Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 222/2026 van 15 oktober 2026

Betreft: advies betreffende een ontwerp van wet tot wijziging van de wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's, van de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid, van de wet van 15 mei 2007 tot instelling van de functie van gemeenschapswacht, tot instelling van de dienst gemeenschapswachten en tot wijziging van artikel 119bis van de nieuwe gemeentewet en van de wet van 15 mei 2007 betreffende de civiele veiligheid teneinde het gebruik van individuele camera's mogelijk te maken (ADV-2026-00146)

Trefwoorden: Bodycams – Individuele camera's – Niet-politioneel personeel – Testfase – Machtigingen waartegen beroep kan worden aangetekend – Waarschuwing – Beperking van de rechten van de betrokkenen – Cyberveiligheid

Vertaling

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, met name de 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 de heer Bernard Quintin, minister van Veiligheid en Binnenlandse Zaken, belast met Beliris, (hierna "de aanvrager"), ontvangen op 4 september 2026;

Gelet op de aanvullende informatie, gevraagd op 17 september 2026 en ontvangen op 23 september 2026;

Enkel adviezen met betrekking tot ontwerpen en voorstellen met rang van wet die uitgaan van de federale overheid, het Brussels Hoofdstedelijk Gewest en de Gemeenschappelijke Gemeenschapscommissie worden zowel in het Nederlands als in het Frans door de Autoriteit gepubliceerd. De 'Originele versie' is de versie die gevalideerd werd.

De Autorisatie- en Adviesdienst van de Gegevensbeschermingsautoriteit (hierna "de Autoriteit"), brengt op 15 oktober 2026 het volgende advies uit:

I. VOORWERP EN CONTEXT VAN DE ADVIESAANVRAAG

1. De aanvrager heeft het advies gevraagd van de Autoriteit betreffende een ontwerp van wet tot wijziging van de wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's, van de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid, van de wet van 15 mei 2007 tot instelling van de functie van gemeenschapswacht, tot instelling van de dienst gemeenschapswachten en tot wijziging van artikel 119bis van de nieuwe gemeentewet en van de wet van 15 mei 2007 betreffende de civiele veiligheid teneinde het gebruik van individuele camera's mogelijk te maken (hierna "het ontwerp").

2. Het ontwerp heeft tot doel het regeerakkoord uit te voeren, waarin de verdere uitbreiding wordt voorzien van "*de wettelijke mogelijkheden inzake het gebruik van camera's […]*" en door ervoor te zorgen *"dat onze hulpdiensten, de openbare vervoersdiensten (De Lijn, TEC, MIVB) en treinbegeleiders op de lijnen met de meeste incidenten na een degelijke opleiding en binnen een welomlijnd kader met respect voor de privacywetgeving ook gebruik kunnen maken van 'bodycams' of toezichtcamera's"*[1].

3. Naar aanleiding van incidenten waarbij eind mei 2026 vijf medewerkers van De Lijn gewond raakten tijdens een controle in De Haan, heeft de federale regering aangekondigd dat de Ministerraad[2] een voorontwerp van wet heeft goedgekeurd tot regeling van het gebruik van bodycams (in het ontwerp en in de rest van dit advies aangeduid met de term "individuele camera's") voor de "*diensten die tijdens de uitoefening van hun opdrachten met geweld kunnen worden geconfronteerd*"[3].

4. Het ontwerp gaat echter verder dan in het regeerakkoord was aangekondigd, aangezien artikel 5 het volgende beoogt:

- de operationele diensten van de civiele bescherming;
- de bestuurders en personeelsleden van het openbaar vervoer;
- de beëdigde personeelsleden die belast zijn met de controle op en de vaststelling van overtredingen;
- het treinbegeleidingspersoneel;

---

[1] https://www.belgium.be/sites/default/files/resources/publication/files/Regeerakkoord-Bart_De_Wever_nl.pdf, p. 135

[2] Op 22 mei 2026 (https://news.belgium.be/nl/gebruik-van-bodycams-door-personeelscategorieen-die-niet-tot-de-politie-behoren)

[3] https://www.vrt.be/vrtnws/nl/2026/05/26/regering-maakt-bodycams-mogelijk-voor-personeel-van-openbaar-ver/

- de bewakingsagenten voor bewakingsactiviteiten op evenementen en vaststellingsactiviteiten; en
- de gemeenschapswachten-vaststellers.

5. Bovendien kan de Koning, bij een besluit vastgesteld na overleg in de Ministerraad, dit toepassingsgebied uitbreiden tot andere categorieën van personeelsleden die onder een overheidsinstantie vallen of die optreden in het kader van een dienst die door of voor een overheidsinstantie wordt georganiseerd. In de nota van de Ministerraad bij het ontwerp wordt bovendien vermeld dat wordt onderzocht of het mogelijk is om het dragen van individuele camera's door bewakingsagenten uit te breiden[4] naar het onthaal van ziekenhuizen, luchthavens en recreatiedomeinen.

6. Opgemerkt moet worden dat, wat de operationele diensten van de civiele bescherming betreft, het ontwerp een eerder ontwerp opvolgt[5] dat de wet van 21 februari 2024 is geworden tot wijziging van de wet van 15 mei 2007 betreffende de civiele veiligheid, om het gebruik van camera's door de operationele diensten van de civiele veiligheid te regelen, waarover de Autoriteit advies nr. 114/2023 heeft uitgebracht. **De Autoriteit verwijst naar §§ 57 en volgende[6] van dit advies voor alles wat niet uitdrukkelijk in het onderhavige advies wordt vermeld**.

---

[4] In het kader van de activiteit bedoeld in artikel 3.13°, van de wet tot regeling van de private en bijzondere veiligheid.

[5] *Parl. St.* Kamer, 16 januari 2024, 55-3769/001, 2023-2024.

[6] De Autoriteit vermeldde het volgende: "*Een norm die het gebruik van technologie op deze manier door niet-repressieve diensten toestaat, zou eerst de **legitimiteit van het** beoogde **doel** moeten aantonen. Vervolgens moet worden aangetoond dat **de maatregel noodzakelijk en evenredig is** ten aanzien van de nagestreefde doelen, naargelang de betrokken diensten en hulpverleningszones. Daartoe moet op basis van feitelijke en objectieve elementen worden aangetoond dat de beoogde verwerking van persoonsgegevens doeltreffend is om het nagestreefde doel te bereiken en dat het nagestreefde doel niet kan worden bereikt met een minder ingrijpende maatregel voor het recht op eerbiediging van de persoonlijke levenssfeer of het recht op bescherming van persoonsgegevens. Daarvoor moeten de redenen waarom andere, minder ingrijpende maatregelen (zoals het vragen om aanwezigheid van de politie, die niet alleen over de technische middelen beschikt om bewijsmateriaal te verzamelen, maar ook een proces-verbaal kan opmaken van de geconstateerde overtredingen en vooral gebruik kan maken van haar legitieme bevoegdheid om openbare macht uit te oefenen om een aanval op de hulpdiensten te voorkomen) niet volstaan om het gewenste doel te bereiken, gedetailleerd worden uiteengezet en kunnen worden aangetoond aan de hand van feitelijke en objectieve bewijzen.*

Indien de noodzaak van de verwerking van persoonsgegevens is aangetoond, moet nog worden

*aangetoond dat de verwerking evenredig is (in de strikte zin) met het beoogde doel. Een dergelijk bewijs moet gebaseerd zijn op een **objectief verslag**, dat moet worden voorgelegd voor parlementair debat. Dit verslag kan het resultaat zijn van een testfase, strikt beperkt in de tijd door de wettelijke norm die erop van toepassing is, of een buitenlands verslag.*

Ten slotte moet een norm die het gebruik van een dergelijk technisch middel regelt, zelfs voor een beperkte periode in het kader van een testfase, ook bepalen:

- *dat het gebruik van deze technische middelen facultatief moet zijn en moet worden goedgekeurd door een politieke autoriteit die bevoegd is voor het betrokken gebied, die haar toestemming kan weigeren of intrekken in geval van misbruik (met andere woorden, een autoriteit die verschilt van degene die de aanvraag doet), en waarvan de beslissing kan worden aangevochten bij de Raad van State*
- *de identiteit van de verwerkingsverantwoordelijke(n) (gezien de grote geografische verschillen, niet op federaal niveau zou moeten liggen);*

I.1. Wijziging van de wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's (hierna "camerawet");

7. De **doeleinden** van het "*gebruik*"[7] van de **individuele camera's** zoals vastgelegd in het ontwerp zijn:

- de bescherming van de veiligheid van de personeelsleden;
- de afschrikking van agressief gedrag, de de-escalatie van conflictsituaties; en
- de objectieve vaststelling van incidenten[8] die personen of goederen in gevaar kunnen brengen in een context van geweld tegen personen (art. 6)[9].

8. Artikel 6 van het ontwerp bepaalt tevens dat de individuele camera's moeten zijn uitgerust met een voorafgaande-opnamefunctie van 30 seconden en dat de activering moet worden voorafgegaan door een **mondelinge waarschuwing** "*zodra de omstandigheden het toelaten*". Er kan overigens van de waarschuwingsplicht worden afgeweken[10].

- *de regels voor activering en gebruik met bijzondere aandacht voor de noodzaak om het medisch beroepsgeheim te respecteren;*
- *de (categorieën van) gegevens die noodzakelijk zijn om de beoogde doeleinden te bereiken (met inbegrip van de identificatiegegevens van de agent die de bodycam draagt en het feit dat die agent een waarschuwing heeft gegeven);*
- *de bewaartermijn (met inbegrip van de termijn waarbinnen de wissing van de gegevens met betrekking tot een betrokkene die toegang tot zijn gegevens wenst, bijvoorbeeld in het kader van een procedure, een inbreuk vormt en de sanctie voor een dergelijke inbreuk) en de vermelding van de verplichting om de gegevens aan het einde van deze termijn definitief te wissen;*
- *de (categorieën van) betrokkenen van wie de gegevens zullen worden verwerkt (waarbij moet worden aangegeven of, bijvoorbeeld, in de context van een woordenwisseling met de agent die de camera draagt of met de politiediensten, een betrokkene kan vragen dat de camera van de hulpdiensten wordt geactiveerd en, indien negatief, wat de rechtvaardiging voor een dergelijke weigering zou kunnen zijn);*
- *de ontvangers of categorieën van ontvangers aan wie de gegevens zullen worden meegedeeld (met toepassing van een gradatieschaal die gekoppeld is aan de omvang van de aangetroffen noodsituatie);*
- *de omstandigheden waarin de gegevens zullen worden meegedeeld.*
- *in voorkomend geval, de beperking van de verplichtingen en/of rechten bedoeld in de artikelen 5, 12 t.e.m. 22 en 34 van de AVG (met dien verstande dat, zelfs in geval van gebruik voor bewijsdoeleinden, de verzamelde gegevens geen politiegegevens zijn en de verwerkingsverantwoordelijke zich dus niet kan beroepen op het geheim van het onderzoek om de toegang van de betrokkene tot zijn gegevens te beperken); alsmede*
- *de toepasselijke beveiligingsmaatregelen (waaronder de versleuteling, de automatische wissing en de registratie van de verwerkingen).*

[7] De toelichting bij artikel 6 gebruikt de term "*activering*".

[8] De toelichting bij artikel 6 verduidelijkt dat het begrip "incident" "*elke concrete situatie* [omvat] *die een risico inhoudt voor de veiligheid van personen of goederen, of die aanleiding kan geven tot spanningen of betwistingen in het kader van de interventie, met uitsluiting van gewone interacties*" en dat "*het louter vaststellen van een inbreuk, met inbegrip van inzake parkeren of controle van vervoersbewijzen, op zich geen incident* [vormt]". Daarentegen kunnen "*gedragingen die schade aan goederen kunnen veroorzaken of tot vernielingen kunnen leiden*" wel aanleiding geven tot het activeren van een individuele camera.

[9] Artikel 7 bepaalt bovendien dat "*individuele camera's* ***niet mogen worden gebruikt met het doel*** *gegevens te capteren of te verwerken die betrekking hebben op bijzondere categorieën van persoonsgegevens, zoals de raciale of etnische afkomst, de religieuze of levensbeschouwelijke overtuigingen, de politieke opvattingen, het lidmaatschap van een vakbond, de gezondheidstoestand, het seksuele leven of de seksuele geaardheid*".

