewist. Enkel wanneer de wet voorziet in een periodieke noodzakelijkheidstoets kan een verlenging worden toegestaan, maar ook dan moet een absolute maximale termijn worden bepaald.
73. De Autoriteit acht het daarbij aangewezen om te differentiëren naar gelang van de aard en het doeleinde van de gegevens. Zo hoeven gegevens betreffende een lopende veiligheidscontrole, een geweigerde contactpersoon, een toegelaten contactpersoon, een plaatsingsbeslissing, een psycho-medische opvolging en een beroepsprocedure niet noodzakelijk gedurende dezelfde periode te worden bewaard. De termijnen kunnen onder meer worden gekoppeld aan de duur van de plaatsing, de eventuele behandeling van het beroep en een nader gemotiveerde periode waarin de gegevens nog noodzakelijk zijn voor wettelijk toezicht of gerechtelijke procedures.
74. Voor zover het centrale register wordt gebruikt voor het opstellen van “geanonimiseerde statistieken”, geeft dit doeleinde als dusdanig geen aanleiding tot bijzondere opmerkingen. De Autoriteit benadrukt evenwel dat de aldus verkregen statistieken slechts buiten het toepassingsgebied van titel 2 WVG vallen indien zij daadwerkelijk anoniem zijn. Overweging 21 van richtlijn (EU) 2016/680 preciseert in dit verband dat informatie slechts als anoniem kan worden beschouwd wanneer zij geen betrekking heeft op een geïdentificeerde of identificeerbare natuurlijke persoon, waarbij rekening moet worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij door de verwerkingsverantwoordelijke of een andere persoon zullen worden gebruikt om de betrokkene rechtstreeks of onrechtstreeks te identificeren. Het louter verwijderen van namen, identificatienummers of andere rechtstreekse identificatoren volstaat bijgevolg niet. Ook geaggregeerde gegevens kunnen nog persoonsgegevens uitmaken wanneer individuele gedetineerden redelijkerwijs kunnen worden onderscheiden of geïdentificeerd, bijvoorbeeld op basis van een combinatie van de betrokken gevangenis, de periode en duur van de plaatsing, leeftijd, detentieregime of andere bijzondere kenmerken. Bij de anonimisering moet derhalve rekening worden gehouden met het risico op afzondering (*singling out*), koppeling met andere beschikbare gegevens en gevolgtrekkingen die alsnog identificatie

mogelijk maken.³ Ter vergelijking merkt de Autoriteit op dat artikel 197 WVG voor de onder artikel 89 AVG ressorterende statistische verwerkingen eveneens als uitgangspunt vooropstelt dat anonieme gegevens worden gebruikt en slechts wanneer daarmee het statistische doel niet kan worden bereikt, het gebruik van gepseudonimiseerde of vervolgens niet-gepseudonimiseerde gegevens toelaat.

c.5 Informatie, toegang en beroepsprocedure

75. Het ontworpen artikel 118/3 van de basiswet van 12 januari 2005 voorziet in beginsel in een relevante procedurele waarborg doordat de gedetineerde bij de opstart van de plaatsingsprocedure kennis krijgt van de redenen en van het advies van het openbaar ministerie en opmerkingen kan formuleren. Hetzelfde geldt bij een eventuele hernieuwing van de plaatsing. Het ontwerp maakt daarop evenwel een uitzondering wanneer de wet dit bepaalt of wanneer het advies zelf vermeldt dat zijn inhoud niet openbaar mag worden gemaakt ter vrijwaring van het geheim van het opsporings- of gerechtelijk onderzoek.
76. De Autoriteit begrijpt dat de mededeling van bepaalde informatie lopende onderzoeken, bronnen, onderzoeksmethoden of de veiligheid van derden kan schaden. De beperking van het recht op informatie en toegang kan evenwel niet uitsluitend afhangen van de enkele vermelding door de opsteller van het advies dat de inhoud niet mag worden meegedeeld. Voor zover de ontworpen niet-mededeling tevens een beperking inhoudt van de in de artikelen 37 en 38 WVG bedoelde informatie- en toegangsrechten, moet zij voldoen aan de in die bepalingen gestelde vereisten van noodzakelijkheid en evenredigheid. Een weigering of beperking van een verzoek om toegang overeenkomstig artikel 38 WVG moet bovendien overeenkomstig de paragrafen 3 en 4 van die bepaling worden gemotiveerd en gedocumenteerd. Dit geldt onverminderd het bijzondere regime van artikel 45 WVG voor persoonsgegevens die rechtstreeks of onrechtstreeks afkomstig zijn van de in titel 3 WVG bedoelde overheden.
77. Waar volledige mededeling niet mogelijk is, moet bijgevolg worden onderzocht of kan worden volstaan met het weglaten van de betrokken passages of met het verstrekken van een samenvatting van de feitelijke elementen waarop de plaatsingsbeslissing steunt. De gedetineerde moet in ieder geval voldoende kennis kunnen nemen van de dragende redenen om daarover op

³ Zie voor het bestaande Europese referentiekader inzake anonimisering: Groep gegevensbescherming artikel 29, *Opinion 05/2014 on Anonymisation Techniques*, WP216, aangenomen op 10 april 2014, waarin met name de risico's van *singling out*, *linkability* en *inference* als relevante maatstaven voor de beoordeling van de doeltreffendheid van anonimisering worden gehanteerd: [Opinion 05/2014 on Anonymisation Techniques](#). Zie tevens EDPB, *Guidelines 02/2026 on Anonymisation*, versie 1.0, op 7 juli 2026 aangenomen **met het oog op publieke consultatie** en derhalve nog niet definitief vastgesteld; deze richtsnoeren beogen voormelde Opinion 05/2014 te actualiseren en verder te verfijnen, onder meer aan de hand van de criteria *No Record Isolation*, *No Linkage* en *No Inference*: [EDPB – Guidelines 02/2026, public consultation](#).

nuttige wijze opmerkingen te kunnen formuleren en het voorziene beroep daadwerkelijk te kunnen uitoefenen, zonder dat informatie wordt vrijgegeven waarvan de bescherming noodzakelijk is.

