DPIA Bodycams Voorne-Putten

Gegevensbeschermingseffectbeoordeling op inzet van bodycams

5 juli 2021

Versie 1.0

DPIA Bodycams Voorne-Putten

Gegevensbeschermingseffectbeoordeling op inzet van bodycams

Auteurs
Privacy Management Partners:
Alfonso Okué, LL. B CIPP/E CIPM
Sander van der Smissen, MSc, CIPM, CIPP/e
Michelle Wassenaar, BA, CIPP/e

5 juli 2021

Managementsamenvatting

Dit rapport is bedoeld om inzicht te krijgen in de rechtmatigheid van de verwerking van persoonsgegevens en de daaraan verbonden risico's voor de burgers, Buitengewone Opsporingsambtenaar (BOA) en de gemeenten op Voorne-Putten. Het doel is om voor deze risico's passende mitigerende maatregelen op te stellen waarmee de rechten en vrijheden van de betrokken personen en de organisatie voldoende beschermd zijn.

De bodycams hebben als hoofddoel om de BOA een veiligere werkomgeving te bieden. Daarnaast zullen de gemeenten de beelden kunnen gebruiken om de bewijspositie bij incidenten te verbeteren. Dit gebeurt doordat het mogelijk wordt dat de camerabeelden aan het Openbaar Ministerie (OM) of de politie kunnen worden verstrekt. Een enkele gemeente heeft de wens uitgesproken om de camerabeelden voor individuele scholing- en opleiding te gebruiken. In de bijlage hebben wij hiervoor de onderbouwing opgesteld.

Hoofdstuk 1 van dit rapport beschrijft de werking van de bodycam met het gebruik van alle persoonsgegevens, aanverwante applicaties en betrokken partijen.

De rechtmatigheid van deze verwerkingen worden in hoofdstuk 2 zorgvuldig afgewogen en zijn juridisch onderbouwd. Kort samengevat geldt dat de gemeenten een gerechtvaardigd belang hebben om het privaatrechtelijk gebruik van bodycams te rechtvaardigen. Privacy Management Partners (PMP) merkt daarbij wel op dat deze grondslag voor discussie vatbaar is.

Voor een overheidsoptreden met de bodycam dient men in beginsel te verwijzen naar een expliciete wettelijke grondslag of openbare taak, hetgeen nu voor de bodycams in de Nederlandse wetgeving ontbreekt. Gemeenten hebben daardoor een verzwaarde verantwoordingsplicht om het gerechtvaardigd belang voor de inzet van bodycams te rechtvaardigen.

Toch zijn er steeds meer gemeenten die de bodycam implementeren. De huidige situatie lijkt er daardoor op dat de Autoriteit Persoonsgegevens het gebruik van bodycams door gemeenten gedoogt. Het is evengoed mogelijk dat zij pas gaat handelen als er een bestuurlijke klacht of handhavingsverzoek wordt ingediend. De nadere onderbouwing hebben wij in de paarse vakken opgenomen.

Daarnaast heeft PMP ook de uitkomsten van een burgerpanel-uitvraag bij Gemeente Nissewaard meegenomen bij het onderbouwen van de noodzaak, proportionaliteit en subsidiariteit van de gemeentelijke inzet van bodycams.

In hoofdstuk 3 is geanalyseerd welke risico's ontstaan die impact kunnen hebben op burgers, toeristen en gemeenten. Hoewel het filmen primair gaat om de BOA een veiligere werkplek te bieden, kunnen de gegevens ook worden gebruikt om een BOA te monitoren en daar (arbeidsrechtelijke) conclusies aan te verbinden of een burger op een ongemakkelijk moment te filmen.

Daarom zijn alle relevante risico's op basis van realistische scenario's in kaart gebracht. Naast deze specifieke risico's bestaan er ook meer algemene risico's die betrekking hebben op het proces. Hierbij kunt u denken aan informatiebeveiliging, klachten vanuit de stakeholders en verkeerd gebruik van de gegevens. Maar ook risico's die uw organisatie bij fouten of incidenten kunnen treffen.

Op basis van de vastgestelde risico's zijn in hoofdstuk 4 specifieke en algemene maatregelen geformuleerd die gezamenlijk deze risico's mitigeren. Met deze maatregelen wordt een balans

gevonden tussen enerzijds het belang van de gemeenten op Voorne-Putten, als goed werkgever en anderzijds de verantwoorde bescherming van persoonsgegevens. In dit hoofdstuk zijn alle concrete maatregelen die voortvloeien uit de risicoanalyse opgenomen. De uitvoering van deze maatregelen vereist allereerst gezond verstand. Belangrijk is het besef dat met dit rapport slechts de basis is gelegd voor een verantwoorde gegevensbescherming.

Het vormt daarmee de start van het daadwerkelijk bereiken van *privacy by design*. Naast de implementatie van de voorgestelde maatregelen is het belangrijk dat de gemeenten in overeenstemming met de AVG en andere geldende wet- en regelgeving zoals de Wet op de Ondernemingsraden, arbeidswetgeving en Algemene Wet Bestuursrecht handelen.

Pas bij implementatie van deze maatregelen en structurele aandacht, bijvoorbeeld voor het juist informeren van personen en nemen en het naleven van de bewaartermijnen, kunnen de gemeenten waarborgen bieden die nodig zijn. Op die manier kunnen de gemeenten de filmende bodycams gebruiken zonder dat de privacy van haar BOA's, burgers en toeristen in het geding komt.