[10] *Wanneer de activering:*

1° de veiligheid van de drager van de individuele camera of van de aanwezige personen in gevaar kan brengen;

2° of materieel onuitvoerbaar is gelet op het aantal aanwezige personen dat moet worden verwittigd of deze rechtstreeks in gevaar zijn of niet ten volle bij bewustzijn;

9. Artikel 8 verplicht elke bevoegde verwerkingsverantwoordelijke ertoe voor elke categorie van dragers een **register van de inschakelingen** van de individuele camera's bij te houden. In dit register worden "*automatisch of onmiddellijk na hun registratie*" de volgende gegevens gedocumenteerd:

1° de audiovisuele opnames;
2° het tijdstip en de periode van het gebruik;
3° de identificatie van de drager van de individuele camera die er gebruik van heeft gemaakt; en
4° de plaats of het traject waarvoor de gegevens bewaard zijn geweest.

10. Deze gegevens worden minimaal 30 en maximaal 90 dagen bewaard.

11. De **doeleinden** van de verwerking van de in het **register** opgenomen gegevens zijn:

1° ter staving bij het opstellen van een verslag betreffende feiten die zich voordeden bij de uitvoering van een wettelijke of reglementaire opdracht, teneinde ze over te dragen aan de interne diensten of aan de overheid die bevoegd is om die feiten op bestuurlijk of gerechtelijk gebied te verwerken met het oog op het opleggen van administratieve of gerechtelijke sancties;
2° als ondersteuning bij de opleiding of professionele begeleiding of om veiligheidsprocessen te verbeteren[11]*;*
3° voor het behandelen van de klachten met betrekking tot een interventie, een gedrag of een incident waarbij een drager van een camera of een derde betrokken is.

12. Voor de opvraging heeft geen enkele externe dienst rechtstreekse toegang tot de gegevens in het register. Nadat deze gegevens zijn opgevraagd en doorgegeven aan de in artikel 8[12] opgesomde ontvangers, voor de hierboven genoemde doeleinden, worden deze gegevens bewaard volgens de regels die gelden voor elk van de bovengenoemde procedures. De modaliteiten voor de doorgifte van de gegevens van de camera naar de server zijn niet geregeld.

3° of manifest ongepast of nutteloos is, in het bijzonder wanneer de individuele camera wordt gebruikt op een plaats zonder menselijke aanwezigheid.

[11] Op voorwaarde dat de gegevens worden geanonimiseerd, tenzij dit het beoogde doeleinde in gevaar brengt; in dat geval worden ze gepseudonimiseerd.

[12] *1° de leden van de politiediensten die de behoefte hebben om er kennis van te hebben voor de uitoefening van hun wettelijke opdrachten bepaald in de artikelen 14 en 15 van de wet op het politieambt;*

2° de administratieve overheden en interne diensten die bevoegd zijn voor het opleggen van administratieve sancties, alsook de gerechtelijke autoriteiten die handelen in het kader van de uitoefening van hun wettelijke opdrachten;

3° de overheden, diensten en personen die bevoegd zijn voor het behandelen van de klachten;

4° de leden die verantwoordelijk zijn voor de opleiding of professionele begeleiding, of de verbetering van veiligheidsprocessen en die zijn aangewezen door de verwerkingsverantwoordelijke.

13. De raadplegingen en opvragingen van gegevens of registraties worden **gelogd**. Logs worden gedurende 3 jaar bewaard.

I.2. Wijziging van de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid

14. Artikel 10 van het ontwerp wijzigt de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid, zodat **bewakingsagenten** individuele camera's mogen gebruiken bij de activiteiten van evenementenbewaking en bij de verrichting van vaststellingen.

15. Dezelfde bepaling stelt het gebruik van individuele camera's bij het uitoefenen van bewakingsactiviteiten afhankelijk van de informatie en de **formele en uitdrukkelijke toestemming** van de opdrachtgever of de beheerder van de "*bewaakte*" plaats.

16. Deze bepaling voorziet er ook in dat de verwerkingsverantwoordelijke voor de gegevens die geregistreerd zijn in het register van de inschakelingen van de individuele camera's, een werkelijke leidinggevende is van de bewakingsonderneming of interne bewakingsdienst.

17. Artikel 11 wijzigt dezelfde wet om de **veiligheidsagenten van openbare vervoersmaatschappijen** toe te laten individuele camera's te gebruiken.

I.3. Wijziging van de wet van 15 mei 2007 tot instelling van de functie van gemeenschapswacht, tot instelling van de dienst gemeenschapswachten en tot wijziging van artikel 119bis van de nieuwe gemeentewet

18. Artikel 12 van het ontwerp wijzigt de wet van 15 mei 2007 tot instelling van de functie van gemeenschapswacht, tot instelling van de dienst gemeenschapswachten en tot wijziging van artikel 119bis van de nieuwe gemeentewet, zodat **gemeenschapswachten-vaststellers** kunnen worden uitgerust[13] met individuele camera's, en wijst de gemeente (vertegenwoordigd door het gemeentebestuur) of, in voorkomend geval, de publiekrechtelijke rechtspersoon waarvan de dienst gemeenschapswachten afhangt, aan als verwerkingsverantwoordelijke.

I.4. Wijziging van de wet van 15 mei 2007 betreffende de civiele veiligheid

19. De artikelen 13 tot en met 29 wijzigen de wet van 15 mei 2007 betreffende de civiele veiligheid, zodat een personeelslid van een operationele dienst van de civiele veiligheid dat een **individuele camera**

[13] Zoals is toegestaan op grond van het nieuwe hoofdstuk IV/1 van de camerawet.

met realtime bijstand bij interventie draagt en activeert met het oorspronkelijke doel de interventie te ondersteunen[14], en geconfronteerd wordt met een situatie van agressie of een risico op agressie, deze camera ook kan gebruiken voor beschermingsdoeleinden. Krachtens het ontwerp blijft een dergelijk gebruik volledig onderworpen aan de bepalingen van de wet van 15 mei 2007 betreffende de civiele veiligheid en niet aan de camerawet.

20. In tegenstelling tot de (klassieke) individuele camera maakt de individuele camera met realtime bijstand bij interventie audiovisuele opnames en maakt de overdracht in real time of tijdens een incident van beelden, geluiden en GPS-gegevens alsook de ontvangst van audiocommunicatie (zonder gebruik te hoeven maken van de radio) mogelijk[15].

---

[14] Overeenkomstig de wijziging van de wet van 15 mei 2007 door de wet van 21 februari 2024.

[15] Artikel 15 van het ontwerp. Artikel 17 wijzigt de gebruiksdoeleinden van deze camera's (namelijk *1° het verkrijgen van een overzicht en het in kaart brengen van het interventieterrein, het evalueren van de situatie en het opvolgen van de evolutie van het incident met het oog op het beheer ervan; 2° het op een preventieve manier bewaken van het interventieterrein of bepaalde plaatsen die een bijzonder risico inhouden; 3° het herkennen van voorwerpen, lichamen of incidenten; 4° het beschermen van het personeel en 5° het maken van beelden en/of geluidsopnames in het kader van de noodplanning en het beheer van noodsituaties* (…)), zodat het doeleinde van het indienen van een klacht wordt toegevoegd en erin wordt voorzien dat de verdere verwerking van GPS-gegevens alleen is toegestaan voor het evalueren van een interventie.

Artikel 18 van het ontwerp verplicht dat bij de **aanvraag voor het gebruik** van camera's door de operationele diensten van de civiele bescherming, die door de zonecommandant of de voorzitter van het Directiecomité van de Federale Overheidsdienst Binnenlandse Zaken aan de minister van Binnenlandse Zaken of zijn afgevaardigde wordt gericht, het te gebruiken type camera en de gebruiksmodaliteiten worden voorgesteld (*De gebruiksmodaliteiten bepalen met name wanneer het dragen van de individuele camera met realtime transmissie voor bijstand bij interventie: verplicht is en of de opname van het geluid al dan niet noodzakelijk is wanneer het geluid technisch kan worden losgekoppeld van de beelden*).

Artikel 19 van het ontwerp legt de **maximale bewaartermijn** voor beelden, geluidsopnames en GPS-gegevens vast op 30 dagen vanaf het moment van opname, tenzij deze opnames "*nuttig zijn voor het onderzoek en de evaluatie van de interventies*", in welk geval ze 90 dagen mogen worden bewaard als ze afkomstig zijn van individuele bijstandscamera's en 365 dagen als ze afkomstig zijn van andere camera's. Na afloop van deze termijn voorziet het ontwerp in de anonimisering van de bewaarde opnames die bestemd zijn voor opleidings-, sensibiliserings- of informatiedoeleinden, en in de verwijdering ervan in alle andere gevallen.

Artikel 20 van het ontwerp maakt de **uitwisseling** van gegevens in real time of tijdens het incident met de politiediensten mogelijk.

Artikel 24 van het ontwerp voegt het **traject** van de camera en de identiteit van de drager toe aan de opsomming van de gegevens die in het register moeten worden opgenomen. (De Autoriteit merkt op dat vanaf artikel 23 de nummering van het commentaar bij de artikelen niet meer overeenkomt met de tekst van het ontwerp)

Artikel 25 van het ontwerp bevat dezelfde uitzonderingen als voor individuele camera's wat betreft de verplichting tot mondelinge waarschuwing bij het "gebruik" van een camera. Namelijk wanneer de waarschuwing:

1° […] de veiligheid van het personeelslid of de aanwezige personen in gevaar kan brengen;

2° […] materieel onhaalbaar is gezien het aantal aanwezige personen dat gewaarschuwd moet worden of gezien het feit dat de te waarschuwen personen in direct gevaar verkeren of buiten bewustzijn zijn;

3° […] duidelijk ongepast of nutteloos is, met name wanneer de camera wordt gebruikt op een plaats waar geen mensen aanwezig zijn.

Krachtens artikel 28 van het ontwerp zijn de **doeleinden** van het gebruik van individuele camera's met realtime bijstand bij interventie door de operationele diensten van de civiele bescherming:

1° begeleiden van het personeel teneinde de veiligheid van de interveniërende operationele personeelsleden van de civiele veiligheid en van derden die aanwezig zijn binnen de interventiezone;

2° helpen bij het verkrijgen van een overzicht van de interventiezone en helpen bij het evalueren van de situatie teneinde adequaat te interveniëren;

3° lokaliseren, indien nodig, van de interveniërende operationele personeelsleden van de civiele veiligheid via de GPS-gegevens van de individuele camera.

Bij het gebruik van een dergelijke camera voor een van de bovengenoemde doeleinden zijn echter **ook de volgende gebruiksdoeleinden toegestaan**, op voorwaarde dat er sprake is van "*feiten […] die een inbreuk op de fysieke integriteit van personeelsleden kunnen vormen, of schade aan goederen kunnen veroorzaken, of indien de situatie een, ernstig risico op escalatie naar dergelijke inbreuken inhoudt*":

II. ONDERZOEK VAN HET ONTWERP

II.1. Inleidende opmerking

21. Het formulier bij de adviesaanvraag rechtvaardigt de toepassing van een verkorte termijn van 30 dagen als volgt: "*Mm de veiligheid en het veiligheidsgevoel van de beoogde beroepsgroepen prompt te verbeteren, wordt er een advies van 30 dagen gevraagd*" en "*Na de inwerkingtreding van het ontwerp zullen de beroepsgroepen nog een operationele en gegevensbeschermingseffectbeoordeling dienen uit te voeren*".

22. De Autoriteit wil erop wijzen dat alle ontwerpen die bij haar worden ingediend in meer of mindere mate een dimensie van algemeen belang hebben en dat zij niet over voldoende middelen beschikt om alle ingediende aanvragen binnen de 30 dagen te verwerken. De Autoriteit betreurt bovendien dat, hoewel de beslissing om haar deze termijn op te leggen al was opgenomen in de nota aan de Ministerraad van 22 mei 2026, het ontwerp pas op 4 september 2026 bij haar is ingediend.

23. Dit gezegd zijnde, stelt de Autoriteit alles in het werk om haar advies zo snel mogelijk uit te brengen, maar verzoekt zij – met het oog op een doeltreffende uitoefening van haar taken – dat, indien de wetgever geen uitbreiding van haar personeelsbestand toestaat, ervoor wordt gezorgd dat zij haar adviezen binnen een termijn van 60 dagen kan uitbrengen.

II.2. Keuze van het wettelijk kader

24. De memorie van toelichting van het ontwerp stelt dat de keuze om het gebruik van individuele camera's in de camerawet op te nemen, aansluit "*bij de standpunten die de Gegevensbeschermingsautoriteit heeft ingenomen, met name in haar advies nr. 114/2023, waarin zij eraan herinnerde dat wanneer camera's worden gebruikt door hulpdiensten of gelijkaardige diensten voor het voorkomen, vaststellen of opsporen van misdrijven tegen personen of goederen deze onder het toepassingsgebied van de wet van 21 maart 2007 vallen en door deze wet moeten worden omkaderd".*

1° beschermen van de veiligheid van de personeelsleden;

2° bevorderen van de de-escalatie van conflictsituaties;

3° op objectieve wijze vaststellen van het verloop van incidenten of situaties die de veiligheid van een personeelslid in gevaar brengen of schade toebrengen aan de goederen van de operationele dienst van de civiele bescherming, met name in geval van geweld, zodat deze kunnen worden gemeld aan de bevoegde diensten.