78. In dezelfde zin is artikel 118/8 in ontwerp te absoluut geformuleerd. Deze bepaling schrijft voor dat alle informatie over de persoon van een gedetineerde in de gespecialiseerde afdeling die door personeelsleden van de penitentiaire administratie wordt opgesteld "om veiligheidsredenen" niet aan hem wordt meegedeeld. Een dergelijke algemene uitsluiting, zonder onderscheid naargelang de aard van de informatie, het concrete veiligheidsrisico of de duur ervan, voldoet niet aan het vereiste dat een beperking noodzakelijk en evenredig moet zijn. Artikel 118/8 moet worden herwerkt zodat alleen de informatie waarvan de bekendmaking daadwerkelijk een wettelijk beschermd belang in gevaar brengt geheel of gedeeltelijk kan worden afgeschermd en dit slechts zolang dat risico bestaat.
79. Dezelfde problematiek doet zich voor in de ontworpen beroepsprocedure. Artikel 166/2 bepaalt dat de gedetineerde geen toegang heeft tot stukken wanneer het advies vermeldt dat de inhoud ervan niet openbaar mag worden gemaakt, terwijl artikel 166/3 bepaalt dat de beslissing van de Beroepscommissie geen melding maakt van elementen waarvan de opsteller de openbaarmaking uitdrukkelijk heeft verboden. De opsteller van informatie kan uiteraard aangeven welke concrete risico's aan openbaarmaking verbonden zijn, maar mag niet door een loutere vermelding zelfstandig en definitief bepalen welke informatie buiten iedere tegenspraak en beoordeling blijft.
80. De Beroepscommissie moet minstens zelf toegang kunnen hebben tot het volledige, niet-geredigeerde dossier en zelfstandig kunnen beoordelen of de niet-mededeling noodzakelijk en evenredig is. Waar mogelijk moet zij de gedetineerde kennis geven van de essentie van de redenen en feiten waarop de bestreden beslissing berust, zonder beschermde bronnen, personen of onderzoeksmethoden prijs te geven. Dit is tevens van belang omdat uit de memorie van toelichting blijkt dat de directeur-generaal zich bij de plaatsing volledig baseert op het advies van het openbaar ministerie en dat het beroep tegen de plaatsings- en hernieuwingsbeslissing in hoofdzaak een toetsing van de wettelijke criteria en procedure beoogt.
81. In het licht van het bovenstaande is de Autoriteit aldus van oordeel dat de ontworpen regeling inzake de oprichting van gespecialiseerde afdelingen en de daarmee gepaard gaande verwerkingen van persoonsgegevens aanzienlijk moet worden aangevuld wat betreft de wettelijke omkadering van de veiligheidscontroles, de kwaliteit en herkomst van de gegevens waarop de plaatsing steunt, de verwerking en mededeling van gezondheidsgegevens, de interne coherentie, toegang en bewaartermijnen van de centrale en lokale registers en de beperkingen van de informatie- en toegangsrechten van de betrokkenen.

d. Identificatie van de personeelsleden van de penitentiaire administratie

d.1 Algemene beoordeling en identificatiemiddel

82. De artikelen 39 tot en met 41 van het ontwerp wijzigen de wijze waarop bepaalde personeelsleden van de penitentiaire administratie worden geïdentificeerd. Het ontworpen artikel 14/1 van de wet van 23 maart 2019 *betreffende de organisatie van de penitentiaire diensten en van het statuut van het penitentiair personeel* (hierna: de wet van 23 maart 2019) bevestigt als uitgangspunt dat deze personeelsleden in alle omstandigheden identificeerbaar moeten zijn, maar laat toe dat zij zich, in plaats van met hun naam en voornaam, identificeren aan de hand van een voornaam en een persoonlijk identificatienummer. Dit nummer wordt gegenereerd door het detentiebeheersysteem en wordt daarin gekoppeld aan de werkelijke identiteit van het personeelslid.
83. Uit de memorie van toelichting blijkt dat deze maatregel is ingegeven door een toename van bedreigingen en intimidatie ten aanzien van penitentiaire personeelsleden, waaronder incidenten waarbij hun woonplaats of andere privégegevens werden achterhaald. Tegelijkertijd beoogt het ontwerp de mogelijkheid te behouden om ieder personeelslid achteraf ondubbelzinnig te identificeren. De aanvrager verwijst in dit verband tevens naar de rechtspraak van het Europees Hof voor de Rechten van de Mens en naar de aanbevelingen van het Europees Comité ter voorkoming van foltering en onmenselijke of vernederende behandeling of bestraffing (CPT), waaruit volgt dat personeelsleden die in een detentiecontext optreden identificeerbaar moeten blijven, zonder dat daartoe noodzakelijk hun naam en voornaam systematisch aan de gedetineerde moeten worden bekendgemaakt.
84. De Autoriteit is van oordeel dat de bescherming van penitentiaire personeelsleden tegen bedreiging, intimidatie en represailles een gerechtvaardigd doeleinde vormt en dat het gebruik van een identificatienummer, mits de werkelijke identiteit op betrouwbare wijze kan worden achterhaald wanneer dit noodzakelijk is, in beginsel een geschikt en evenredig middel kan vormen om dit doeleinde te verwezenlijken. Een dergelijk systeem laat immers toe de bekendmaking van identificatiegegevens te beperken zonder afbreuk te doen aan de vereisten inzake identificeerbaarheid, verantwoordingsplicht en de mogelijkheid om klachten of procedures tegen een concreet personeelslid in te stellen.
85. Net zoals bij de in onderdeel b besproken beschermingscode is evenwel geen sprake van anonimisering. De werkelijke identiteit blijft immers via het detentiebeheersysteem gekoppeld aan het identificatienummer. Het nummer en de daarmee verbonden gegevens blijven bijgevolg