Inhoud

Begrippen en afkortingen

Persoonsgegeven: *alle* informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Identificatie kan ook *indirect*, het hoeft niet altijd een naam te zijn om informatie te kunnen herleiden naar een persoon. Ook maakt de vorm van de informatie niet uit; het kan zowel schriftelijke informatie betreffen, als bijvoorbeeld een foto, film of geluidsopname. Voorbeelden van persoonsgegevens: NAW-gegevens, rekeningnummer, identificatienummer, locatiegegevens, online identificator of elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van een persoon.

Bijzondere persoonsgegevens: persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, genetische gegevens, gezondheidsgegevens of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Gevoelige persoonsgegevens: gegevens die naar hun aard gevoelig zijn en daarom extra bescherming behoeven. Hierbij kan gedacht worden aan inloggegevens, financiële gegevens, gegevens waarmee identiteitsfraude gepleegd kan worden, gegevens die onder een wettelijke geheimhoudingsplicht vallen etc.

Verwerking: *alle handelingen* die een organisatie kan uitvoeren met persoonsgegevens. Denk aan het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van persoonsgegevens.

Betrokkene: een geïdentificeerde of identificeerbare *natuurlijke persoon* over wie persoonsgegevens worden verwerkt. Ook bedrijven zonder rechtspersoonlijkheid kunnen, afhankelijk van de structuur, als 'betrokkene' worden aangemerkt. Hierbij kan gedacht worden aan een ZZP'er of aan een maatschap waarbij de maten natuurlijke personen zijn (en niet bv's).

Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een dienst of een ander orgaan die, alleen of samen met anderen, het *doel* van en de *middelen* voor de verwerking van persoonsgegevens vaststelt.

Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die *ten behoeve van* de verantwoordelijke persoonsgegevens verwerkt.

Functionaris voor Gegevensbescherming (FG): een door de organisatie aangestelde privacytoezichthouder. Zijn positie, kwalificaties en taken zijn bij wet geregeld. De belangrijkste taken zijn:

- toezien op naleving van de privacywetgeving en intern privacybeleid;
- informeren en adviseren van directie en medewerkers over naleving van privacywetgeving;
- onderhouden van de contacten met de Autoriteit Persoonsgegevens.

Afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BOA	Buitengewone Opsporingsambtenaren
DPIA	Data Protection Impact Assessment (ook wel PIA – Privacy Impact Assessment)
EPDB	European Data Protection Board
FG	Functionaris Gegevensbescherming
NAW	Naam Adres Woonplaats
OM	Openbaar Ministerie
RTGB	Regeling toetsing geweldsbeheersing BOA

Inleiding

Aanleiding

Steeds meer gemeenten besluiten om voor de uitvoering van hun werkzaamheden nieuwe technologie toe te passen. Eén van de ontwikkelingen is het gebruik van de bodycam. Dit is een kleine draagbare camera die op of aan het lichaam wordt bevestigd en waarmee video- en geluidsfragmenten worden geregistreerd en/of opgeslagen. Vervolgens kunnen dergelijke videobeelden worden uitgelezen en door de gemeente worden gebruikt.

Op Voorne-Putten krijgen buitengewone opsporingsambtenaren (BOA's) en toezichthouders steeds vaker te maken met verbale agressie en geweld. Er hebben zich al meerdere (gewelds)incidenten met BOA's en toezichthouders voortgedaan. Uit een pilot van de Nationale Politie blijkt dat politieambtenaren die een bodycam dragen zich veiliger voelen. Verder blijkt uit de pilot dat er minder agressie en geweld wordt gebruikt tegen ambtenaren die uitgerust zijn met een bodycam[1]. Concluderend, een bodycam zou dus kunnen helpen om (gewelds-)incidenten op Voorne-Putten preventief te voorkomen.

In februari 2020 hebben de gemeenten op Voorne-Putten (Nissewaard, Brielle, Hellevoetsluis en Westvoorne) de intentie uitgesproken om gezamenlijk op te trekken bij de inzet van bodycams. Immers levert een samenwerking tussen vier gemeenten schaalvoordelen op. De gemeenten op Voorne-Putten hebben besloten dat de bodycams door de gemeentelijke toezichthouders en BOA's in het kader van hun openbare taak worden gedragen.

In april 2020 hebben de vier gemeenten hun functionaris gegevensbescherming (hierna: FG of FG's) om advies gevraagd. Het FG-advies betreft de privacyrisico's die bij de aanschaf van bodycams zouden kunnen spelen. Door het advies van de gezamenlijke FG's is de aanschaf van bodycams voorlopig *on hold* gezet. De aanschaf van bodycams dient op grond van de AVG eerst te worden getoetst.

Gelet op het zware maatschappelijk belang van het gebruik van bodycams, is het voor de gemeenten van belang om helderheid over dergelijke privacyrisico's te krijgen. Daarbij is een spoedige inzet van de bodycams altijd de wens geweest. De gemeenten zijn op zoek naar een manier waarop dit verantwoord (met inachtneming van de privacy-vereisten) kan gebeuren, maar waarbij de BOA's zo snel mogelijk kunnen worden uitgerust met de bodycams.

Privacy Management Partners (PMP) is gevraagd om haar hierin bij de uitvoering te ondersteunen. In voorliggend document wordt de inzet van bodycams weergegeven, resulterend in een set aanbevelingen om aan de uitgangspunten van de AVG te voldoen.

Wat is een Data Protection Impact Assessment (DPIA)?
Een DPIA heeft als doel om een inschatting te maken van de impact die een product, dienst of proces op de privacy van betrokkenen kan hebben, en om de maatregelen te bepalen die nodig zijn om risico's te mitigeren. Het DPIA-rapport is idealiter een levend document: een eerste versie wordt opgesteld zodra de contouren van het proces gestalte krijgen.