25. **Zonder het principe van de integratie van het wettelijk kader met betrekking tot het gebruik van individuele camera's in de camerawet in twijfel te trekken**, wil de Autoriteit verduidelijken dat de §§ 11 tot en met 18 van haar voornoemde advies betrekking hadden op de bepalingen van een ontwerp dat tot doel had de camera's van de operationele diensten van de civiele bescherming[16] van het toepassingsgebied van de camerawet uit te sluiten, aangezien "*deze diensten verschillende types camera's willen kunnen gebruiken voor andere doeleinden dan alleen bewaking*"[17]. Met andere woorden, de Autoriteit wilde de aanvrager [18] uitleggen dat, als de hulpverleningszones bewakingscamera's willen installeren om hun gebouwen te beveiligen, er geen reden is om deze camera's niet onder de camerawet te laten vallen. Het gaat dus om een afzonderlijk geval van de inzet van individuele camera's.

II.3. Belang van de inmenging

26. De Autoriteit stelt vast dat de **inmenging** die voortvloeit uit de in het ontwerp voorziene gegevensverwerkingen van **bijzonder grote omvang** is, vanwege de mogelijkheid dat de individuele camera's de betrokkenen van zeer korte afstand (en dat op een hele reeks voor het publiek toegankelijke plaatsen, met inbegrip van gevoelige plaatsen en zelfs voor of, in uitzonderlijke gevallen, in de woning van de betrokkene) zowel beeld als geluid kunnen vastleggen (en dus gezichten en stemmen kunnen opnemen)[19].

27. Hoewel de bepalingen in ontwerp en de bijbehorende toelichtingen met de nodige zorgvuldigheid zijn opgesteld, in overeenstemming met het belang van de inmenging, geeft de Autoriteit hieronder aan welke **wijzigingen noodzakelijk** zijn om het niveau van voorspelbaarheid te bereiken dat het beginsel van rechtmatigheid vereist, en om te waarborgen dat de gegevensverwerking die voortvloeit uit het gebruik van individuele camera's door de betrokken diensten noodzakelijk en evenredig is.

II.4 Doeleinden van de verwerkingen van persoonsgegevens

---

[16]Namelijk de hulpverleningszones, de Brusselse Hoofdstedelijke Dienst voor Brandbestrijding en Dringende Medische Hulp (DBDMH) en de operationele eenheden van de civiele bescherming.

[17]De memorie van toelichting van het ontwerp verduidelijkte bovendien: "*De praktijk toont de moeilijkheden aan van de toepassing van deze algemene wet op de specifieke opdrachten van de operationele diensten van de civiele veiligheid, in het bijzonder wat het gebruik van mobiele camera's betreft*", zonder dat de in de praktijk ondervonden moeilijkheden in die memorie van toelichting werden genoemd.

[18] Door te zeggen dat "*de plaatsing en het gebruik van camera's voor diefstalpreventie op plaatsen waar de operationele diensten van de civiele veiligheid verwerkingsverantwoordelijke zijn, op geen enkele wijze een uitzonderingsregeling* [kan] *rechtvaardigen ten opzichte van andere scholen, ziekenhuizen, banken, enzovoort*" (§ 11).

[19]De EDPB wijst in dit verband op het volgende: "*Het intensieve gebruik van videoapparatuur heeft effect op het gedrag van burgers. Het wijdverbreide gebruik van dergelijke apparaten op allerlei gebieden van het leven zet burgers onder toenemende druk om gedragingen te vermijden die als afwijkend zouden kunnen worden gezien. De facto kunnen deze technologieën de mogelijkheden van anoniem verkeer en het anoniem gebruik van diensten beperken en in het algemeen de mogelijkheid beperken om onopgemerkt te blijven. De gevolgen hiervan voor gegevensbescherming zijn vérstrekkend*" (Richtsnoeren 03/2019 vastgesteld op 29 januari 2020, punt 1).

1) Camerawet

1.1. Doel van het gebruik van de camera's

28. Ten eerste is de Autoriteit van mening dat, in het licht van het regelen van de verwerking van persoonsgegevens, de term "*gebruik*" onvoldoende nauwkeurig is (in tegenstelling tot de term "activering", die in de toelichting bij artikel 6 van het ontwerp wordt vermeld). De Autoriteit begrijpt echter dat gegevensbescherming niet de enige zorg is van de opstellers van het ontwerp en dat het gebruik van dergelijke camera's ook geregeld moet worden. De Autoriteit beveelt daarom aan om een **onderscheid te maken tussen de redenen waarom het "*dragen*" van een individuele camera door een dienst kan worden toegestaan, en vervolgens de doeleinden vast te stellen voor het "*activeren*" van de camera door een lid van die dienst**[20].

29. Ook is de Autoriteit van mening dat het doeleinde met betrekking tot de bescherming van de **veiligheid** van "agenten" moet worden verduidelijkt, zodat het uitsluitend betrekking heeft op "***de agent die de camera draagt***".

30. Toen hem werd gevraagd naar het doeleinde van de "***objectieve vaststelling van incidenten***", gaf de afgevaardigde ambtenaar aan dat het risico op escalatie als gevolg van het activeren van een individuele camera ten behoeve van een vaststelling niet kon worden uitgesloten[21]. Hij voegt eraan toe dat dit de reden is waarom het ontwerp "*voorziet in een voorafgaande opleiding van de dragers en de waarschuwing voorafgaand aan de activering regelt, waarbij met name rekening wordt gehouden met de kwetsbaarheid van de betrokkene en de concrete omstandigheden van de interventie*". (vertaald door de Autoriteit) De Autoriteit neemt hiervan kennis, maar is van mening dat er een **hiërarchie van doeleinden** moet worden **vastgesteld** door uitdrukkelijk te bepalen dat "*het activeren van de individuele camera met het oog op de vaststelling van incidenten in geen geval mag plaatsvinden wanneer de drager niet rechtstreeks en persoonlijk het doelwit is van agressief gedrag en het activeren ervan kan leiden tot een escalatie en/of hem in gevaar kan brengen*"[22].

---

[20] Het opvallend dragen van een individuele camera kan namelijk al volstaan om de doelstellingen op het gebied van de bescherming van de veiligheid van agenten, de afschrikking van agressief gedrag en de de-escalatie van conflictsituaties te bereiken. Het louter dragen van een dergelijke camera houdt echter nog geen verwerking van persoonsgegevens in, maar moet niettemin worden geregeld, aangezien het dragen een activering en daarmee een inmenging in de rechten en vrijheden van de betrokkenen mogelijk maakt. Omgekeerd kan het doeleinde van de objectieve vaststelling van incidenten alleen worden gerealiseerd in combinatie met het activeren van deze camera's.

[21] De afgevaardigde ambtenaar verwijst in dit verband naar het jaarverslag van het Vast Comité P waarin "*wordt opgemerkt dat hoe de activering van de bodycam wordt aangekondigd, kan leiden tot een de-escalatie of, integendeel, een escalatie van geweld, en wordt benadrukt dat net om die reden een passende opleiding belangrijk is, met name op het gebied van communicatie*" (Vast Comité P, Jaarverslag 2021, blz. 71).

[22] Met andere woorden is de Autoriteit van mening dat het faciliteren van de bestraffing van schade aan goederen in geen geval een rechtvaardiging kan vormen voor de verwerking van persoonsgegevens die een hulpverlener in gevaar kan brengen.

31. Ook het **"*objectieve*" karakter van de vaststellingen** roept vragen op. Toen hem werd gevraagd of het gebruik van deze term relevant is, gaf de afgevaardigde ambtenaar aan dat het begrip "*objectivering*" inhoudt dat "*er sprake is van een continue opname die niet door de betrokken agent kan worden gewijzigd, waardoor het feitelijke verloop van de interventie zo volledig mogelijk kan worden gedocumenteerd*"[23]. (vertaald door de Autoriteit)

32. De Autoriteit is van mening dat de betekenis die de opstellers van het ontwerp aan de term "*objectief*" toekennen, aanvaardbaar is. Om echter te voorkomen dat de term "*doelstelling*" zo wordt geïnterpreteerd dat hiermee een grotere bewijskracht wordt toegekend aan een opname gemaakt door een individuele camera, in vergelijking met een opname – die niet is bewerkt, gemonteerd[24], – gemaakt door een derde, terwijl in dat geval alleen de invalshoek van de opname zou verschillen, is de Autoriteit van mening dat in het ontwerp moet worden **vermeld dat voor het doeleinde van vaststelling van incidenten de term "*objectief*" inhoudt dat de opnames die door de individuele camera worden gemaakt, zowel bedoeld zijn om de gefilmde personen te beschermen tegen mogelijk misbruik door de dragers als om de dragers te beschermen tegen het indienen van ongegronde klachten**. De Autoriteit is bovendien van mening dat de toelichting bij het betrokken artikel rekening zou moeten houden met het feit dat uit verschillende onderzoeken is gebleken dat er **vooringenomenheid** bestaat die ertoe kan leiden dat bepaald gedrag ten onrechte als agressief wordt geïnterpreteerd[25].

33. Artikel 7 van het ontwerp voegt toe dat individuele camera's **niet kunnen worden gebruikt**:
    - voor biometrische authenticatie of identificatie, het automatisch herkennen van emoties of biometrische categorisering; noch
    - **met als doel** gegevens te verzamelen of te verwerken die betrekking hebben op de raciale of etnische afkomst van een persoon, zijn religieuze of levensbeschouwelijke overtuigingen,

---

[23] De afgevaardigde ambtenaar haalt het voorbeeld aan van het jaarverslag 2023 van het Vast Comité P, waarin "*wordt vermeld dat van de 16 in 2023 afgesloten klachten waarin naar een bodycam werd verwezen, uit de analyse van de beelden in negen gevallen kon worden geconcludeerd dat er geen sprake was van een tekortkoming bij de betrokken politieagenten. Het Comité P stelt bovendien vast dat de beelden klaarheid hebben gebracht over de wijze waarop de interventies zijn verlopen en dat men zich bij gebrek aan beelden niet had kunnen uitspreken over het al dan niet bestaan van een tekortkoming.*" De afgevaardigde ambtenaar voegt hieraan toe dat "*de ervaring leert dat de filmpjes die op sociale media worden verspreid, doorgaans slechts een deel van een interactie of een incident laten zien. Ze vloeien bovendien voort uit een selectie van beelden die tot gevolg kan hebben dat een bepaald verhaal wordt ondersteund, in plaats van dat het volledige verloop van de gebeurtenissen wordt weergegeven.*" De opname die met een bodycam is gemaakt kan daarentegen "*niet worden verwerkt, gemanipuleerd of bewerkt door de agent die de opname maakt. Hiermee kunnen de interactie en het verloop van het incident van begin tot eind continu worden gedocumenteerd.*" (vertaald door de Autoriteit)

[24] Zoals hieronder zal worden toegelicht (met betrekking tot bijzondere categorieën van gegevens en de uitoefening van de rechten van de betrokkenen), vormt de mogelijkheid dat de verwerkingsverantwoordelijke of zelfs de camerasoftware (maar niet de drager) de opname kan bewerken, echter een essentiële waarborg voor de daadwerkelijke toepassing van het beginsel van minimale gegevensverwerking. Deze bewerkingsmogelijkheid moet dus uitdrukkelijk in het ontwerp worden opgenomen.

[25] Zie bijvoorbeeld Paul B. Hutchings, Geoffrey Haddock, Look Black in anger: The role of implicit prejudice in the categorization and perceived emotional intensity of racially ambiguous faces, Journal of Experimental Social Psychology, Volume 44, Issue 5, 2008, Pages 1418-1420, ISSN 0022-1031, https://doi.org/10.1016/j.jesp.2008.05.002 (https://www.sciencedirect.com/science/article/pii/S0022103108000772)

zijn politieke opvattingen, zijn lidmaatschap van een vakbond, zijn gezondheidstoestand, zijn seksuele leven of zijn seksuele geaardheid".

34. De Autoriteit staat positief tegenover deze verboden. De Autoriteit is echter van mening dat **de verwijzing naar slechts één doel ("*met als doel*") moet worden vermeden**. Daarentegen zou het aanvaardbaar kunnen zijn om een verbod in te voeren op het activeren van de video- en/of audio-opname van de camera's zoals bedoeld in het ontwerp "*in omstandigheden waarin het verzamelen van beelden en geluiden die bijzondere categorieën van gegevens in de zin van artikel 9 van de AVG bevatten, mogelijk is, zonder dat kan worden aangetoond dat deze inschakeling noodzakelijk is*"[26]. Een dergelijke formulering biedt namelijk het voordeel dat zij de drager houvast biedt bij de toepassing van het beginsel van minimale gegevensverwerking (ondanks het feit dat van hem uiteraard niet kan worden verwacht dat hij controle heeft over de uitspraken of het gedrag van de betrokkene tijdens het incident) en de verwerkingsverantwoordelijke wat betreft het verbod op hergebruik van de (niet-geanonimiseerde) beelden voor andere doeleinden dan die welke de activering van de camera rechtvaardigden.