persoonsgegevens. De memorie van toelichting moet de notie “anonimiteit” in deze context vermijden.

86. Artikel 14/1, § 4, in ontwerp machtigt de Koning om de nadere regels voor de identificatie vast te stellen. Uit de memorie van toelichting blijkt dat de Koning daarbij tevens zal bepalen **welke personeelsleden volgens welk identificatiemiddel identificeerbaar zijn**. De keuze welke categorieën van personeelsleden hun werkelijke naam niet hoeven bekend te maken, raakt evenwel rechtstreeks aan de draagwijdte van de ontworpen beschermingsmaatregel en kan niet zonder enige materiële begrenzing aan de Koning worden overgelaten. Het ontwerp moet minstens de objectieve criteria bepalen op basis waarvan deze categorieën worden vastgesteld, bijvoorbeeld rekening houdend met de functie, de aard van het contact met gedetineerden en de daarmee verbonden veiligheidsrisico's.
87. De memorie van toelichting vermeldt bovendien dat de “voornaam” op het identificatiemiddel niet noodzakelijk een officiële voornaam hoeft te zijn, maar eveneens een **alias** kan zijn. Deze mogelijkheid blijkt niet uit artikel 14/1 zelf. Indien daadwerkelijk wordt beoogd een alias te gebruiken, moet daarvoor een voldoende duidelijke grondslag in de normatieve tekst worden opgenomen. Tevens moet worden verzekerd dat de alias op unieke en duurzame wijze met het betrokken personeelslid verbonden blijft, zodat het gebruik ervan de mogelijkheid tot identificatie, klachtbehandeling en controle achteraf niet ondermijnt.

d.2 Bekendmaking van de achterliggende identiteit

88. Artikel 14/2, § 1, in ontwerp regelt vervolgens de gevallen waarin de achter het identificatienummer schuilgaande identiteit wordt meegedeeld. De directeur-generaal van de penitentiaire administratie of zijn afgevaardigde deelt deze identiteit mee op verzoek van onderzoeks- of vonnisgerechten waarbij strafbare feiten aanhangig zijn, administratieve rechtscolleges, of “*elke andere persoon of instantie die van een wettig belang doet blijken*”.
89. De eerste twee categorieën beantwoorden in beginsel aan duidelijk identificeerbare procedurele behoeften, voor zover de kennisname van de identiteit noodzakelijk is voor de behandeling van de betrokken zaak. Wat het wettig belang betreft, begrijpt de Autoriteit deze formulering in die zin dat een louter feitelijk of opportuniteitsgebonden belang niet volstaat, maar dat de verzoeker moet aantonen dat de kennisname van de identiteit noodzakelijk is voor de uitoefening of bescherming van een door de rechtsorde erkend belang. In die lezing vormt de vereiste dat een wettig belang wordt aangetoond een relevante waarborg tegen ongegronde, oneigenlijke of louter vindictieve verzoeken.

90. De Autoriteit acht het derhalve niet noodzakelijk dat de wetgever de categorieën van personen of instanties die zich op een dergelijk wettig belang kunnen beroepen exhaustief opsomt. Het verdient evenwel aanbeveling om minstens in de memorie van toelichting nader te verduidelijken volgens welke criteria het bestaan van een wettig belang wordt beoordeeld. Daarbij kan bijvoorbeeld worden verwezen naar de noodzaak om een klacht in te dienen of te behandelen, rechten uit te oefenen, een gerechtelijke, administratieve of tuchtrechtelijke procedure te voeren of een wettelijk opgedragen toezichts- of controlebevoegdheid uit te oefenen. In ieder geval moet er een voldoende nauw verband bestaan tussen het ingeroepen belang en de noodzaak om de werkelijke identiteit van het betrokken personeelslid te kennen.
91. De Autoriteit stelt zich wel vragen bij de keuze om de beoordeling van het bestaan van een “wettig belang” – zoals de bepaling thans is geformuleerd – uitsluitend toe te vertrouwen aan de directeur-generaal van de penitentiaire administratie of diens afgevaardigde, zonder dat de ontworpen regeling ten behoeve van de verzoeker voorziet in voldoende procedurele waarborgen om een objectieve en onpartijdige beoordeling van zijn verzoek te verzekeren. De penitentiaire administratie heeft immers zelf tot opdracht haar personeelsleden te beschermen en het verzoek om bekendmaking kan juist betrekking hebben op het vermeend onrechtmatig handelen van een personeelslid dat onder haar hiërarchisch gezag staat. Dit is in het bijzonder relevant wanneer het verzoek uitgaat van de betrokken gedetineerde, diens advocaat of een andere persoon die diens belangen behartigt. In dergelijke gevallen bestaat minstens een objectief risico op een belangenconflict, aangezien de administratie mogelijk betrokken is bij de onderliggende betwisting en tegelijkertijd moet oordelen over de voorwaarden waaronder de identiteit van een van haar personeelsleden wordt bekendgemaakt.
92. Deze problematiek doet zich niet op dezelfde wijze voor wanneer het verzoek uitgaat van een onderzoeks- of vonnisgerecht, dan wel van een administratief rechtscollege. In dat geval behoort de beoordeling of de identiteit noodzakelijk is voor de behandeling van de zaak in beginsel toe aan de betrokken onafhankelijke rechterlijke instantie. De rol van de directeur-generaal of zijn afgevaardigde zou zich in dergelijke gevallen dan ook moeten beperken tot de verificatie van het verzoek en de uitvoering ervan.
93. Voor verzoeken die uitgaan van andere personen of instanties verdient het aldus aanbeveling een procedure te voorzien waarin de noodzakelijkheid van de bekendmaking door een onafhankelijke instantie wordt beoordeeld. Op die wijze blijft het door het ontwerp nagestreefde beschermingsdoeleinde behouden, zonder dat de penitentiaire administratie zelf finaal moet beslissen over de toegang tot de identiteit van een personeelslid in een geschil waarbij zij mogelijk rechtstreeks betrokken is. Indien de aanvrager niettemin bepaalde gevallen van rechtstreekse bekendmaking op verzoek van een particulier of een andere instantie wenst te behouden, moeten