Vervolgens wordt het document waar nodig aangepast en geactualiseerd al naar gelang het initiatief meer vorm krijgt en het inzicht in de privacyaspecten en de mogelijke risicobeperkende maatregelen zich verdiept.

[1] https://www.politie.nl/themas/landelijk-project-bodycams.html

Beschrijving van het DPIA-proces

Het proces om te komen tot de DPIA is hieronder beschreven. De gemeenten op Voorne-Putten hebben voorafgaand aan een eerste conceptversie input geleverd via deelname aan een aantal workshops en door de documentatie die met is PMP gedeeld. De documenten zijn:

- Protocol Cameratoezicht
- Specificaties van de camera
- Het inkoopvoorstel

In de workshops waren verschillende stakeholders aanwezig uit alle deelnemende gemeenten en zijn de volgende thema's uitvoerig besproken:

- Kenmerken die bij de verwerking van persoonsgegevens passen;
- Juridische afweging
- Scenario's
- Risico's voor de organisatie
- Verwerkingsbelang - doeleinden
- Voorgenomen proces

PMP heeft van de documenten enkele aantekeningen gemaakt en gecombineerd met de input uit de workshops. Deze aantekeningen en input zijn vervolgens gekoppeld aan bestaand onderzoek naar bodycams, een (privacy)juridische onderbouwing, evaluaties van ervaringen in andere gemeenten en een inschatting van beheersmaatregelen. Dit hebben wij naar een tussenrapportage vertaald (QuickScan).

In de definitieve versie van de DPIA is bovenstaande samengevoegd met het voorlopige FG-advies, een risicoinschatting gebaseerd op een aantal praktijkscenario's, om zo te komen tot de uiteindelijke conclusies en aanbevelingen voor de implementatie van de bodycams.

Versie 0.1	26 – 02 – 2021	Concept DPIA-rapport
Versie 0.2	15– 03 – 2021	Concept met integratie feedback
Versie 0.5	09 – 04 – 2021	Verwerking commentaren, herschrijven bijlage
Versie 0.9	07- 05-2021	Definitieve versie met check FG's,
Versie 1.0	12 -05-2021	Toevoegen managementsamenvatting
Versie 1.0a	05-07-2021	Aanvulling laatste feedback

Verantwoording en leeswijzer

Deze DPIA is onder begeleiding van PMP uitgevoerd met medewerkers van de vier gemeenten. Dit DPIA-rapport volgt het in artikel 35 AVG voorgeschreven stramien. De AVG bepaalt dat een gegevensbeschermingseffectbeoordeling (DPIA) minimaal de volgende elementen bevat:

1. Een systematische beschrijving van de verwerkingen en de verwerkingsdoelen (*zie hoofdstuk 1 van dit rapport*);
2. Een beoordeling van de noodzaak en evenredigheid van die verwerkingen met betrekking tot de doelen (*zie hoofdstuk 2*);
3. Een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen, de zogenaamde impactanalyse (*zie hoofdstuk 3*);
4. De beoogde maatregelen om risico's aan te pakken, waaronder waarborgen en veiligheidsmaatregelen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan de AVG is voldaan met inachtneming van de rechten en belangen van betrokkenen en de andere personen in kwestie (*zie hoofdstuk 4*).

Afbakening

De gegevensverwerkingen binnen het onderzochte gebruik van bodycams – inclusief interne overdracht van gegevens (tot en met het moment van overdracht) – zijn voor de DPIA bekeken. De AVG en de aanverwante privacy en arbeidswet- en regelgeving gelden hierbij als het juridisch kader. Richtinggevend zijn bovendien gezaghebbende uitwerkingen van de Autoriteit Persoonsgegevens (AP) en de Europese toezichthouder (EDPB).

1 Systematische beschrijving

In dit hoofdstuk volgt een systematische beschrijving van de voorgenomen inzet van bodycams. Met de systematische beschrijving wordt bedoeld:

- beschrijvingen van de processen;
- applicaties (opzet en bestaan);
- keten (samenwerkingspartners en privacyrechtelijke positie);
- welke persoonsgegevens binnen deze processen voorkomen; en de
- grootschaligheid van de verwerking.

Aan de hand van deze kaders beschrijven wij het proces 'bodycams'. Allereerst, wat is een bodycam? Een bodycam is een draagbare camera die onderdeel kan zijn van de uitrusting van een BOA. De camera kan videobeelden en audio registreren, opslaan en optioneel real-time verzenden. Bodycams zijn gemakkelijk aan de kleding of uniform te bevestigen.

1.1 Hoe werkt de bodycam?

Het filmen met een bodycam is feitelijk een observatie met behulp van een technisch middel: een vorm van versterkte waarneming. De camera registreert datgene waarop hij gericht is. In veel gevallen zijn dat de gebeurtenissen die de drager zelf meemaakt, ziet en/of hoort. Voor het grootste gedeelte zullen de opnamen ook opgeslagen worden, maar dat hoeft niet. Er zijn drie modi beschikbaar om de werking van de bodycam te onderscheiden:

- de stand-by modus;
- record-modus;
- post-record modus.

De vier gemeenten hebben qua model gekozen voor de camera IWitness IW1B. Hieronder beschrijven wij de werking van deze camera.

Stand-by modus bodycam

De BOA draagt de bodycam tijdens zijn gehele dienst in stand-by modus. Dit houdt in dat de bodycam altijd aan staat, maar geen beelden opslaat. Dit wordt ook wel de pre-recordingfunctie genoemd. De bodycam maakt opnames van 120 seconden en wanneer de opnameknop niet wordt ingedrukt, worden deze beelden overgeschreven en filmt de bodycam opnieuw 120 seconden. In de stand-by modus wordt dus geen enkel beeldmateriaal opgeslagen.