35. Het spreekt vanzelf dat, zelfs als de individuele camera's alleen in volkomen gepaste situaties worden geactiveerd, het onmogelijk zal zijn om volledig te voorkomen dat bepaalde categorieën van gegevens worden verwerkt[27]. Ondanks de verplichting die rust op de verwerkingsverantwoordelijke om de beginselen van minimale gegevensverwerking[28] en gegevensbescherming door ontwerp[29] na te leven, is de Autoriteit van mening dat **het ontwerp de volgende minimumvereisten moet bevatten**:

- de back-endsoftware[30] moet standaard beschikken over een functie voor het automatisch bewerken van beeld en geluid[31] waarmee delen van de opnames op doeltreffende en efficiënte wijze kunnen worden vervaagd of gemaskeerd om de rechten en vrijheden van de betrokkenen te beschermen;
- (tenzij er een absoluut verbod wordt ingesteld op het activeren van een individuele camera op gevoelige plaatsen[32]) mag het inschakelen van een camera om personen te filmen op

---

[26] Zie in die zin ICO guidance on Body Worn Video (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/additional-considerations-for-technologies-other-than-cctv/body-worn-video-bwv/)

[27] Dit geldt met name voor de operationele diensten van de civiele bescherming, die mogelijk moeten tussenkomen bij medische noodsituaties of woningen moeten betreden. Maar ook de andere potentiële dragers kunnen dergelijke gegevens verwerken, bijvoorbeeld indien de gefilmde persoon kleding draagt in de kleuren van zijn vakbond.

[28] Artikel 5.1.c) van de AVG.

[29] Wat het bewaren betreft, wordt uitsluitend verwezen naar het nieuwe artikel 13/7 van de wet betreffende de civiele veiligheid.

[30] Geïnstalleerd op de server waarop de verwerking van de opnames plaatsvindt.

[31] Het gaat om een technologie die al lang in gebruik is (zie https://www.ojp.gov/pdffiles1/nij/grants/250381.pdf) en die verplicht is in landen die vooroplopen op het gebied van het gebruik van individuele camera's (zie https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/additional-considerations-for-technologies-other-than-cctv/body-worn-video-bwv/).

[32] Dat in het ontwerp moet worden vastgelegd.

gevoelige locaties, zoals in een woning[33], een school of in de patiëntenruimte (achterin) van een voertuig van de medische hulpdiensten, op initiatief van de drager alleen plaatsvinden in geval van aantoonbare absolute noodzaak (dat wil zeggen in geval van ernstig en dreigend gevaar voor zijn veiligheid of, voor zover het inschakelen van een camera een aantoonbaar positief effect kan hebben, die van derden), en er mag nooit worden afgeweken van de verplichting tot voorafgaande informatie, MAAR indien de gefilmde persoon hierom verzoekt, moet de camera verplicht worden ingeschakeld;

1.2. Doelstellingen van de verwerkingen van de gegevens uit het register "van de inschakelingen"[34]

36. Uit artikel 8 van het ontwerp blijkt dat het register van de inschakelingen niet mag worden verward met een register van de verwerkingen, noch met een logboek. Het gaat hier namelijk om de **gegevensbank waarin de audiovisuele opnames zullen worden opgeslagen**. Dit houdt in dat de doeleinden van de opname en de verdere verwerking van de gegevens in het register niet beantwoorden aan een behoefte aan bescherming van de dragers, maar aan bestraffing (van het gedrag van derden of van de dragers) en aan educatieve ondersteuning.

37. De Autoriteit is uiteraard van mening dat deze doeleinden gerechtvaardigd zijn. Wat de evenredigheid betreft, kunnen deze echter **geen rechtvaardiging vormen voor een inmenging die zo vergaand is als de doeleinden die verband houden met de bescherming van de lichamelijke integriteit van de betrokkenen**[35]. Het beginsel van minimale gegevensverwerking zal dus strikter moeten worden toegepast (bijvoorbeeld automatische wissing na 30 dagen en het bewerken van de opname[36]). Dit geldt in het bijzonder voor het doeleinde van ondersteuning van opleidingen (waarbij de verwerking van gepseudonimiseerde gegevens alleen mag plaatsvinden wanneer de opnames absoluut noodzakelijk zijn om dit doeleinde te bereiken en het gebruik van correct geanonimiseerde gegevens[37] niet volstaat om het beoogde doel te bereiken).

---

[33] Dit zal vooral betrekking hebben op de medewerkers van de operationele diensten van de civiele bescherming.

[34] Ter herinnering, krachtens artikel 8 van het ontwerp zijn deze doeleinden:

1° ter staving bij het opstellen van een verslag betreffende feiten die zich voordeden bij de uitvoering van een wettelijke of reglementaire opdracht, teneinde ze over te dragen aan de interne diensten of aan de overheid die bevoegd is om die feiten op bestuurlijk of gerechtelijk gebied te verwerken met het oog op het opleggen van administratieve of gerechtelijke sancties;

2° als ondersteuning bij de opleiding of professionele begeleiding of om veiligheidsprocessen te verbeteren;

3° voor het behandelen van de klachten met betrekking tot een interventie, een gedrag of een incident waarbij een drager van een camera of een derde betrokken is.

[35] Over deze kwestie, zie *infra*.

[36] Deze voorbeelden worden hieronder nader toegelicht.

[37] De Autoriteit maakt van deze gelegenheid gebruik om de aandacht te vestigen op de goedkeuring door de EDPB van Richtsnoeren nr. 02/2026 op 7 juli 2026 (https://www.edpb.europa.eu/system/files_en?file=2026-09/edpb_guidelines_202602_anonymisation_v1_en_0.pdf)

38. Bovendien bevestigt dit dat in bepaalde gevallen het louter dragen van een individuele camera of de "*dreiging*" deze te activeren al voldoende kan zijn om de doelstellingen van het beschermen van de veiligheid van de agenten en de de-escalatie te bereiken. Bij de opleiding van de dragers moet hiermee rekening worden gehouden. Rekening houdend met deze elementen is de Autoriteit van mening dat **het ontwerp moet bepalen dat "*de dragers moeten worden opgeleid om hun camera's niet in te schakelen wanneer een voorafgaande waarschuwing heeft geleid tot het bereiken van het doel van de-escalatie van het conflict*".** (vertaald door de Autoriteit)

2) Civiele veiligheid

39. De wet betreffende de civiele veiligheid betreft een specifiek type camera's[38] dat mogelijk een verhoogd risico op inmenging met zich meebrengt vanwege de mogelijkheid om opnames in real time[39] door te sturen, alsook vanwege de eigen doeleinden[40] (die dit risico enigszins temperen), aangezien deze camera's slechts bijkomstig[41] ook kunnen worden gebruikt ter bescherming van de drager.

40. Wat de doeleinden van de verwerking van **GPS-gegevens** betreft, is de Autoriteit van mening dat in het ontwerp een duidelijker onderscheid moet worden gemaakt tussen de doeleinden die een realtime-doorgifte (of toegang) niet kunnen rechtvaardigen en de doeleinden die dat wel kunnen rechtvaardigen.

41. De Autoriteit voegt in dit verband toe dat moet worden **gerechtvaardigd waarom het noodzakelijk is dat deze geolocatiegegevens worden verzameld**[42] en vooral (in real time) **via de camera worden doorgegeven**. Gelet op de omvang van een camera en de manier waarop deze wordt gedragen, is het risico op beschadiging of verlies van de camera veel groter dan het risico op verlies van een GPS-tracker die in de dienstkleding is ingebouwd. De verwerking van de GPS-gegevens die via een individuele camera zijn verzameld, zou dan ook mogelijk niet het doel dienen om de locatie

---

[38] De "*individuele camera's voor realtime ondersteuning bij interventies".*

[39] Aan de personen bedoeld in artikel 13/8, § 1, van de wet betreffende de civiele veiligheid, zijnde:

1° de personeelsleden van de operationele diensten van de civiele veiligheid;

2° de verschillende disciplines, overlegorganen en coördinatiestructuren;

3° de personen die voor de uitoefening van hun taken een meldkamer delen met het personeel van de operationele diensten van de civiele veiligheid en voor wie het noodzakelijk is er kennis van te nemen;

4° de personen, andere dan de personen, die omwille van hun bijzondere kennis of expertise die noodzakelijk is voor de interventie worden uitgenodigd in de overlegorganen of coördinatiestructuren.

[40] *1° het verkrijgen van een overzicht en het in kaart brengen van het interventieterrein, het evalueren van de situatie en het opvolgen van de evolutie van het incident met het oog op het beheer ervan;*

2° het op een preventieve manier bewaken van het interventieterrein of bepaalde plaatsen die een bijzonder risico inhouden;

3° het herkennen van voorwerpen, lichamen of incidenten;

[41] Wanneer een medewerker van een operationele dienst van de civiele veiligheid "*wordt geconfronteerd met een situatie van agressie of een risico op agressie*" (toelichting bij artikel 14 van het ontwerp).

[42] De verzameling kan het mogelijk maken om de metagegevens betreffende locatie aan de opname te koppelen (en zo te controleren of de medewerker zich daadwerkelijk bevond waar hij beweerde te zijn en of hij het recht had om daar te zijn).

van het personeel tijdens een interventie te bepalen. Erger nog, de verwerking van deze gegevens zou het personeel dat ter plaatse is in gevaar kunnen brengen (bijvoorbeeld als de hulpdiensten die worden gestuurd om een collega in gevaar te helpen, worden geleid naar de plek waar de camera werd uitgeschakeld en niet naar de plek waar de persoon zich daadwerkelijk bevindt).

42. Bij de aanpassing van het ontwerp op dit punt vraagt de Autoriteit de aanvrager er rekening mee te houden dat het feit dat er technologie bestaat waarmee de GPS-functionaliteit in bepaalde cameramodellen kan worden geïntegreerd, geen aanvaardbare rechtvaardiging vormt. De bestekken moeten namelijk worden opgesteld op basis van de wetgeving en niet op basis van de kenmerken van een product waarvan men op de hoogte zou zijn.

43. Bovendien moet worden bepaald dat de communicatie in real time **door de drager moet kunnen worden in- en uitgeschakeld** (net zoals de functies voor het opnemen van beeld en geluid door de camera's afzonderlijk van elkaar moeten kunnen worden in- en uitgeschakeld)[43].

II.5. Noodzakelijkheid en evenredigheid van de maatregel

44. De memorie van toelichting van het ontwerp rechtvaardigt de noodzaak om het dragen van individuele camera's toe te staan met het argument dat personeelsleden "*die geen deel uitmaken van de politiediensten*, [optreden] *in gevoelige contexten die soms gepaard gaan met aanzienlijke spanningen. Ter illustratie kunnen bepaalde interventies van hulpdiensten, zoals de brandweer, verstoord worden door vijandig gedrag dat zowel gericht is tegen de interveniënten zelf als tegen hun interventiemiddelen, met inbegrip van de voertuigen*".

45. Op de vraag of de maatregel in ontwerp was gebaseerd op wetenschappelijke studies die een correlatie aantonen tussen het dragen van individuele camera's en de de-escalatie van spanningen, verduidelijkte de afgevaardigde ambtenaar dat er in het kader van de uitwerking van het onderhavige ontwerp geen specifiek onderzoek was opgestart. De afgevaardigde ambtenaar verwijst naar een in Nederland uitgevoerd onderzoek[44] waaruit blijkt dat "*het gebruik van bodycams een de-escalerend effect kan hebben op geweld tegen politieambtenaren*" en voegt eraan toe dat individuele camera's slechts een van de instrumenten zijn binnen een reeks preventieve maatregelen, die in combinatie een passend antwoord kunnen bieden op situaties van spanning of agressie[45].

---

[43] Onverminderd de noodzaak om het inschakelen (en meer in het algemeen het gebruik) van individuele camera's te reguleren via een bindende procedure (naar het voorbeeld van wat er in het Verenigd Koninkrijk bestaat: https://assets.publishing.service.gov.uk/media/5bb769f6ed915d23b3cabd20/safeguarding-body-worn-video-data-01118p.pdf) zodat de beslissing om de camera in te schakelen niet naar eigen goeddunken door de drager kan worden genomen.