de toepasselijke criteria nauwkeurig worden bepaald en moet minstens worden voorzien in een effectieve mogelijkheid tot onafhankelijke toetsing van een weigering.

94. Voorts dient het begrip "identiteit van een personeelslid" nauwkeuriger te worden gepreciseerd. Voor het nagestreefde doeleinde zal in beginsel kunnen worden volstaan met de naam en voornaam en, waar nodig, de professionele hoedanigheid van het betrokken personeelslid. De bepaling mag niet aldus worden geïnterpreteerd dat zij toegang verleent tot het Rijksregisternummer, privéadres, persoonlijke contactgegevens of andere personeelsgegevens die niet noodzakelijk zijn om de betrokken persoon ondubbelzinnig te identificeren.
95. Zoals reeds werd uiteengezet in onderdeel a, moet het toepasselijke gegevensbeschermingsrechtelijke kader daarbij nader worden vastgesteld. De koppeling en eventuele bekendmaking van de identiteit in het kader van de uitvoering van een vrijheidsbenemende straf of maatregel en de daarmee samenhangende veiligheids- of onderzoeksdoeleinden kunnen onder titel 2 WVG vallen, doch omvat artikel 14/2 in ontwerp ook mededelingen aan administratieve rechtscolleges en potentieel aan andere publieke of private personen en instanties. Dergelijke verwerkingen vallen niet noodzakelijk onder de doeleinden van artikel 27 WVG. De ruime formulering van artikel 14/2 in ontwerp bevestigt bijgevolg de noodzaak om de doeleinden en categorieën van ontvangers nauwkeuriger af te bakenen, zodat voor iedere gegevensstroom kan worden bepaald welk gegevensbeschermingsrechtelijk regime van toepassing is.

d.3 Detentiebeheersysteem, register van aanvragen en verwerkingsverantwoordelijkheid

96. De artikelen 39 en 40 van het ontwerp maken voor de uitvoering van de ontworpen identificatieregeling gebruik van het reeds bestaande **detentiebeheersysteem**. Dit betreft de bij de FOD Justitie opgerichte geïnformatiseerde gegevensbank, bedoeld in artikel 3 van de wet van 5 mei 2019 *houdende diverse bepalingen inzake informatisering van Justitie* (hierna: de wet van 5 mei 2019), waarin de gegevens worden verwerkt die noodzakelijk zijn voor de adequate uitoefening van de wettelijke opdrachten van de penitentiaire administratie, waaronder het beheer en de beveiliging van de penitentiaire inrichtingen en de uitvoering van vrijheidsstraffen en vrijheidsbenemende maatregelen. De penitentiaire administratie treedt daarbij op als beheerder van het systeem.
97. Binnen de onderhavige regeling vervult het detentiebeheersysteem een specifieke functie voor de identificatie van het penitentiair personeel. Het ontworpen artikel 14/1, § 3, van de wet van 23 maart 2019 bepaalt dat het identificatienummer van de personeelsleden die zich identificeren aan de hand van een voornaam en een identificatienummer door dit systeem wordt gegenereerd en

dat daarin de werkelijke identiteit van het betrokken personeelslid aan dit identificatienummer wordt gekoppeld. Artikel 14/2, § 3, in ontwerp bepaalt vervolgens dat iedere raadpleging die ertoe strekt de identiteit achter een dergelijk identificatienummer te kennen, in hetzelfde systeem wordt geregistreerd. Het detentiebeheersysteem verzekert in de onderhavige context aldus zowel de koppeling tussen het identificatienummer en de werkelijke identiteit als de technische traceerbaarheid van de raadplegingen van deze koppeling.