Record-modus bodycam

Wanneer de BOA het noodzakelijk acht, kan de BOA – door middel van de grote knop op de bodycam – een opname starten. Wanneer deze knop wordt ingedruktwordt er beeldmateriaal opgenomen. Daarnaast wordt er 120 seconden vooraf aan het indrukken van de knop opgeslagen en de 120 seconden nadat de bodycam weer op stand-by is gezet. In de record-modus worden er wel beelden opgeslagen.

Bij opname van individuen wordt indien mogelijk door de BOA vooraf gemeld (met een luide stem) dat er opnamen gemaakt gaan worden. Indien waarschuwing vooraf niet mogelijk is, omdat er door de BOA direct gehandeld moet worden, wordt de bodycam direct aangezet

Als de opnamemodus is ingezet tijdens de dienst, dan wordt dit vervolgens bij terugkomst op het bureau geregistreerd en gerapporteerd.

Post-record modus

Als na afloop van de gebeurtenis weer op de grote knop wordt gedrukt, wordt de opname gestopt en gaat de camera over in Post-record modus. De camera kan dan nog 300 seconden (5 minuten) opslaan (in dit geval is er gekozen voor 120 seconden - 2 minuten), en gaat dan definitief op stand-by. In de post record-modus worden er wel beelden op de camera opgeslagen.

Registratie en opslag

Bij terugkomst van de dienst wordt de bodycam aan het dockingstation gekoppeld. Het dockingstation heeft twee functies: enerzijds het opladen van de batterij, en anderzijds het opslaan van gemaakte beelden. Het moment waarop de bodycam op het dockingstation is aangesloten wordt automatisch gelogd. De beeld- en geluidopnamen worden – met encryptie – rechtstreeks geüpload naar de opslagruimte. Als dit proces is voltooid, dan wordt de opslagruimte van de bodycam door het systeem automatisch geleegd.

1.2 Informatievoorziening

In onderstaand overzicht worden de systemen opgesomd waarin persoonsgegevens verwerkt worden. Het doel van het gegevensgebruik binnen de applicaties is eveneens opgenomen.

Naam /systeem	Uitleg gebruik van systeem
Syntrophos	Syntrophos is het Shared Service Centre van de vier gemeenten op Voorne-Putten. Syntrophos zorgt o.a. voor de ICT-huishouding van de gemeenten. Dat zal binnen het proces vermoedelijk niet heel veel anders zijn. Het zal dan gaan om de wijze van opslag van de beelden en dan wel bijwerken van de informatiebeveiligingsvoorzieningen.
City Control	City Control is het zaaksysteem van de BOA en is geleverd in de vorm van een applicatie. In dit systeem verwerken BOA's hun handhavingshandelingen (uitschrijven boete, proces-verbaal enzovoorts). ANPR-toegangscontrole voor voertuigen. Hierbij hebben zij toegang tot landelijke en lokale bronnen (zoals RDW, BRP en KvK). Binnen City Control is het denkbaar dat BOA's aan kunnen geven dat er beelden van een incident zijn.

1.3 Betrokken partijen en hun rollen (de keten)

We identificeren voor dit proces verschillende betrokken partijen. Daarbij kunnen diverse privacyrollen aan de orde kunnen zijn. Bij de partijen hebben we onderscheid gemaakt tussen de rol van verwerkingsverantwoordelijke en die van verwerker. De verwerkingsverantwoordelijke is de natuurlijke persoon of rechtspersoon, overheidsinstantie, dienst of ander orgaan die/ dat, alleen of samen met anderen, het doel en de middelen vaststelt voor de verwerking van persoonsgegevens (art. 4 lid 7 AVG). Gemeenten (OM buiten beschouwing) zijn, hoewel ze gezamenlijk optrekken, ieder afzonderlijk verwerkingsverantwoordelijke.

Een verwerker is: "een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt", als staat aangegeven in artikel 4 lid 8 AVG.

Ketenpartner	Privacyrechtelijke positie ketenpartner
Gemeenten	Verwerkingsverantwoordelijke
Politie	Verwerkingsverantwoordelijke
Openbaar Ministerie	Verwerkingsverantwoordelijke

Syntrophos[2]	Verwerker
Sigmax[3]	Verwerker

Partijen die gelden als verwerker voeren enkel gegevensverwerkingen uit voor zover zij daartoe opdracht en aanwijzingen hebben gekregen van de gemeenten. Met deze partijen moeten verwerkersafspraken zijn gemaakt waarin onder meer de gegevens die verwerkt worden, de doelen daarvan en de afgesproken maatregelen vastliggen.

Hoogstwaarschijnlijk is alleen Syntrophos relevant voor dit proces als zijnde verwerker voor de opslag van die persoonsgegevens, tenzij zij niet bij de opslag is betrokken en alleen de randapparatuur (computers, netwerklijnen, beveiliging etc.) levert.

Daarnaast delen (voor wat betreft verstrekkingen *tussen* verwerkingsverantwoordelijken) de gemeenten enkel beeldmateriaal met OM en politie. De overige partijen zijn ketenpartners in het werkveld van de BOA's en ontvangen – in beginsel – geen bodycambeelden.

1.4 Persoonsgegevens

Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon wordt aangemerkt als persoonsgegeven (artikel 4 AVG). Denk dan bijvoorbeeld aan:

- NAW-gegevens;
- Woonsituatie;
- Verblijfsstatus;
- burgerlijke staat;
- e-mailadres;
- pasfoto.