[44] Evaluatie bodycams Landelijke Eenheid; proeftuin bodycams Dienst Infrastructuur 2018, Sdu Uitgevers, Den Haag; Politie & Wetenschap, Den Haag; Sander Flight, Amsterdam.

[45] "*De auteurs benadrukken echter dat de individuele camera alleen geen oplossing biedt voor situaties van spanning of agressie. De camera moet worden beschouwd als een hulpmiddel dat deel uitmaakt van een breder pakket aan maatregelen op het*

46. De Autoriteit stelt echter vast dat de methodologie van de aangehaalde studie niet toelaat om een daadwerkelijk causaal verband aan te tonen tussen het dragen van individuele camera's en de afname van geweld[46]. Andere studies lijken overigens het bestaan van een dergelijk oorzakelijk verband[47] te betwisten of vermoeden zelfs een omgekeerd effect[48].

47. De Autoriteit besluit daaruit dat in dit stadium onvoldoende is aangetoond dat de uitbreiding van de mogelijkheid om bodycams te dragen naar niet-politionele diensten noodzakelijk en evenredig is. De Autoriteit geeft echter toe **dat voor het leveren van dit bewijs wellicht een testfase moet worden doorlopen.** In dit verband staat de Autoriteit positief tegenover het feit dat in de memorie van toelichting wordt verduidelijkt dat de invoering van de individuele camera's kan beginnen "*met proefprojecten ("proofs of concept"), die toelaten de gebruiksmodaliteiten te valideren, de effecten ervan op het terrein te evalueren en na te gaan of het systeem daadwerkelijk beantwoordt aan de beoogde doelstellingen, alvorens eventueel tot een ruimere uitrol over te gaan*", en dat artikel 30 van het ontwerp voorziet in een evaluatie en het opstellen van een verslag dat "*ten minste een kwantitatief overzicht* [bevat] *van de inzet van individuele camera's binnen de verscheidene personeelscategorieën, alsmede een kwalitatieve evaluatie van het gebruik van individuele bewakingscamera's en een overzicht van de procedurele moeilijkheden die de toepassing van deze wet heeft veroorzaakt*".

48. Aangezien de in artikel 30 van het ontwerp voorziene evaluatie echter niet onafhankelijk zal zijn en pas na vier jaar zal plaatsvinden, vormt deze geen voldoende tussenoplossing om het evenredige karakter van de maatregel te waarborgen.

49. **De Autoriteit is van mening dat de evenredigheid van de maatregel gewaarborgd zou zijn indien het ontwerp het volgende zou bevatten:**

    - een **opheffingsbepaling** waarin wordt voorzien in de opheffing van alle bepalingen in ontwerp **twee jaar** na de inwerkingtreding van de wet (deze termijn kan worden benut om

---

gebied van preventie, opleiding en conflictbeheersing. De combinatie van deze verschillende instrumenten, aangepast aan de concrete omstandigheden, kan een passend antwoord bieden."

[46] *De bodycams zijn niet willekeurig verdeeld over een experimentele groep en een controlegroep. Er zijn om die reden ook geen enquêtes gehouden in een controlegroep* (punt 3.2, p. 20)

[47] National Institute of Justice, "Research on Body-Worn Cameras and Law Enforcement," January 7, 2022, nij.ojp.gov: https://nij.ojp.gov/topics/articles/research-body-worn-cameras-and-law-enforcement

[48] Ariel, B., Sutherland, A., Henstock, D., Young, J., Drover, P., Sykes, J., Megicks, S., & Henderson, R. (2016). Wearing body cameras increases assaults against officers and does not reduce police use of force: Results from a global multi-site experiment. *European Journal of Criminology*, *13*(6), 744-755. https://doi.org/10.1177/1477370816643734; Ariel, B., Sutherland, A., Henstock, D. *et al.* Report: increases in police use of force in the presence of body-worn cameras are driven by officer discretion: a protocol-based subgroup analysis of ten randomized experiments. *J Exp Criminol* 12, 453–463 (2016). https://doi.org/10.1007/s11292-016-9261-3

de conclusies van een onafhankelijk verslag te beoordelen en, indien nodig, bepaalde bepalingen aan te passen en, indien nodig, de opheffingsbepaling zelf op te heffen); en

- een slotbepaling die een **onafhankelijke (universitaire) studie oplegt**[49], waarvan de conclusies aan de bevoegde minister van Veiligheid en Binnenlandse Zaken EN aan de Kamer van volksvertegenwoordigers moeten worden voorgelegd alvorens de opheffingsbepaling wordt gewijzigd;

50. Bovendien, wat betreft de vaststelling van de **personen die in aanmerking komen voor een machtiging om individuele camera's te dragen**, heeft de afgevaardigde ambtenaar verduidelijkt dat deze personen, naast het behoren tot een van de categorieën van personeelsleden en het uitoefenen van een van de in het ontwerp genoemde taken, tijdens de uitoefening van die taken in contact moeten staan met het publiek EN objectief gezien en herhaaldelijk[50] moeten worden blootgesteld aan situaties van spanning, agressie of verzet tegen hun interventie. De onafhankelijke evaluatie moet dan ook de mogelijkheid bieden om (op een onafhankelijke en wetenschappelijke manier), in functie van de betrokken dienst, de **herhaalde blootstelling** aan situaties van spanning, agressie of verzet tegen categorieën van dragers zoals bedoeld in het ontwerp te **objectiveren**.

51. Om ervoor te zorgen dat alleen die diensten worden aangewezen waarvoor een behoefte is aangetoond, en vooral om de maatregel te beëindigen wanneer de behoefte verdwijnt of wanneer niet aan de voorwaarden wordt voldaan of niet worden nageleefd, is de Autoriteit van mening dat het ontwerp **de Koning** zou kunnen **machtigen om "[periodiek]**, *na verificatie van de operationele behoefte en de naleving van de voorwaarden*[51]*,* ***de lijst vast te stellen van de verwerkingsverantwoordelijken***[52] ***die bevoegd zijn om hun personeelsleden uit te rusten met individuele camera's"*** (tot de vaststelling van het besluit dat geldig is voor de volgende periode). (vertaald door de Autoriteit) De Autoriteit is namelijk van mening dat de vereiste van een operationele analyse (die van nature zeer ondoorzichtig is) volstrekt ontoereikend is en ertoe kan leiden dat de diensten van de minister van Veiligheid en Binnenlandse Zaken worden vrijgesteld van elke controleplicht en elke verantwoordelijkheid.

---

[49] De Autoriteit preciseert dat van deze eis in geen geval mag worden afgeweken omwille van budgettaire redenen. Het Hof van Justitie van de Europese Unie is namelijk van oordeel "*dat de omstandigheid dat aan overheidsinstanties te weinig middelen worden toegekend, **in geen geval** een legitieme reden kan vormen die vermag te rechtvaardigen dat inbreuk wordt gemaakt op de door het Handvest gewaarborgde grondrechten*" (HvJ-EU, 1 augustus 2022, C-184/20, OT tegen Vyriausioji tarnybinės etikos komisija, punt 89)

[50] *Het feit dat zij objectief gezien en herhaaldelijk worden blootgesteld aan situaties van spanning, agressie of verzet tegen hun interventie, blijkt met name uit de operationele risicoanalyse. De operationele analyse beoordeelt de concrete toegevoegde waarde van het gebruik van individuele camera's bij de uitvoering van taken, door na te gaan in welke situaties deze daadwerkelijk bijdragen aan het vergroten van de veiligheid van de personeelsleden, het bevorderen van de-escalatie in conflictsituaties of het objectiveren van het verloop van incidenten.*

[51] Door middel van evaluaties en audits.

[52] Zoals hieronder zal worden toegelicht met betrekking tot de veiligheidsmaatregelen (en hun kosten), vormt een machtiging die specifiek betrekking heeft op de betrokken bewakingsondernemingen een essentiële waarborg.

II.6. Machtiging

52. Het nieuwe artikel 12/1, § 2, in ontwerp, van de camerawet bepaalt dat het aan de verwerkingsverantwoordelijke is om, op basis van de operationele analyse en de gegevensbeschermingseffectbeoordeling en met inachtneming van de toepasselijke overlegmechanismen, het dragen van individuele camera's toe te staan.

53. Gevraagd naar dit onderwerp verduidelijkt de afgevaardigde ambtenaar dat dit verschil met de regeling voor vaste bewakingscamera's in openbare ruimtes te verklaren is door de aard van het systeem[53].

54. De Autoriteit neemt kennis van het argument, maar stelt allereerst vast dat een machtigingsregeling is voorzien voor de operationele diensten van de civiele bescherming. Vervolgens wijst de Autoriteit erop dat **individuele camera's**, vanwege de mogelijkheid om op zeer korte afstand spraak- en beeldgegevens van betrokkenen vast te leggen (op allerlei voor het publiek toegankelijke plaatsen en zelfs vóór of, in uitzonderlijke gevallen, in de woning van de betrokkene), **een nog veel groter risico op inbreuk op de privacy van de betrokkenen inhouden dan vaste camera's**. Bovendien is de beslissing van de verwerkingsverantwoordelijken **onvoldoende transparant** en **beperkt** zij daardoor **de mogelijkheid** om tegen deze beslissing **in beroep te gaan**.

55. Hieruit volgt volgens de Autoriteit dat de opmerkingen die professor De Hert in 2006 heeft geformuleerd - en die ertoe hebben geleid dat de beslissing om bewakingscamera's te installeren werd onderworpen aan een positief advies van de gemeenteraad van de gemeente waar de plaats zich bevindt (art. 5, § 2, van de camerawet)[54] - in dit geval nog steeds volledig relevant zijn.

56. Dat gezegd zijnde, begrijpt de Autoriteit dat het in dit geval onnodig complex en zelfs contraproductief zou kunnen zijn voor de transparantie om een positief advies te eisen van de gemeenteraden van alle

---

[53] *De individuele camera is niet geïnstalleerd om een bepaalde plaats te bewaken: het is een hulpmiddel dat verband houdt met de uitvoering van een opdracht en dat de drager ervan bijstaat bij de uitvoering daarvan. Er is dan ook geen reden om het gebruik ervan afhankelijk te maken van een machtiging die verband houdt met de plaats waar de opdracht wordt uitgevoerd.*

[54] Zijnde: "*Het zou echter een goed idee zijn de gemeenten de verantwoordelijkheid en de mogelijkheid te laten bij misbruik op te treden. Dat vereist geen heel zware procedure. Op die manier kunnen de plaatselijke autoriteiten betrokken worden bij de controle op de camera's die op hun grondgebied geïnstalleerd zijn* (…). *Hij stelt daarentegen wel voor dat het publieke aspect een publieke verantwoordelijkheid wordt. Wanneer gemeenten een veiligheidsbeleid voeren, is dat een recht dat bij de Raad van State moet kunnen worden betwist.*

De Raad van State heeft in het verleden bewezen het ideale instrument te zijn om het juiste evenwicht te vinden tussen het recht op veiligheid en de fundamentele rechten. Hij meent dus dat het democratische middel om alle op het spel staande belangen in evenwicht te houden al bestaat.

Ideaal voor hem zou dus zijn hetzij een centraliserende reglementering te overwegen die de FOD Binnenlandse Zaken de macht van scheidsrechter geeft, hetzij de burgers de mogelijkheid te geven bij de Raad van State in beroep te gaan wanneer ze menen dat een camerabewakingssysteem dat door een overheid geïnstalleerd werd, hun rechten met voeten treedt." (Parl. St. Senaat, 28 april 2006, 3-1413/1, 2005-2006, blz. 83 (https://www.senate.be/www/webdriver?MItabObj=pdf&MIcolObj=pdf&MInamObj=pdfid&MItypeObj=application/pdf&MIvalObj=50334894).

gemeenten waar deze diensten hun taken kunnen uitoefenen. Daarom is de Autoriteit - zoals hierboven aangegeven - van mening dat het wenselijk is **de Koning te machtigen om "[periodiek]**, *na verificatie van de operationele behoefte en de naleving van de voorwaarden*[55]*,* ***de lijst vast te stellen van de verwerkingsverantwoordelijken die bevoegd zijn om hun personeelsleden uit te rusten met individuele camera's"***.

57. Het is in ieder geval onaanvaardbaar dat - zoals het ontwerp bepaalt voor de operationele eenheden van de civiele bescherming[56] - de machtigingsaanvraag kan worden gericht aan een **afgevaardigde van de minister**. Deze formulering kan namelijk zo worden geïnterpreteerd dat de verwerkingsverantwoordelijke een machtigingsaanvraag aan zichzelf kan richten.