98. Daarnaast voorziet artikel 14/2, § 2, in ontwerp in een **afzonderlijk register van aanvragen**. Iedere aanvraag om kennis te nemen van de identiteit van een aan de hand van een identificatienummer geïdentificeerd personeelslid wordt daarin ingeschreven. De inschrijving bevat volgens het ontwerp uitsluitend de naam en hoedanigheid van de aanvrager, het identificatienummer waarop het verzoek betrekking heeft en het gevolg dat aan de aanvraag werd gegeven. De Autoriteit begrijpt dat dit register ertoe strekt de behandeling van dergelijke aanvragen en, in voorkomend geval, de bekendmaking van de achterliggende identiteit achteraf controleerbaar te maken.
99. De Autoriteit is evenwel van oordeel dat de thans in het ontwerp bepaalde gegevens niet volstaan om deze controlefunctie daadwerkelijk te vervullen. Op basis daarvan kan immers niet worden nagegaan **wanneer en om welke reden** de identiteit werd gevraagd, op welke grond het verzoek werd ingewilligd of geweigerd en door wie deze beoordeling werd verricht. Dit is in het bijzonder van belang voor de in artikel 14/2, § 1, bedoelde verzoeken die steunen op een “wettig belang”, waarvoor overeenkomstig de voorgaande punten een concrete beoordeling van de noodzaak van de bekendmaking vereist is. Het register moet bijgevolg minstens toelaten de datum en het concrete doeleinde van het verzoek, de hoedanigheid of rechtsgrond waarop de verzoeker zich beroept en, in voorkomend geval, de motivering van het ingeroepen wettig belang, alsook de genomen beslissing, de datum en auteur daarvan vast te stellen. Wanneer de bekendmaking plaatsvindt op verzoek of beslissing van een gerechtelijke instantie, moet ook dit voldoende traceerbaar zijn.
100. Wat de verwerkingsverantwoordelijkheid betreft, wijst artikel 4 van de wet van 5 mei 2019 de FOD Justitie reeds aan als verwerkingsverantwoordelijke voor het detentiebeheersysteem. Deze aanwijzing geldt in beginsel ook voor de daarin tot stand gebrachte koppeling tussen de identiteit en het identificatienummer en voor de registratie van de raadplegingen daarvan. Voor het afzonderlijke register van aanvragen bevat het ontwerp daarentegen geen vergelijkbare aanwijzing en evenmin wordt verduidelijkt of dit register deel uitmaakt van het detentiebeheersysteem dan wel als een afzonderlijke databank wordt georganiseerd. De Autoriteit verzoekt de aanvrager dit te verduidelijken. Gelet op de rol van de penitentiaire administratie bij

de ontvangst en behandeling van de aanvragen lijkt de aanwijzing van de FOD Justitie in beginsel voor de hand te liggen, onder voorbehoud van hetgeen uiteengezet in punt 64 hierboven.

d.4 Bewaartermijnen

101. Ook wat de bewaartermijnen betreft, moet een duidelijk onderscheid worden gemaakt tussen het inhoudelijke register van aanvragen bedoeld in het ontworpen artikel 14/2, § 2, enerzijds en de technische registratie van de raadplegingen in het detentiebeheersysteem bedoeld in paragraaf 3 van datzelfde artikel anderzijds. De memorie van toelichting stelt dat "*voor de bewaartermijnen van beide gegevensverwerkingen*" om redenen van samenhang wordt verwezen naar artikel 23 van de wet van 5 mei 2019. Deze bedoeling komt evenwel onvoldoende duidelijk tot uiting in het dispositief. De verwijzing naar artikel 23 staat immers uitsluitend in paragraaf 3, onmiddellijk na de bepaling betreffende de registratie van de raadplegingen, en bepaalt dat "*die gegevensverwerkingen*" overeenkomstig artikel 23 worden bewaard. Deze formulering lijkt naar haar bewoordingen dan ook enkel betrekking te hebben op de in die paragraaf bedoelde raadplegingen en registraties.
102. Wat vooreerst het **register van aanvragen** betreft, stelt het ontwerp bijgevolg geen ondubbelzinnige maximale bewaartermijn vast. Voor zover deze verwerking onder titel 2 WVG valt, herinnert de Autoriteit eraan dat artikel 30 WVG vereist dat de wet, het decreet of de ordonnantie de maximale bewaartermijn bepaalt, waarna de gegevens moeten worden gewist. Ook wanneer een concrete verwerking in dit register onder de AVG zou ressorteren, moet de bewaring overeenkomstig artikel 5.1.e) AVG (beginsel van opslagbeperking) beperkt blijven tot hetgeen noodzakelijk is voor het nagestreefde doeleinde. De bewaartermijn moet in dit geval worden vastgesteld in functie van het eigen doeleinde van het register, met name het mogelijk maken van controle achteraf op de rechtmatigheid van verzoeken en bekendmakingen en, in voorkomend geval, de behandeling van klachten, beroepsprocedures of andere betwistingen. De Autoriteit is in dit verband van oordeel dat een loutere verwijzing naar de bewaartermijn van de technische loggegevens bedoeld in artikel 23 van de wet van 5 mei 2019 niet passend is. De finaliteit van deze technische logging verschilt immers wezenlijk van die van het inhoudelijke register van aanvragen. Bovendien voorziet artikel 23 in een bijzonder ruime bewaartermijn van ten minste tien en ten hoogste dertig jaar, zonder te preciseren in welke omstandigheden een bewaring gedurende dertig jaar noodzakelijk is, noch uitdrukkelijk te waarborgen dat de gegevens vóór het verstrijken van die maximale termijn worden gewist wanneer hun verdere bewaring niet langer noodzakelijk is. Voor het register van aanvragen moet bijgevolg een eigen, functioneel verantwoorde maximale bewaartermijn worden vastgesteld.