De persoonsgegevens die worden verwerkt in de context van de veiligheid van de BOA kunnen ook gevoelige informatie omvatten. Dit treft mogelijkerwijs andere burgers, en behelst bijvoorbeeld bezittingen zoals woningen of tuinen enzovoorts.

De AVG maakt onderscheid tussen normale persoonsgegevens, bijzondere persoonsgegevens en overige wettelijke categorieën (zoals het BSN en strafrechtelijke gegevens). Op het verwerken van bijzondere persoonsgegevens rust in beginsel een verwerkingsverbod. Dit zijn gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, biometrische of genetische gegevens met op het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, iemands seksueel gedrag of seksuele gerichtheid. Dit verbod is echter niet absoluut, er gelden uitzonderingen die het mogelijk maken om deze gegevens te verwerken (art. 9 lid 2 AVG).

Doordat een bodycam filmt kan het zijn dat er onbedoeld toch bijzondere persoonsgegevens worden verwerkt. Hierbij kun je denken aan het verwerken van gegevens waaruit de gezondheid of gezondheidstoestand van een betrokkene valt af te leiden[4]. Denk bijvoorbeeld aan een betrokkene die

[2] Syntrophos is het Shared Service Centre van de vier gemeenten op Voorne-Putten. Syntrophos zorgt o.a. voor de ICT-huishouding van de gemeenten. Dat zal binnen het proces vermoedelijk niet heel veel anders zijn. Als Syntrophos ook persoonsgegevens zal verwerken, moet zij worden beschouwd als een verwerker in de zin van de AVG.

[3] Het kan zijn dat de gemeenten het gebruik van bodycambeelden hierin registreren. Gemeenten hebben al verwerkersovereenkomsten met deze partij afgesloten.

[4] Heel strikt genomen betreft dit de zienswijze van de Autoriteit Persoonsgegevens en definitie van artikel 9 AVG. Wij denken dat binnen deze context de gegevens vooral als gevoelig moeten worden gekwalificeerd en niet zozeer als gezondheidsgegevens. Er worden immers geen ziektebeelden genoteerd.

te zien is in een rolstoel, op krukken rondloopt of een bril draagt. Het ziektebeeld van de betrokkene kan dus aan de hand van de beelden worden afgeleid. Wij beschouwen de bodycambeelden niet als een bijzonder persoonsgegeven[5] in de zin van de AVG.[6]

Daarnaast heeft de camera een optie om het hartritme van drager te monitoren. De gemeenten op Voorne-Putten hebben nadrukkelijk besloten om dit niet in hun werkproces te gebruiken.

De camera's registreren hoofdzakelijk de beelden van burgers die de BOA in een penibele situatie brengen. Die beelden kunnen, ondanks dat zij bijna in geen enkel geval overduidelijk binnen de beschreven juridische categorie van 'bijzondere gegevens' vallen, wel gevoelig zijn. Dat komt door de aard van de beelden en van de mogelijke situaties of incidenten waarvan zij een afspiegeling zijn.

Gebruikte persoonsgegevens binnen het volledige proces

Gewone:

- Locatie (aan de hand van GPS-coördinaten), datum, tijdstip en cameranummer;
- Algemene beelden van – hoofdzakelijk de BOA zelf, van inwoners, van bezoekers en/of toevallige passanten, of van bezittingen.

Gevoelig:

- Beelden waaruit verbaal of fysiek geweld blijkt te zijn toegepast, of die een indicatie geven van een gezondheidstoestand.

Bijzonder:

- Hartritme van de BOA (optioneel).

Overig:

- Strafbare feiten waaruit (meer dan) een redelijk vermoeden van schuld ontstaat.

1.5 Grootschaligheid en categorieën van personen

De betrokken personen van wie gegevens worden verwerkt, zijn alle personen die op wat voor manier dan ook in aanraking komen met de bodycams van de BOA's. Dit kunnen de betrokkenen zijn die pontificaal in beeld komen bij de opname, maar betreft eveneens de personen die op de achtergrond zichtbaar zijn. Bovenal zijn de BOA's zelf in te schalen als betrokkenen onder de AVG.

De verwachting is dat het aantal beelden van de gemeenten betreft enkele tot tientallen beelden per jaar[7] zullen zijn. Dat maakt de gegevensverwerking bij de gemeenten een kleinschalige gegevensverwerking in de zin van de AVG[8].

[5] Zie ook overweging 51 AVG.

[6] Cameratoezicht. Beleidsregels voor de toepassing van bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens." Autoriteit Persoonsgegevens, 28 januari 2016.

[7] AVG definieert in de Engelse vertaling hiervoor het aantal 'records'. Wij vertalen dit naar het aantal dossiers en niet het aantal documenten.

[8] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-uitleg-over-grootschalige-gegevensverwerking-de-zorg

2 Noodzaak en evenredigheid

Na de systematische beschrijving van het proces en de verwerkingen van de bodycams in hoofdstuk 1, beoordelen wij in dit hoofdstuk – in overeenstemming met artikel 35 lid 7 onder b AVG – of deze verwerkingen rechtmatig zijn. Verder bekijken wij of de verwerking van deze gegevens noodzakelijk en evenredig (proportioneel) is, gelet op de verwerkingsdoeleinden. Deze strenge eisen gelden omdat het verwerken van persoonsgegevens mogelijk bepaalde risico's met zich meebrengt voor de persoonlijke levenssfeer van de betrokkene en zijn omgeving.