II.7. Regels voor activering en gebruik

58. De Autoriteit staat positief tegenover de verduidelijking (die op verschillende plaatsen in de memorie van toelichting wordt herhaald): de activering van de camera "*mag in geen geval leiden tot een continue opname van beeld en geluid gedurende de volledige duur van een opdracht of dienst*. *Deze beperking vloeit voort uit de aard zelf van de individuele camera, dat een instrument is dat bedoeld is om te worden gebruikt in het kader van specifieke interventies en niet als middel voor <u>permanente</u> bewaking van de openbare ruimte of van personen"*.

59. De Autoriteit is echter van mening dat de term "*permanent*" moet worden geschrapt[57]. **De bewaking (zelfs tijdelijk) van de openbare ruimte of van personen is** namelijk **niet verenigbaar met de in het ontwerp genoemde doelstellingen**.

60. Bovendien, is de Autoriteit van mening dat de opstellers van het ontwerp zouden moeten overwegen om **bepaalde plaatsen op te sommen waar de individuele camera's alleen op verzoek van de betrokkene mogen worden geactiveerd** (bijvoorbeeld privéruimtes of gevoelige plaatsen[58], voor dragers die mogelijk toegang hebben tot dergelijke plaatsen[59]) en de personen die, voor zover mogelijk, beter niet gefilmd worden (zeer jonge kinderen, geredde slachtoffers[60], enz.). De Autoriteit is niet van mening dat een verbod noodzakelijkerwijs betrekking moet hebben op alle hierboven als voorbeeld genoemde plaatsen en personen, maar is van oordeel dat **het noodzakelijke en evenredige karakter van het activeren van een individuele camera op deze plaatsen of ten**

[55] Door middel van evaluaties en audits.

[56] In het nieuwe artikel 12/1, § 2, *in fine* van de camerawet.

[57] Uit de laatste zin van de paragraaf.

[58]

[59] Zoals de operationele diensten van de civiele bescherming;

[60] Bijvoorbeeld het slachtoffer dat de interventie van de operationele diensten van de civiele bescherming rechtvaardigt.

aanzien van deze categorieën van personen op zijn minst met bijzondere zorgvuldigheid moet worden aangetoond in de toelichting bij de artikelen van het ontwerp. Merk op dat zou kunnen worden bepaald dat het advies van de gemeenteraden (zoals hierboven aanbevolen) ook op dit aspect betrekking heeft.

61. De Autoriteit staat eveneens positief tegenover de verplichting om de activering van een individuele camera te laten voorafgaan door een mondelinge **waarschuwing**[61]. Zij is echter van mening dat de **uitzonderingen**[62] op deze regel **te algemeen zijn geformuleerd**. De Autoriteit geeft natuurlijk toe dat "*de veiligheid van de drager van de individuele camera of van de aanwezigen*" een belangrijke en gerechtvaardigde zorg is. Er zijn echter omstandigheden waarin juist de activering een gevaar kan vormen voor "*de veiligheid van de drager van de individuele camera of van de aanwezigen*"[63]. Daarom moet ook worden bepaald dat "*de individuele camera niet mag worden geactiveerd wanneer dit de veiligheid van de drager in gevaar kan brengen*".

62. Wat betreft de **onuitvoerbaarheid die wordt gerechtvaardigd door het aantal personen dat moet worden gewaarschuwd**, is de Autoriteit van mening dat er rekening moet worden gehouden met het feit dat de waarschuwing op zichzelf al een de-escalerend effect kan hebben en dat het aantal te waarschuwen personen de drager niet mag ontslaan van de plicht om de activering op een zodanige wijze aan te kondigen dat deze hoorbaar is voor de personen die zich het dichtst in de buurt bevinden[64].

63. De onuitvoerbaarheid die wordt gerechtvaardigd door het **onmiddellijke gevaar voor de te waarschuwen persoon** roept de vraag op of de activering van een camera dit onmiddellijke gevaar kan afwenden. Indien een dergelijk geval echter naar behoren wordt toegelicht in de toelichting bij het betrokken artikel, is de Autoriteit van mening dat deze uitzondering kan worden toegestaan. Daarentegen, als de te waarschuwen persoon zich in een verwarde toestand bevindt, zal de waarschuwing niet onuitvoerbaar zijn. Het zou hoogstens nutteloos kunnen blijken te zijn. Aangezien deze nuttelоosheid echter pas achteraf met zekerheid zal blijken, is de Autoriteit van mening dat de waarschuwing in dit geval moet worden gehandhaafd.

64. Ten slotte zou de waarschuwing "***duidelijk ongepast of nutteloos**, met name wanneer de individuele camera wordt gebruikt op een plaats waar geen mensen aanwezig zijn*" alleen **van**

[61] Art. 12/1, § 3 (nieuw), 12/2, § 3 (nieuw) en 13/14, tweede lid (nieuw).

[63] De afgevaardigde ambtenaar merkt in dit verband overigens op dat "*het genoemde risico in een specifieke situatie uiteraard niet kan worden uitgesloten. Het effect van het gebruik van een individuele camera hangt met name af van de omstandigheden van de interventie en van de manier waarop de activering ervan wordt aangekondigd.*"

[64] Onverminderd de lichtwaarschuwing waarvan hieronder sprake zal zijn.

toepassing moeten zijn **op de operationele diensten van de civiele bescherming**. Dit dient te worden verduidelijkt in het ontwerp.

65. De Autoriteit dringt erop aan dat deze wijzigingen gepaard gaan met de verplichting dat de gebruikte camera's worden uitgerust met een **zichtbare lichtwaarschuwing** die aangeeft dat de camera actief is en dat er wordt opgenomen. Het gaat hier overigens om een klassieke eis in rechtsgebieden waar het dragen van individuele camera's is toegestaan[65].

66. De Autoriteit staat ook positief tegenover het feit dat er minimale vereisten zijn vastgelegd om aan de transparantieverplichting te voldoen[66]. De Autoriteit is echter van mening dat het privacybeleid, waarin wordt gewezen op de mogelijkheid om het recht van inzage uit te oefenen en/of een klacht in te dienen bij de GBA, alsook de regels voor het gebruik van de camera's, op eenvoudig verzoek **te raadplegen** moeten zijn **op de plaatsen** waar de individuele camera's worden gedragen. Wanneer er online toegang wordt aangeboden (bijvoorbeeld via een QR-code), moet rekening worden gehouden met de digitale kloof[67] en moeten personeelsleden die met individuele camera's zijn uitgerust, worden verplicht dat allen tijde (zo niet bij zich, dan toch in het voertuig) over een papieren versie van dit document beschikken. Het ontwerp dient in die zin dus gewijzigd te worden.

67. De door het ontwerp opgelegde **pré-opnamefunctie** vormt in de ogen van de Autoriteit eveneens een zeer belangrijke waarborg. De afgevaardigde ambtenaar wijst er overigens op dat het begrip "*objectivering*" van interacties of dat van "*objectieve vaststelling van het verloop van incidenten*" "*met name* [voortvloeit] *uit de pré-opnamefunctie: wanneer de camera wordt ingeschakeld, wordt de pré-*

---

[65] Zie ICO guidance on Body Worn Video (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/additional-considerations-for-technologies-other-than-cctv/body-worn-video-bwv/)

[66] Art. 12/1, § 4, *nieuw* van de camerawet: "*De beslissing* [over het gebruik van individuele camera's] *wordt ter informatie aan het publiek bekend gemaakt. Daartoe publiceert de verwerkingsverantwoordelijke op zijn officiële website informatie over het bestaan van het gebruik van individuele camera's en de belangrijkste regels die het gebruik ervan omkaderen, in het bijzonder de nagestreefde doeleinden, de voorwaarden voor activering en de waarborgen inzake gegevensbescherming*." Een vrijwel soortgelijke bepaling is opgenomen in artikel 13/6, § 5 en artikel 13/14, derde lid, van de wet inzake civiele bescherming.

[67] Zoals het Grondwettelijk Hof in zijn arrest nr. 126/2025 heeft benadrukt, bestaat de digitale kloof nog steeds. Dit blijkt ook uit de collectieve klacht die op 28 september 2026 tegen de Belgische Staat is ingediend om de ongelijkheden aan de kaak te stellen die voortvloeien uit de digitalisering van openbare en particuliere diensten; zie in dit verband ook het verslag van de Koning Boudewijnstichting "Digitale inclusie, Barometer digitale inclusie, 2022", de studie 2022 van de Belgische Vereniging voor Onderzoek en Expertise voor Consumentenorganisaties "De digitale kloof overbruggen voor alle consumenten" alsook hetadvies over de impact van de digitalisering van (overheids- of particuliere) diensten uitgebracht op 3 februari 2023 door Unia en het Steunpunt tot bestrijding van armoede, bestaansonzekerheid en sociale uitsluiting; zie bovendien het arrest nr. 106/2004 waarbij de wettelijke bepalingen werden vernietigd die voorzagen dat het Belgisch Staatsblad voortaan alleen nog op het internet zou worden gepubliceerd en niet meer in papieren vorm (met uitzondering van drie exemplaren). Het Hof oordeelde: deze maatregel voerde aldus "*een verschil in behandeling in tussen diegene die, aangezien hij toegang heeft tot informaticamaterieel, op eenvoudige wijze alle nummers kan raadplegen van het Belgisch Staatsblad die zijn uitgegeven sinds de inwerkingtreding van de aangevochten bepalingen en daaronder de tekst kan vinden die hem interesseert, en diegene die, aangezien hij geen toegang heeft tot de informatica, het nummer waarin die tekst is bekendgemaakt niet kan identificeren*" en "*Aangezien de bestreden maatregel niet gepaard gaat met voldoende maatregelen die waarborgen dat de rechtsonderhorigen een gelijke toegang hebben tot die teksten, heeft hij onevenredige gevolgen ten nadele van bepaalde categorieën van personen. Hij is dan ook niet bestaanbaar met de artikelen 10 en 11 van de Grondwet*"; zie in dezelfde zin het arrest nr. 10/2007

opnamesequentie automatisch toegevoegd aan het begin van de effectieve opname. *Deze functie maakt het mogelijk om de context vast te leggen waarbinnen de interventie begint*."

68. Om te voorkomen dat er sprake is van permanente bewaking, bepaalt het ontwerp logischerwijs dat de opname die voortvloeit uit de continue opname na 30 seconden wordt overschreven en dat alleen bij activering (voor een van de doeleinden van het ontwerp) de pré-opnamesequentie aan de effectieve opname wordt toegevoegd en bewaard[68]. De Autoriteit trekt de relevantie van de pré-opnamefunctie geenszins in twijfel, maar is van mening dat, aangezien de activering van de individuele camera bepalend is voor de inhoud van deze pré-opname, het niet gepast is om de gegevens die uit deze opname voortkomen als "*objectief*" aan te duiden. De Autoriteit is van mening dat, indien deze term in het ontwerp, de memorie van toelichting en de toelichting bij de betrokken bepalingen zou worden gehandhaafd, deze tussen aanhalingstekens moet worden geplaatst en dat **in de toelichting bij het betrokken artikel moet worden vermeld dat het tijdstip waarop de camera wordt geactiveerd invloed heeft op de inhoud van de pré-opname**.

II.8. Ontvangers van de gegevens en opnames

69. Allereerst stelt de Autoriteit vast dat artikel 8 van het ontwerp de toegang tot de gegevens en opnames beperkt tot uitsluitend de personen die door de verwerkingsverantwoordelijke zijn aangewezen. De Autoriteit begrijpt dat deze bepaling betrekking heeft op de toegang van haar personeelsleden. Het verdient echter de voorkeur om dit begrip 'toegang' in het ontwerp te verduidelijken. In dit verband zouden de "*leden die verantwoordelijk zijn voor de opleiding of professionele begeleiding, of de verbetering van veiligheidsprocessen en die zijn aangewezen door de verwerkingsverantwoordelijke*" niet als ontvangers moeten worden beschouwd (aangezien het om medewerkers van de verwerkingsverantwoordelijke gaat). De Autoriteit wijst er terloops op dat zij positief staat tegenover het feit dat in het ontwerp is bepaald dat de gegevens die in het kader van dit doeleinde worden verwerkt, op zijn minst vooraf gepseudonimiseerd moeten zijn.

70. Bovendien vermeldt hetzelfde artikel 8 zowel *rechtstreekse* als *onrechtstreekse* toegang, zonder deze begrippen te definiëren. Naast de noodzaak om deze begrippen te definiëren, is de Autoriteit van mening dat deze aanwijzing moet berusten op bindende regels waarvan de naleving kan worden gecontroleerd, en dat de bepaling in ontwerp de verwerkingsverantwoordelijken moet verplichten **een toegangsbeleid op te stellen**, als voorwaarde om als verwerkingsverantwoordelijke te worden opgenomen in het koninklijk besluit waarin de verwerkingsverantwoordelijken worden opgesomd die bevoegd zijn om individuele camera's te gebruiken[69].