103. Voor de **technische registratie van de raadplegingen in het detentiebeheersysteem** is de verwijzing naar artikel 23 van de wet van 5 mei 2019 daarentegen functioneel coherent. Dit artikel bepaalt reeds dat iedere verwerking van persoonsgegevens in het detentiebeheersysteem automatisch wordt geregistreerd en dat deze registratie gedurende ten minste tien en hoogstens dertig jaar vanaf de uitgevoerde verwerking wordt bewaard. De in artikel 14/2, § 3, ontworpen verplichting maakt aldus gebruik van het bestaande loggingmechanisme om iedere raadpleging van de achter een identificatienummer schuilgaande identiteit traceerbaar te maken. Dit neemt evenwel niet weg dat ook voor deze verwerking de noodzakelijkheid en evenredigheid van de concrete bewaartermijn moeten kunnen worden aangetoond. In het bijzonder laat de enkele verwijzing naar een termijn van tien tot dertig jaar niet toe vast te stellen op grond van welke objectieve criteria wordt bepaald hoe lang de betrokken loggegevens daadwerkelijk worden bewaard en in welke omstandigheden een bewaring gedurende maximaal dertig jaar gerechtvaardigd is. De Autoriteit beveelt bijgevolg aan objectieve criteria te bepalen aan de hand waarvan wordt vastgesteld gedurende welke termijn de betrokken loggegevens binnen deze wettelijke vork moeten worden bewaard, in het bijzonder wanneer een bewaring langer dan de minimumtermijn van tien jaar noodzakelijk kan worden geacht, en te waarborgen dat de maximale termijn van dertig jaar niet als standaardtermijn wordt toegepast wanneer een kortere bewaring volstaat.
104. Ook de formulering van artikel 14/2, § 3, in ontwerp volgens welke "*die gegevensverwerkingen worden bewaard overeenkomstig artikel 23 (...)*", moet worden aangepast. Artikel 23 van de wet van 5 mei 2019 voorziet niet in de bewaring van de verwerking zelf, maar in de automatische **registratie** van iedere verwerking en de bewaring van die registratie. Er moet bijgevolg worden bepaald dat de registraties of loggegevens betreffende de raadplegingen worden bewaard overeenkomstig artikel 23 van de wet van 5 mei 2019.
105. Tot slot moet ook worden verduidelijkt gedurende welke termijn de **onderliggende koppeling tussen het identificatienummer en de werkelijke identiteit van het personeelslid** in het detentiebeheersysteem wordt bewaard. De verwijzing naar artikel 23 van de wet van 5 mei 2019 regelt uitsluitend de bewaring van de logregistraties en bepaalt als dusdanig niet hoe lang de gegevens waarop de raadpleging betrekking heeft mogen worden bewaard. Voor deze koppeling moet bijgevolg een eigen maximale bewaartermijn worden vastgesteld die aansluit bij haar specifieke finaliteit. Daarbij lijkt het passend minstens rekening te houden met de duur van de tewerkstelling of functie waarin het identificatienummer wordt gebruikt en, na de beëindiging daarvan, met de periode gedurende welke de identificatie van het betrokken personeelslid nog noodzakelijk kan zijn met het oog op controle, klachten, aansprakelijkheidsvorderingen of gerechtelijke procedures. Indien de aanvrager deze verwerking binnen het bestaande regime van het detentiebeheersysteem wenst te regelen, moeten de

relevante bepalingen van de wet van 5 mei 2019, in het bijzonder inzake de betrokken gegevenscategorieën en bewaartermijnen, dienovereenkomstig worden aangepast.

e. Gegevensbeschermingseffectbeoordeling en beveiliging

106. Uit het aanvraagformulier blijkt dat de door het ontwerp omkaderde verwerkingen **niet aan een gegevensbeschermingseffectbeoordeling werden onderworpen**. De Autoriteit wijst erop dat artikel 58 WVG de verwerkingsverantwoordelijke verplicht vóór de verwerking een dergelijke beoordeling uit te voeren wanneer een soort verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Voor de verwerkingen die onder de AVG ressorteren, geldt de overeenkomstige verplichting van artikel 35 AVG. Voor de verwerkingen door federale overheden die onder de AVG en titel 1 WVG ressorteren, bepaalt artikel 23 WVG bovendien, ter uitvoering van artikel 35.10 AVG, dat vóór de concrete verwerkingsactiviteit een specifieke gegevensbeschermingseffectbeoordeling wordt verricht, ook wanneer reeds in het kader van de vaststelling van de wettelijke grondslag een algemene beoordeling werd uitgevoerd.
107. Gelet op de aard van de in het ontwerp voorziene verwerkingen is de Autoriteit van oordeel dat minstens verschillende daarvan waarschijnlijk een hoog risico in voormelde zin met zich meebrengen. Het ontwerp voorziet immers onder meer in de verwerking van gegevens betreffende personen die betrokken zijn bij zware vormen van criminaliteit, de combinatie en mededeling van gerechtelijke, politionele en in voorkomend geval inlichtingengegevens, de verwerking van gezondheidsgegevens, de verwerking van gegevens van bezoekers en telefonische contactpersonen van gedetineerden, alsook in registers en identificatiesystemen waarvan ongeoorloofde toegang ernstige gevolgen kan hebben voor zowel magistraten, gedetineerden als personeelsleden. Daarnaast kunnen bepaalde verwerkingen rechtstreeks bijdragen tot beslissingen die de betrokkenen aanzienlijk treffen, zoals de plaatsing in een gespecialiseerde afdeling of de weigering van bezoek of telefonisch contact.
108. De Autoriteit is bijgevolg van oordeel dat de betrokken verwerkingen voor hun operationalisering aan een gegevensbeschermingseffectbeoordeling onderworpen moeten worden. Gelet op de uiteenlopende doeleinden, gegevensstromen, betrokkenen en verwerkingsverantwoordelijken lijkt het daarbij niet aangewezen alle verwerkingen zonder onderscheid in één globale beoordeling samen te brengen. Minstens de verwerking inzake de beschermingscode en het vertrouwelijke register, de veiligheidscontroles en registers in het kader van de gespecialiseerde afdelingen, de verwerking van psycho-medische gegevens en het identificatie- en raadplegingssysteem voor het penitentiair personeel moeten als onderscheiden of voldoende duidelijk afgebakende verwerkingsprocessen worden beoordeeld.