2.1 Organisatiedoelstelling en doelbinding bodycams

De wet geeft aan dat als er gegevens worden verzameld door een organisatie, zij alleen maar voor het gerechtvaardigde doel waarvoor ze zijn gekregen (of een daarmee verenigbaar doel) mogen worden verwerkt (art. 5 lid 1 AVG). Als gegevens worden verzameld om deze in het kader van de *veiligheid van boa's* in te zetten, dan mogen die gegevens in beginsel alleen maar voor de *veiligheid van boa's* worden gebruikt. Dit vereiste heet doelbinding.

Het doel

De primaire doelstellingen waarvoor de gemeenten op Voorne-Putten bodycams inzetten zijn:

- **Het vergroten van de persoonlijke veiligheid van de BOA;**
- **Het versterken van de bewijslast bij de persoonlijke aangifte of aangifte van de gemeente in zijn rol als werkgever.**

Het versterken van de veiligheidspositie van de BOA omhelst niet enkel fysieke veiligheid. Door de bodycam en diens rechtszekerheid en bewijsondersteuning groeit ook het gevoel aan persoonlijke veiligheid. De vier gemeenten hebben reeds ervaring met een aantal incidenten waarin dat laatste in het geding was. Wanneer bijvoorbeeld de verbalisantenverplichting onvoldoende bewijs opleverde voor een strafrechtelijke vervolging.

Daarnaast gaf één gemeente aan dat het gevoel van onveiligheid werd versterkt door het ontbreken aan voldoende mankracht in de avonduren en de lange aanrijdtijden van de politie en andere hulpdiensten. Het kunnen gebruiken van de beelden voor bewijslast voor een aangifte, vergroot daarom eveneens het gevoel van veiligheid van de BOA.

Bovenstaande doelen zijn op voorhand bepaald en uitdrukkelijk beschreven. Inzet van bodycams ten behoeve van dergelijke doeleinden is al vaker legitiem geacht[9], aldus de VNG[10].

Doelbinding

Kort samengevat hebben de gemeenten op Voorne-Putten er een belang bij om voor haar werknemers een veilige werkomgeving te garanderen. Dit vloeit voort uit verplichtingen en bestaande wensen rondom het streven naar 'goed werkgeverschap'. Ondersteuning in de bewijslast draagt indirect bij aan het veiligheidsgevoel van de BOA.

Gebruik van het beeldmateriaal/ de persoonsgegevens op een wijze die onverenigbaar is met deze doelen, is daarmee uitgesloten[11]. Bij het laatste kunt u denken aan de inzet voor het bewaken van de openbare orde. De verwerking moet primair bijdragen aan het vergroten van veiligheid bij BOA's (of

[9] Oratie Sander Flight bij de VNG: Het gebruik van bodycam voor gemeenten, 9 februari 2021.

[10] Zie VNG FG-Spreekuur Publiek Cameratoezicht deel II, het gebruik van bodycams voor gemeenten, 9 februari 2021.

[11] Dat geldt dus Openbare orde, veiligheid, politietaken in de zin van Politiewet, sociale recherche enzovoorts.

aan daarmee verenigbare nevendoeleinden).

Verenigbaar gebruik
Een verdere verwerking van de beelden is in sommige gevallen mogelijk. Omdat persoonsgegevens alleen voor nevendoeleinden mogen worden gebruikt als deze "verenigbaar" zijn met het doel waarvoor de persoonsgegevens oorspronkelijk werden verzameld, moet eventueel nevengebruik worden onderworpen aan de verenigbaarheidstoets. Die eisen zijn:

a) Welk verband is er tussen het oorspronkelijke verzameldoel en het nieuwe doel?
b) Wat is het kader van de oorspronkelijke verzameling (met name de verhouding tussen de verwerkingsverantwoordelijke en de betrokkene)?
c) Wat is de aard van de persoonsgegevens?
d) Wat zijn de mogelijke gevolgen van deze verwerking?
e) Welke passende waarborgen (waaronder versleuteling en pseudonimiseren) zijn er ingebouwd?

1. Het gebruik van bodycambeelden ten behoeve van het versterken van bewijs bij incidenten met verbale of fysieke agressie onderschrijven wij als het enige primair verenigbaar gebruik, mits er voldoende passende waarborgen worden getroffen en in de volledigheid zijn ingebouwd. Hierbij kunt u onder andere denken dat de verstrekking van beelden veilig verloopt en dat de gemeenten op Voorne-Putten en de politie hierover afspraken maken.

2. Het gebruik van bodycambeelden ten behoeve van training en opleiding van de BOA onderschrijven wij als secundair verenigbaar gebruik, mits er aanvullende passende waarborgen worden getroffen en in de volledigheid zijn ingebouwd. Hierbij kunt u onder andere denken aan het pseudonimiseren[12] van beelden. In Bijlage 1 hebben wij die juridische onderbouwing opgenomen.

2.2 Rechtmatigheid

Persoonsgegevens mogen enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld (artikel 5 lid 1 sub b AVG). Aan het vereiste 'welbepaald en uitdrukkelijk omschreven' is bij een wettelijk toegewezen rol bij voorbaat voldaan. Voor 'gerechtvaardigde doeleinden' dient artikel 6 van de AVG geraadpleegd te worden. Daar staat dat een verwerking alleen gerechtvaardigd is als deze onder één van de genoemde grondslagen valt.

De vier gemeenten beroepen zich op de wettelijke verplichtingen die op hen als een goed werkgever rust. Goed werkgeverschap is geregeld in art. 7:611 BW.