---

[68] Zie met name artikel 28 van het ontwerp.

[69] Met betrekking tot deze machtiging aan de koning, zie hierboven.

71. De Autoriteit voegt hieraan toe dat het ontwerp, eveneens als voorwaarde voor het gebruik van individuele camera's door de verwerkingsverantwoordelijke, moet opleggen dat "*iedere persoon die niet rechtmatig gebonden is aan het beroepsgeheim en die toegang heeft tot de beeld- en geluidsopnames, alsook tot de GPS-gegevens, onderworpen is aan een discretieplicht of een* ***contractuele vertrouwelijkheidsverplichting****, waarvan de niet-naleving gepaard moet gaan met* ***afschrikkende sancties***"[70].

72. Wat betreft de (andere) ontvangers die in dit artikel 8 worden genoemd, rijzen er verschillende vragen. Wat de leden van de **politiediensten en de gerechtelijke overheden** betreft, gaat het er dus om dat de betrokkene en/of de verwerkingsverantwoordelijke de mogelijkheid krijgt om een strafrechtelijke klacht in te dienen, en in dat geval is deze bepaling gerechtvaardigd, ofwel gaat het erom leden van de politiediensten en gerechtelijke autoriteiten in staat te stellen deze gegevens, informatie en opnames op te vragen bij de verwerkingsverantwoordelijke, ten behoeve van een onderzoek naar een persoon wiens gegevens in het register voorkomen, voor feiten die losstaan van een klacht van de drager en/of de verwerkingsverantwoordelijke (bijvoorbeeld om de personen te kunnen identificeren die op een bepaalde locatie aanwezig waren)[71].

73. Wat dit tweede geval betreft, staat de Autoriteit positief tegenover het feit dat het register **geen identificatiegegevens** van de gefilmde persoon zal bevatten, dat artikel 7 het gebruik van individuele camera's en bijbehorende software **voor biometrische authenticatie of identificatie verbiedt** en dat de toelichting bij deze bepaling elke **koppeling**[72] met databanken met persoonsgegevens **verbiedt**. Indien het anders was bepaald, zou dit onvermijdelijk hebben geleid tot de invoering van een onevenredig toezichtsmechanisme. Om deze verboden echter daadwerkelijk effect te geven, is de Autoriteit van mening dat moet worden **verduidelijkt dat "*de naleving van deze verboden door de eventuele ontvangers een onmisbare voorwaarde is voor de mededeling van deze gegevens*"**. Er kan echter een uitzondering op dit communicatieverbod worden gemaakt (onverminderd het advies van het COC), met inachtneming van het evenredigheidsbeginsel[73] en op

---

[70] Artikel 13/10 van de wet van 2007 betreffende de civiele veiligheid is op vergelijkbare wijze geformuleerd, maar vermeldt noch de contractuele vertrouwelijkheidsverplichting (die voor personeel in de particuliere sector moet worden voorzien) noch het afschrikkende karakter van de sancties die kunnen worden opgelegd.

[71] Wat – onverminderd hetgeen hieronder wordt vermeld – ook zou kunnen worden toegestaan in een beperkt aantal gevallen (bijvoorbeeld in het kader van een gerechtelijk onderzoek naar misdrijven waarop de zwaarste gevangenisstraffen staan), waarbij in gedachten moet worden gehouden dat de beperking van de mogelijkheden om de opnames te gebruiken ook een beschermingsmaatregel is voor de dragers (van wie niet mag worden vergeten dat zij geen leden van de politiediensten zijn).

[72] Het ontwerp voegt "in real time" toe, maar de afgevaardigde ambtenaar heeft verduidelijkt dat "*de opstellers van het ontwerp met deze formulering niet de bedoeling hebben om een specifieke mogelijkheid tot koppeling achteraf vast te leggen*." *De verwijzing naar realtime is bedoeld om te verduidelijken dat de individuele camera tijdens het gebruik ervan niet kan worden ingezet als instrument voor een geautomatiseerde vergelijking met externe databanken.*"

[73] Bijvoorbeeld in het kader van een gerechtelijk onderzoek naar misdrijven die kunnen leiden tot de zwaarste gevangenisstraffen, zoals hierboven vermeld.

voorwaarde dat het voor de betrokken ontvanger geldende wettelijke kader hem toestaat biometrische gegevens te verwerken.

74. Bovendien moet **ervoor worden gezorgd dat het dragen van individuele camera's er nooit toe leidt dat een politie-interventie wordt uitgesteld** onder het voorwendsel dat de daders mogelijk zijn gefilmd, want, zoals de afgevaardigde ambtenaar aangaf "*is het de combinatie van deze verschillende instrumenten, aangepast aan de concrete omstandigheden, die een passend antwoord kan bieden*".

75. De Autoriteit is van mening dat het aan de opsteller van het ontwerp is om aan te tonen dat de eventuele mededeling van de gegevens uit het register (met inbegrip van de opnames) aan leden van de politiediensten die handelen in het kader van hun **bevoegdheden op het gebied van bestuurlijke politie**, noodzakelijk en evenredig is.

II.9. Mogelijkheid tot beperking van de rechten van betrokkenen

76. Volgens artikel 5 van het ontwerp heeft "*elke persoon van wie audiovisuele gegevens worden gecapteerd* […] *een recht van toegang tot de audiovisuele gegevens*", maar voegt daaraan toe dat dit recht tijdelijk kan worden beperkt in de gevallen bedoeld in artikel 23.1.c en d, van de AVG.

77. Hoewel een dergelijke beperking begrijpelijk is voor de politiediensten[74], lijkt de **noodzaak van een dergelijke beperking** voor niet-politieagenten aanzienlijk minder vanzelfsprekend. Ingevolge bevraging verduidelijkte de afgevaardigde ambtenaar dat "*de noodzaak van een dergelijke beperking niet afhangt van het al dan niet bestaan van politiebevoegdheden bij de dienst die de opname heeft gemaakt, maar van de aard van de opgenomen beelden en de omstandigheden waarin toegang wordt gevraagd*.
Zo kunnen beelden die door een niet-politionele dienst zijn opgenomen, later van belang zijn voor een administratief of gerechtelijk onderzoek. Het onmiddellijk meedelen ervan kan bijvoorbeeld de rechten van derden schenden of het goede verloop van een lopend onderzoek in gevaar brengen."

78. Zoals de Autoriteit in haar voornoemde advies nr. 114/2023[75] aangaf "*zelfs in geval van gebruik* [van de opnames] *voor bewijsdoeleinden, de verzamelde gegevens geen politiegegevens zijn en de verwerkingsverantwoordelijke zich dus niet kan beroepen op het geheim van het onderzoek om de toegang van de betrokkene tot zijn gegevens te beperken*". Er kan daarentegen worden bepaald dat *"indien de opgenomen feiten het voorwerp uitmaken van een gerechtelijk onderzoek, het* ***verzoek***

[74] Die, ter herinnering, niet onder het onderhavige ontwerp vallen.
[75] Punt 60.

om toegang *door een betrokkene, gericht aan de verwerkingsverantwoordelijke, onverwijld wordt* ***doorgestuurd naar het openbaar ministerie of de onderzoeksrechter die belast is met het onderzoek****, en dat de toegang slechts tijdelijk kan worden geweigerd indien deze laatsten zich binnen de vijf dagen uitdrukkelijk tegen de toegang verzetten*". Deze mogelijkheid is toelaatbaar vanwege de waarborgen die aan dit soort onderzoeken zijn verbonden (en in het bijzonder vanwege de tussenkomst van een onafhankelijke magistraat). Aangezien deze waarborgen bij administratieve of tuchtrechtelijke onderzoeken ontbreken, kan de mogelijkheid om de toegang te beperken niet tot deze onderzoeken worden uitgebreid.

79. Dit gezegd zijnde, **erkent de Autoriteit dat**, los van een onderzoek, **een onmiddellijke mededeling de rechten van bepaalde derden** (slachtoffers, getuigen, kwetsbare personen of zelfs collega's van de drager) **kan schaden**. Het gaat er dus om een juist evenwicht te vinden, zodat individuele camera's een instrument blijven voor transparante interventies (en dat de documentatie van "*het feitelijke verloop van de interventie zo volledig mogelijk*", zoals de afgevaardigde ambtenaar[76] aangaf, niet alleen wordt toegelaten wanneer deze "*ten laste*" is) en niet veranderen in een bewakingsinstrument. De Autoriteit is van mening dat dit evenwicht kan worden bereikt **door de onmiddellijke mededeling te vervangen door een raadpleging van de opname in de kantoren van de verwerkingsverantwoordelijke, wanneer het verstrekken van een kopie van de opname de rechten van bepaalde derden zou kunnen schaden**. Ten slotte is het, zoals hierboven vermeld, **noodzakelijk om te bepalen dat de software van individuele camera's moet beschikken over functies voor het vervagen of verbergen van beelden, zodat het recht van inzage kan worden gewaarborgd met inachtneming van de rechten van derden**[77].

II.10. Toepasselijke beveiligingsmaatregelen

80. Individuele camera's zijn mobiele apparaten die zowel beeld als geluid vastleggen (en dus onder meer gezichten en stemmen opnemen), die op verschillende manieren kunnen worden gedragen, maar die tijdens een confrontatie kunnen worden vernield, kwijtgeraakt of gestolen[78]. Bovendien bieden

---

[76] Zie hierboven.

[77] Zie in die zin ICO guidance on Body Worn Video, *op. cit.;* zie ook DPC Guidance on the use of Body Worn Cameras or Action Cameras, p. 6.

(https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20on%20Body%20Worn%20Cameras%20or%20Action%20Cameras_Jan20.pdf)

[78] Peter Hermann, "D.C. Poised to Test Body Cameras for Police Officers," Washington Post, September 6, 2014, accessed January 10, 2015

(http://www.washingtonpost.com/local/crime/dc-poised-to-test-body-cameras-for-police-officers/2014/09/06/358ebc52-3459-11e4-a723-fa3895a25d02_story.html), geciteerd door Alexandra Mateescu, Alex Rosenblat en Danah Boyd, Working Paper on Police-Worn Cameras, Data&Society Research Institute, Feb. 2015, blz. 5.

(https://datasociety.net/wp-content/uploads/2015/10/PoliceBodyWornCameras-1.pdf); zie ook Home Ofiice, Safeguarding Body Worn Video Data, Publication No.011/18, Oct. 2018, blz. 14 e.v. (https://assets.publishing.service.gov.uk/media/5bb769f6ed915d23b3cabd20/safeguarding-body-worn-video-data-01118p.pdf)

bepaalde cameramodellen de mogelijkheid tot toegang op afstand (wifi, bluetooth, enz.), waardoor de gegevens die ze bevatten worden blootgesteld aan zeer ernstige kwetsbaarheden en het in sommige gevallen zelfs mogelijk is om de verplaatsingen van de dragers te volgen[79]. Bovendien is het, vanwege de enorme hoeveelheid gegevens die bij het gebruik van dit soort camera's moet worden opgeslagen, vaak nodig om een beroep te doen op externe verstrekkers van clouddienstverlening. Dit kan ertoe leiden dat de gegevens worden blootgesteld aan internationale doorgiften en/of onderworpen worden aan buitenlandse wetgeving die onverenigbaar is met de AVG[80].

81. In een context waarin cyberaanvallen naar verwachting zullen toenemen en steeds geavanceerder zullen worden als gevolg van de vooruitgang op het gebied van kunstmatige intelligentie[81] en de ontwikkeling van kwantumcomputers, moet de Autoriteit strengere eisen stellen op het gebied van minimale gegevensverwerking en de technische en organisatorische maatregelen die moeten worden getroffen om een hoog niveau van cyberbeveiliging te waarborgen, wanneer nieuwe vormen van gegevensverwerking – zoals het opnemen van stemmen[82] – op dit gebied tot verhoogde risico's kunnen leiden.

82. In dit geval vreest de Autoriteit dat, terwijl de overheid nu al te weinig investeert in cyberbeveiliging[83], commerciële ondernemingen die machtiging hebben om bepaalde personeelsleden uit te rusten met individuele camera's, in de verleiding zouden kunnen komen om hun investeringen zoveel mogelijk te beperken in technologie die nodig is om het vereiste niveau van gegevensbeveiliging te bereiken voor de verwerking van (mogelijk) zeer gevoelige gegevens[84].