109. Deze beoordelingen moeten in het bijzonder aandacht besteden aan de gegevensstromen tussen de verschillende betrokken overheden, de afbakening van de respectieve toegangsrechten, het risico op ongeoorloofde koppeling of verdere verwerking, de kwaliteit en actualiteit van gegevens waarop ingrijpende beslissingen worden gebaseerd, de bescherming van gegevens afkomstig van politie- en inlichtingendiensten, de verwerking van gezondheidsgegevens, de bewaartermijnen en de gevolgen van een eventuele gegevensinbreuk. Zij moeten tevens aantonen waarom de gekozen technische en organisatorische architectuur noodzakelijk en evenredig is ten aanzien van de nagestreefde doeleinden.
110. Onverminderd de specifieke beveiligingsopmerkingen die hierboven reeds werden geformuleerd, herinnert de Autoriteit eraan dat artikel 60 WVG voor de onder titel 2 ressorterende verwerkingen passende technische en organisatorische maatregelen vereist die een op het risico afgestemd beveiligingsniveau waarborgen. Voor de verwerkingen die onder de AVG ressorteren, geldt de overeenkomstige risicogebaseerde beveiligingsverplichting van artikel 32 AVG. Gelet op de bijzondere gevoeligheid van de betrokken gegevens moet daarbij onder meer worden voorzien in een strikt op functies gebaseerd toegangsbeheer, een passende compartimentering van gegevens, beveiligde en geauthentiseerde communicatiekanalen, logging en periodieke controle van raadplegingen en bekendmakingen, alsook maatregelen die de integriteit en traceerbaarheid van de verwerkte informatie verzekeren. Waar identificatiegegevens door middel van een code of identificatienummer worden afgeschermd, moet de informatie die de koppeling met de werkelijke identiteit mogelijk maakt bovendien bijzonder worden beveiligd en slechts toegankelijk zijn voor de personen voor wie dit strikt noodzakelijk is.
111. Ten slotte herinnert de Autoriteit eraan dat artikel 59 WVG voorziet in een voorafgaande raadpleging van de bevoegde toezichthoudende autoriteit (zonder dat dit noodzakelijkerwijze de Gegevensbeschermingsautoriteit is) in de daarin bepaalde gevallen, onder meer wanneer uit de gegevensbeschermingseffectbeoordeling blijkt dat de verwerking zonder risicobeperkende maatregelen een hoog risico zou opleveren of wanneer de aard van een nieuwe verwerking, technologie, mechanisme of procedure op zichzelf een hoog risico met zich meebrengt. Voor eventuele verwerkingen die onder de AVG vallen, geldt mutatis mutandis artikel 36 AVG. De onderhavige raadpleging in het kader van de totstandkoming van de wettelijke regeling doet derhalve geen afbreuk aan een eventuele verplichting tot voorafgaande raadpleging in het licht van de concrete technische en organisatorische uitwerking van de betrokken verwerkingen.

**OM DEZE REDENEN,
de Autoriteit,**

is van oordeel dat het ontwerp moet worden aangepast teneinde:

- de terminologie inzake de bescherming van de identiteit van magistraten en griffiers aan te passen aan het feit dat sprake is van pseudonimisering en niet van anonimisering, en de individuele beoordeling van het risico, de noodzakelijkheid en de evenredigheid van de toekenning van een beschermingscode uitdrukkelijk in de wet te verankeren (punten 19 – 24);
- de persoonsgegevens die onder het begrip “identiteit” vallen nauwkeuriger af te bakenen, de deelname van bijkomende personen aan de Beschermingscommissie te beperken tot hetgeen noodzakelijk is voor de beoordeling van het concrete verzoek en de raadpleging van het volledige strafdossier slechts toe te laten wanneer de relevante stukken daartoe niet volstaan (punten 25 – 29);
- de verwerkingsverantwoordelijke(n) voor de behandeling van de verzoekschriften en het vertrouwelijke register ondubbelzinnig aan te wijzen, alsook de categorieën van persoonsgegevens die in dit register worden opgenomen wettelijk vast te stellen (punten 30 – 33);
- voor de identiteit-codekoppeling, de verzoekschriften, de beoordelingsstukken en de beslissingen passende en functioneel verantwoorde maximale bewaartermijnen vast te stellen en de toegang tot en raadpleging van de achterliggende identiteit met passende technische en organisatorische beveiligings- en loggingmaatregelen te omkaderen (punten 34 – 38);
- te verduidelijken hoe het wrakingsrecht daadwerkelijk kan worden uitgeoefend wanneer de mogelijke wrakingsgrond slechts kan worden vastgesteld na kennisname van de identiteit van de onderzoeksrechter, en het criterium van de “*concrete elementen*” dienovereenkomstig af te bakenen (punt 41);
- bij de plaatsing in en opvolging van de gespecialiseerde afdelingen te waarborgen dat onderscheid wordt gemaakt tussen feiten, vermoedens, inlichtingen en beoordelingen, dat de herkomst, actualiteit en betrouwbaarheid van de gebruikte gegevens kunnen worden beoordeeld en dat latere correcties of actualiseringen worden doorgegeven, met eerbiediging van het bijzondere regime voor gegevens afkomstig van titel 3 WVG-overheden (punten 44 en 45 – 50);
- de veiligheidscontroles van bezoekers en telefonische contactpersonen nader wettelijk te regelen, met name wat betreft de overheden of diensten die eraan kunnen bijdragen, de toepasselijke verwerkingsverantwoordelijkheid, de gegevenscategorieën en bronnen, de onderzochte veiligheidsrisico's, de informatie die aan de directeur-generaal mag worden meegedeeld en de toepasselijke bewaartermijnen (punten 51 – 55);