De Arbeidsomstandighedenwet schrijft daarnaast voor dat een werkgever voor een veilige werkomgeving moet zorgen. Gelet op de overlast door de jeugd en de groeiende ernst van het gebruikte geweld (steekwapens) wordt de kans op fysiek geweld richting de BOA's steeds groter. De gemeenten dienen daardoor te kijken naar middelen die de arbeidsomstandigheden en de persoonlijke veiligheid van de BOA's verbeteren.

Grondslag gerechtvaardigd belang
Voor een legitieme verwerking van persoonsgegevens moet deze gebaseerd zijn op één van zes wettelijke grondslagen uit de AVG. In dit geval is de verwerking gerechtvaardigd doordat de arbeidsrechtelijke verplichtingen die op de verwerkingsverantwoordelijke rusten, worden

[12] Wij kiezen hier voor het pseudonimiseren – als woordkeuze – omdat als er al eerder aangifte tegen de betrokkene is gedaan, dat al wel bekend wie het is. In de praktijk gaat het om het vervormen van beelden, geluid of dergelijke, wat tot anonimiserend moet werken.

onderbouwd in de grondslag *gerechtvaardigd belang* (art. 6 lid 1 onder f AVG). Deze grondslag vereist dat er een belangafweging moet plaatsvinden (zie paragraaf 2.3.), dat de verwerking subsidiair en proportioneel is (zie paragraaf 2.3 en 2.4). In de komende alinea's werken wij de volgende punten uit.

Fundamentele discussie over het gerechtvaardigd belang
PMP opmerkt dat de bovengenoemde grondslag voor de verwerking van persoonsgegevens is vatbaar voor discussie. De grondslag waarop dit te baseren is geenszins eenduidig of duidelijk aanwijsbaar en vergt dus uitgebreide onderbouwing van het gerechtvaardigd belang.

Het feit dat Nederlandse gemeenten voor een soortgelijke inzet van bodycams hun rechtvaardiging baseren op drie verschillende grondslagen (in sommige gevallen vanuit een wettelijke verplichting, vanuit hun openbare taken of vanwege het gerechtvaardigd belang) toont dit verder aan.

Artikel 6 lid 1, laatste volzin AVG beschrijft *dat het gerechtvaardigd belang niet kan worden ingeroepen als de verwerking door overheidsinstanties in het kader van hun openbare taakstelling plaatsvindt*. De reden waarom dit in de AVG is opgenomen is dat voor elke overheidsoptreden altijd een duidelijke wettelijke basis moet zijn. Iets wat ook valt terug te voeren naar het EVRM, EU Handvest en de Grondwet.

Neem het voorbeeld gemeentelijk cameratoezicht en het gebruik van bodycams door de politie. In de onderstaande punten ziet u hoe het werkt:

- In artikel 151c Gemeentewet is de toepassing van cameratoezicht binnen de Nederlandse wet- en regelgeving verankerd.
- Voor de politie biedt artikel 3 Politiewet een grondslag voor de uitvoering van de algemene politietaak, waarin de gegevensverwerking door bodycam als een vorm van niet-stelselmatige observatie is verankerd.

Omdat het gebruik van een bodycam – in dit geval – ondersteunend is aan het vergroten van het veiligheidsgevoel van een BOA, kan het aanzetten van de camera als een verdere verwerking van openbare orde en veiligheid worden beschouwd. Hoewel de vier gemeenten dit niet beogen, kan een burger kan het onderscheid tussen Openbare Orde & Veiligheid en publiek-privaat gebruik niet onderscheiden. De passende waarborgen dienen er dan ook voor om de discussie enigszins voor te zijn.

Hoewel het gebruik van bodycams binnen de visie van PMP past, kan het door de landelijke toezichthouder worden tegengeworpen. Het gebruik van een bodycam door de gemeenten in Nederland moet ook binnen een democratische rechtsstaat op basis van democratisch toegewezen taken en bevoegdheden plaatsvinden. Er zijn dus ook gemeenten die de Autoriteit Persoonsgegevens laten mee kijken bij de inzet van bodycams[13].

Onlangs heeft de Autoriteit Persoonsgegevens nogmaals in het boetebesluit over Wifi-tracking bij Gemeente Enschede benadrukt. Het ontbreken van een juridische basis vormt een zwaar midden-overtreding in de zin van de AVG[14].

[13] BNR Nieuwsradio, 31 augustus 2020, 'Bodycam BOA's staat op gespannen voet met AVG.'

[14] https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/boete-gemeente-enschede-om-wifitracking, geraadpleegd op 7 mei 2021. Het boetebesluit gaat uit van een boetebedrag van €600.000,- voor onrechtmatige wifi-tracking in de binnenstad van Enschede.

2.3 Noodzaak

Welke verwerkingen zijn noodzakelijk om het doel (beschreven in hoofdstuk 2.1) te bereiken? Zijn de gevraagde gegevens écht nodig voor de goede vervulling van de taak die de gemeenten als werkgevers hebben? Deze vragen moeten gesteld worden bij de vormgeving of evaluatie van verwerkingsprocessen. Cruciaal om de noodzaak te bepalen zijn de belangen die spelen en de (positieve dan wel negatieve) impact die verwerken heeft.

Gerechtvaardigde belangen voor de gemeenten en voor burgers

Het verwerken van persoonsgegevens gaat gepaard met de verschillende belangen. Hieronder hebben wij het organisatiebelang (gemeentelijke organisatie/ publiek belang) nader omschreven. In de tweede tabel volgen de persoonlijke belangen.