83. Bovendien is het, in de Belgische context waarin de overheidsinstanties geen geldboetes opgelegd kunnen krijgen door de Geschillenkamer van de Autoriteit en waarin de rechtspraak van het Marktenhof niet toestaat dat afschrikkende geldboetes worden opgelegd aan private bedrijven, is de Autoriteit van mening dat **het onverantwoord zou zijn om verwerkingsverantwoordelijken toe te staan hun personeelsleden uit te rusten met individuele camera's zonder hen te onderwerpen**

---

[79] Zie https://www.abc.net.au/news/2026-05-04/police-location-tracked-bluetooth-flaw-axon-tasers-bodycams/106610886 en https://azmirror.com/2020/07/02/fort-huachuca-police-body-cam-footage-easily-accessible-after-an-ebay-purchase/; zie ook D. Oberhaus, Hackers Can Edit Police Body Cam Footage Without Anybody Noticing, Vice 13.08.2018 (https://www.vice.com/en/article/hackers-can-edit-police-body-cam-footage-without-anybody-noticing/);

[80] Zie https://securityaffairs.com/81935/digital-id/german-police-bodycam-amazon-servers.html.

[81] https://www.staysafeonline.org/fr/articles/pourquoi-votre-famille-et-vos-coll%C3%A8gues-ont-besoin-d-un-mot-de-passe-dans-l-%C3%A8re-de-l-ia

[82] https://www.bbc.com/future/article/20260804-why-your-family-needs-a-secret-codeword

[83] https://www.vrt.be/vrtnws/nl/2024/01/19/gegevens-hack-limburg-net/; https://www.vrt.be/vrtnws/nl/2022/11/24/hacking-politie-zwijndrecht/

[84] Zoals ook op andere gebieden is vastgesteld, bijv. https://www.computable.be/2024/12/18/forse-boete-voor-ziekenhuis-wegens-gebrekkige-it-beveiliging/ en https://www.lalibre.be/belgique/societe/2022/05/27/cyberattaque-chez-vivalia-une-digitalisation-trop-rapide-pourrait-expliquer-la-fragilite-des-hopitaux-MG5OBCUJSZGXVNEVEAXNOSAURM/

aan minimale veiligheidsvoorwaarden[85], door middel van een bindend veiligheidsbeleid dat wordt vastgesteld en bijgehouden door de diensten van de minister van Veiligheid en Binnenlandse Zaken[86], waarvan de naleving wordt gecertificeerd door een periodieke audit, als voorwaarde om deze verwerkingsverantwoordelijken op de door de Koning vastgestelde lijst te kunnen plaatsen of te laten staan[87].

84. De Autoriteit is bovendien van mening dat het noodzakelijk is om in het ontwerp vast te leggen dat deze minimale veiligheidsvoorwaarden de verplichting inhouden dat de autoriteit of de onderneming die individuele camera's wil inzetten, moet **beschikken over een informatiebeveiligingsfunctionaris (Chief Information Security Officer - CISO) met een masterdiploma in cyberbeveiliging**.

85. De Autoriteit is bovendien van mening dat **het bestaan van rechtsmiddelen geen voldoende waarborg vormt** voor het herstel van de rechten van de gebruikers wier gegevens het voorwerp zouden uitmaken van onrechtmatige toegang (door personeelsleden of een derde die misbruik zou maken van een beveiligingslek) of van doelverschuiving. Bijgevolg is de Autoriteit van mening dat in deze situaties moet worden voorzien in de opstart van een **procedure die ertoe strekt de betrokkene in zijn rechten te herstellen** – onafhankelijk van het initiatief van de betrokkene – en in een schadevergoeding voor de betrokkene.

86. Bovendien moet worden bepaald dat de verwerkingsverantwoordelijken bij de bestelling van individuele camera's **hun leveranciers contractueel** (via de administratieve bepalingen van het speciale bestek voor overheidsinstanties) moeten **verplichten dat "*in geval van onrechtmatige toegang als gevolg van het misbruik van een beveiligingslek in de geleverde producten (met inbegrip van de software), onverminderd het recht van de betrokkenen om de inbreukmakende partij aansprakelijk te stellen, de leverancier van rechtswege aan elke betrokkene die door het lekken van zijn gegevens is getroffen, een geïndexeerd forfaitair bedrag van 3.000 EUR verschuldigd is*"**.

87. De Autoriteit voegt hieraan toe dat het veiligheidsbeleid dat op het niveau van de FOD Binnenlandse Zaken wordt vastgesteld, ervoor moet zorgen dat er een **robuuste versleuteling** wordt opgelegd en dat er een **strategie** wordt opgesteld **om over te stappen op zogenaamde "*post-kwantum*"-versleutelingsstandaarden**[88], dat de implementatie van een technische oplossing wordt opgelegd

[85] Waarbij de verwerkingsverantwoordelijke uiteraard de vrijheid behoudt om deze aan te vullen met een strenger intern veiligheidsbeleid

[86] Zie bijv. Federal Bureau of Investigation, U.S. Department of Justice. Criminal Justice Information Services (CJIS) Security Policy. Versie 5.9.4. 20 december 2023, https://le.fbi.gov/file-repository/cjis_security_policy_v5-9-4_20231220.pdf.

[87] Zie over deze kwestie hierboven.

[88] Zie over deze kwestie https://cybersecuritycoalition.be/wp-content/uploads/CSC-WP-PQC-Vol1_FINAL.pdf

die het **automatisch wissen** van gegevens na 30 dagen mogelijk maakt, onder voorbehoud van een specifieke handeling waarmee de bewaartermijn tot maximaal 90 dagen kan worden verlengd wanneer aan de voorwaarden voor een dergelijke verlenging is voldaan[89], dat het mogelijk wordt gemaakt om **geolocatie**metadata aan de opnames te koppelen, maar deze gegevens niet live te verspreiden (behalve voor de operationele diensten van de civiele bescherming[90]) en **dat de mogelijkheid van automatische activering wordt verboden**[91] vanwege de risico's op storingen die dit met zich meebrengt[92].

OM DEZE REDENEN,
is de Autoriteit de volgende mening toegedaan:

1. Er moet een onderscheid worden gemaakt tussen de redenen waarom het "dragen" van een individuele camera door een dienst kan worden toegestaan, en de doeleinden van het "activeren" van de camera (**punt 28**);
2. Het doeleinde met betrekking tot de bescherming van de veiligheid van "agenten" zou uitsluitend van toepassing moeten zijn op "de agent die de camera draagt" (**punt 29**);
3. Er moet een hiërarchie van doeleinden worden vastgesteld (**punt 30**);
4. De term "*objectief*", die wordt gebruikt om de vaststellingen van incidenten via individuele camera's te omschrijven (**punten 31-32 en 68**), moet in het juiste perspectief worden geplaatst.
5. De verwijzing naar uitsluitend het doel om bijzondere categorieën van gegevens te verwerken, moet worden vermeden (**punt 34**);
6. Het ontwerp moet minimumvereisten bevatten met betrekking tot de mogelijkheid om opnames te bewerken, en de opstellers van het ontwerp moeten de mogelijkheid overwegen

---

[89] Dit biedt immers een effectieve garantie tegen het vergeten van het wissen.

[90] Onder voorbehoud van hetgeen hierboven is vermeld.

[91] Zie Scientific Working Group on

Digital Evidence, Considerations for Body Worn Camera Systems, SWGDE 23-V-002-1.0, pun 6.8. (https://www.swgde.org/wp-content/uploads/2026/03/2026-02-25-Considerations-for-Body-Worn-Camera-23-V-002-1.0.pdf).

[92] Zie het hoofdstuk met de titel "Concerns regarding their own privacy", in Poirier, B., Charbonneau, É., & Boivin, R. (2024). Police body-worn cameras and privacy: Views and concerns of officers and citizens. *International journal of police science & management*, *26*(2), 170–181. https://doi.org/10.1177/14613557231214383, waarin een ondervraagde gebruiker verklaart: "*Me, personally, I always take off my bulletproof vest* [on which BWCs are attached] *when I go to the bathroom, so that kind of thing won't happen to me. But it happened to one of my colleagues, and she wasn't thrilled. She was like, "Will it be erased?". Well, no, it stays in the cloud. (User/end of pilot; female officer with 9 years of police experience)*".

om bepaalde plaatsen op te sommen waar de individuele camera's alleen op verzoek van de betrokkenen mogen worden geactiveerd (**punten 35, 60 en 79**);

7. De doeleinden die verband houden met het bestraffen van gedragingen van derden of van dragers en met pedagogische ondersteuning kunnen geen rechtvaardiging vormen voor een inmenging die zo vergaand is als de doeleinden die verband houden met de bescherming van de lichamelijke integriteit van de betrokkenen (**punt 37**);

8. Het ontwerp zou moeten bepalen dat wanneer een agent die een camera draagt, wordt geconfronteerd met agressief gedrag, hij zijn individuele camera mag activeren; "*de dragers moeten worden opgeleid om hun camera's niet in te schakelen wanneer een voorafgaande waarschuwing heeft geleid tot het bereiken van het doel van de-escalatie van het conflict*" (**punt 38**);

9. In het ontwerp moet een onderscheid worden gemaakt tussen de doeleinden van de verwerking van GPS-gegevens die een realtime-doorgifte (of toegang) niet kunnen rechtvaardigen en de doeleinden die dit wel kunnen rechtvaardigen (**punt 40**);

10. Er moet worden gerechtvaardigd waarom het noodzakelijk is dat deze geolocatiegegevens in real time via de camera worden doorgegeven (**punten 41-42**);

11. De opnamefuncties van beeld en geluid en voor communicatie in real time moeten door de drager kunnen worden in- en uitgeschakeld (op basis van een bindend beleid) (**punt 43**);

12. Het evenredige karakter van de maatregel kan worden aangetoond in het kader van een testfase die beperkt is tot twee jaar en de verplichting om binnen die termijn een onafhankelijk (universitair) onderzoek te laten uitvoeren (**punten 45-50**);

13. De Koning zou gemachtigd moeten worden om (bijvoorbeeld om de twee jaar), na verificatie van de operationele behoefte en de naleving van de voorwaarden, de lijst vast te stellen van verwerkingsverantwoordelijken die bevoegd zijn om hun personeelsleden uit te rusten met individuele camera's (**punten 51 en 54-56**);

14. Het is onaanvaardbaar om een bepaling zo te formuleren dat de verwerkingsverantwoordelijke een machtigingsaanvraag aan zichzelf kan richten (**punt 57**);

15. De bewaking (zelfs tijdelijk) van de openbare ruimte of van personen is niet verenigbaar met de in het ontwerp genoemde doelstellingen **(punt 59)**;

16. De uitzonderingen op de mondelinge waarschuwing voorafgaand aan de activering zouden sterk moeten worden beperkt (**punten 61-64**);

17. Er moet worden voorzien in een verplichting om de gebruikte camera's uit te rusten met een zichtbare lichtwaarschuwing die aangeeft dat de camera actief is en dat er wordt opgenomen (**punt 65**);

18. Het privacybeleid, waarin wordt gewezen op de mogelijkheid om het recht van inzage uit te oefenen en/of een klacht in te dienen bij de GBA, alsook de regels voor het gebruik van camera's, moet op eenvoudig verzoek te raadplegen kunnen zijn op de plaatsen waar de individuele camera's worden gedragen (**punt 66**);

19. De voorwaarden waaronder de verwerkingsverantwoordelijke kan worden vermeld in het KB waarin de verwerkingsverantwoordelijken worden opgesomd die gemachtigd zijn om individuele camera's te gebruiken, moeten onder meer de vaststelling van een toegangsbeleid omvatten, evenals de verplichting om elke persoon die niet rechtmatig gebonden is aan het beroepsgeheim en die toegang heeft tot de beelden en geluiden (alsook tot de GPS-gegevens, indien van toepassing), aan een discretieplicht of een contractuele vertrouwelijkheidsverplichting te onderwerpen, waarbij niet-naleving gepaard moet gaan met afschrikkende sancties (**punten 70-71**);

20. Het verbod op de verwerking van biometrische gegevens en het koppelen van gegevens moet worden uitgebreid tot de ontvangers (**punten 72-74**);

21. Er moet worden aangetoond dat de mogelijke mededeling van gegevens uit het register (met inbegrip van de opnames) aan de leden van de politiediensten die handelen in het kader van hun bevoegdheden op het gebied van de bestuurlijke politie, noodzakelijk en evenredig is (**punt 75**);

22. De mogelijkheden om de uitoefening van rechten te beperken, zouden moeten worden afgezwakt (**punten 77-79**);

23. Het zou onverantwoord zijn om verwerkingsverantwoordelijken toe te staan hun personeelsleden uit te rusten met individuele camera's zonder dat daarvoor minimale veiligheidsvoorwaarden gelden (**punten 80-83 en 87**);

24. De minimale veiligheidsvoorwaarden moeten de verplichting omvatten om te beschikken over een CISO met een masterdiploma in cyberbeveiliging (**punt 84**);

25. Er moet worden voorzien in een procedure om de rechten van de betrokkene te herstellen, alsmede in een automatische en forfaitaire schadevergoeding (**punten 85-86**).

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