- te verzekeren dat de veiligheidscontroles beperkt blijven tot de voor het concrete veiligheidsrisico noodzakelijke gegevens, bij voorkeur resulteren in een doelgebonden risicobeoordeling zonder systematische doorgifte van alle onderliggende gegevens en worden herbeoordeeld wanneer de gebruikte informatie wordt gecorrigeerd, achterhaald raakt of haar relevantie verliest (punten 56 – 58);
- de inhoud en het doeleinde van de psycho-medische adviezen en andere gezondheidsgegevens nader af te bakenen, de mededeling ervan te beperken tot hetgeen strikt noodzakelijk is en de in de memorie van toelichting voorziene verdere mededeling van psychiatrische informatie aan het openbaar ministerie, indien zij wordt behouden, uitdrukkelijk wettelijk te regelen (punten 59 – 62);
- de verantwoordelijkheid voor het centrale en lokale register te verduidelijken en, in voorkomend geval, de respectieve verantwoordelijkheden van de FOD Justitie en de betrokken penitentiaire inrichting overeenkomstig hun daadwerkelijke beslissingsbevoegdheden vast te stellen (punten 63 – 64);
- de bepalingen betreffende de centrale en lokale registers onderling in overeenstemming te brengen wat betreft hun doeleinden en de daarin verwerkte gegevenscategorieën, inhoudelijke gezondheidsgegevens in beginsel buiten het operationele register te houden en de categorieën van personen en instanties die toegang tot de registers kunnen verkrijgen nauwkeuriger af te bakenen (punten 65 – 71);
- voor de onderscheiden gegevenscategorieën in deze registers passende maximale bewaartermijnen vast te stellen en te waarborgen dat voor statistische doeleinden verkregen gegevens slechts als anoniem worden beschouwd indien heridentificatie redelijkerwijs is uitgesloten (punten 72 – 74);
- de regeling inzake de beperkingen van de informatie- en toegangsrechten van gedetineerden te herwerken, zodat elke niet-mededeling berust op een concrete noodzakelijkheids- en evenredigheidsbeoordeling, waar mogelijk gedeeltelijke toegang of mededeling van de essentie van de dragende redenen wordt verzekerd en de Beroepscommissie zelfstandig over de noodzaak van de afscherming kan oordelen, onverminderd het bijzondere regime voor gegevens afkomstig van titel 3-overheden (punten 75 – 81);
- voor de identificatie van penitentiaire personeelsleden de wettelijke criteria af te bakenen op grond waarvan de werkelijke naam kan worden afgeschermd en, indien het gebruik van een alias wordt beoogd, daarvoor een uitdrukkelijke wettelijke grondslag en passende regels inzake uniciteit en traceerbaarheid te voorzien (punten 82 – 87);
- de regeling inzake de bekendmaking van de achterliggende identiteit zo uit te werken dat het begrip “wettig belang” volgens voldoende duidelijke criteria wordt beoordeeld, een objectieve en onpartijdige beoordeling wordt gewaarborgd en verzoeken van particulieren of andere betrokken personen in beginsel aan een onafhankelijke toetsing kunnen worden onderworpen;

tevens moet worden gepreciseerd welke identificatiegegevens daadwerkelijk mogen worden meegedeeld (punten 88 – 95);

- de verhouding tussen het detentiebeheersysteem en het afzonderlijke register van aanvragen te verduidelijken, voor dit laatste register de verwerkingsverantwoordelijke uitdrukkelijk vast te stellen en de daarin opgenomen gegevens aan te vullen zodat de rechtmatigheid en behandeling van een verzoek achteraf daadwerkelijk controleerbaar zijn (punten 96 – 100);
- afzonderlijke en functioneel verantwoorde bewaartermijnen vast te stellen voor het register van aanvragen, de technische loggegevens en de koppeling tussen het identificatienummer en de werkelijke identiteit van het personeelslid, waarbij in het bijzonder moet worden verantwoord wanneer een langdurige bewaring van loggegevens noodzakelijk is en de maximale termijn van dertig jaar niet als standaardtermijn mag gelden (punten 101 – 105);

De Autoriteit wijst er voorts op dat de betrokken hoogrisicoverwerkingen vóór hun operationalisering aan de vereiste gegevensbeschermingseffectbeoordelingen moeten worden onderworpen, dat bij hun concrete uitvoering passende technische en organisatorische beveiligingsmaatregelen moeten worden getroffen en dat, wanneer aan de toepasselijke voorwaarden is voldaan, de bevoegde toezichthoudende autoriteit voorafgaand moet worden geraadpleegd (punten 106 – 111).

Voor de Autorisatie- en Adviesdienst,
(get.) Alexandra Jaspar, Directeur