Organisatiebelang	Toelichting
Goed werkgeverschap[15] *(primaire belang)*	Naast een publieke/ openbare taak die de gemeente uitvoert ten behoeve van haar inwoners, is zij ook een werkgever. Gemeenten voelen zich verantwoordelijk voor de veiligheid van hun werknemers/ ambtenaren (waaronder BOA's). De huidige instrumenten lijken niet voldoende te zijn of kunnen een aanvulling gebruiken om de veiligheid te waarborgen.
Versterken bewijslast *(primaire belang)*	Beelden kunnen versterkend werken bij de bewijslast die hoort bij een aangifte vanuit de gemeente. Wanneer het daaraan ontbreekt, is het soms onduidelijk wat er is voorgevallen. Het is dan woord tegen woord voor wat betreft het incident (BOA tegenover inwoner). Dit zoveel mogelijk voorkomen is in het gemeentelijk belang, omdat het werk van de BOA dan meer impact kan maken en deze zich zelfverzekerder voelt. Met de duidelijkheid die het schept, ben je slepende rechtszaken voor.
Veiligheid van de omgeving (de-escalatie/ preventie, verhogen) *(bijeffect)*	Aanwezigheid van een camera kan ook de-escalerend of preventief op de omgeving werken. De mate van agressie die zich in de gemeente voor kan doen, kan zo voor een deel afgeremd worden. Dat komt ook ten goede van de openbare orde. Bovendien ontkomt de betrokkene in geval van een incident minder makkelijk aan diens straf of consequenties. Dat leidt op den duur weer tot minder buitensporig gedrag.
Verbetering van de organisatieprocessen *(bijeffect)*	De effectiviteit van (werk)processen van de gemeente is voor een groot deel afhankelijk van de ambtenaren. Een veilige werkomgeving zorgt voor tevreden werknemers; BOA's die zich gesteund en veilig voelen kunnen hun werk beter uitvoeren.
Verminderen van klachten *(bijeffect)*	In de dagelijkse praktijk van een BOA kunnen dingen voorvallen waarover inwoners klagen. Over de precieze toedracht en/of juistheid van afhandeling van een dergelijk incident, kunnen de meningen verschillen. De aanwezigheid van camerabeelden (ongeacht of zij voor dit doel ingezien kunnen worden) kan het aantal klachten verminderen.

Verder staan het persoonlijk belang (BOA's/ inwoners en bezoekers van gemeente) in onderstaande tabel uitgeschreven.

[15] Artikel 7:611 BW

Persoonlijk belang	Toelichting
Veiligheid BOA *(primaire belang)*	De BOA heeft een persoonlijk belang bij het hebben van een veilige werkomgeving. Hierbij horen fysieke veiligheid, een gevoel van rechtszekerheid of ondersteuning wanneer het misgaat en voor zover mogelijk stressvrije uitvoering van werkzaamheden.
Versterken bewijslast *(primaire belang)*	De beelden van de bodycams geven de BOA meer grip op zijn aangifte. Dit geeft de BOA een gevoel van zekerheid en veiligheid, wanneer het aankomt op het woord van de BOA en van de inwoner.
Veiligheid burger *(bijeffect)*	Aanwezigheid van een camera kan de-escalerend werken. De agressie die zich in de gemeente voor kan doen, kan zo voor een deel afgeremd worden. Dat komt het algemene veiligheidsgevoel van inwoners ten goede. Bovendien wordt dat versterkt doordat de BOA zich veiliger voelt in het uitvoeren van zijn werk en zo effectiever kan werken. Deze grotere impact van het werk van tevreden BOA's, verhoogt op haar beurt de algehele veiligheid in de gemeente. Dit is in het belang van de individuele inwoner.
Eerlijkheid/ transparantie *(bijeffect)*	Niet alle incidenten of vormen van agressie zijn weg te nemen met camera's. De beelden kunnen in de afhandeling van een voorval een eerlijkere en transparantere indruk geven. Dit zorgt ervoor dat zowel BOA's als inwoners/ burgers een faire behandeling krijgen.
Traumaverwerking *(bijeffect)*	Bij hele ingrijpende incidenten of voorvallen kan het voor de traumaverwerking van de betrokkenen (BOA's of anderen) geruststellend werken dat er beelden zijn. Deze beelden maken dat er een objectieve weergave van de gebeurtenissen bestaat.

De inmenging in de persoonlijke levenssfeer van de burger moet opwegen tegenover het belang van de veiligheid van de handhaver/BOA. Deze inmenging is toegestaan als er sprake is van een dringende maatschappelijke behoefte. Door de aanwezigheid van de bodycams wordt de veiligheid van de handhavers vergroot. Bodycams bieden daarnaast de mogelijkheid om goed onderbouwd aangifte te doen na een bedreiging of mishandeling op een wijze die niet mogelijk is zonder bodycam. Daarom mag de bodycam worden ingezet en is deze noodzakelijk.

Het noodzakelijkheidscriterium wordt verder ingevuld aan de hand van de drie beginselen: 1) proportionaliteit, 2) subsidiariteit en 3) dataminimalisatie. Het laatste aspect is al aan de orde geweest bij de beschrijving van het doel van de bodycams: het vergroten van het veiligheidsgevoel van de BOA's en het versterken van zijn bewijspositie. Andere primaire doelen zijn uitgesloten. Dit zorgt al voor dataminimalisatie. Ook de passende waarborgen, die in het volgende paragraaf en hoofdstukken 3 en 4 zullen worden besproken, dragen bij aan de dataminimalisatie.

2.4 Evenredigheid

Evenredigheid draait om de vraag: zijn alle verwerkte persoonsgegevens in het proces nodig voor het doel dat wordt uitgevoerd? Voor een deel is hier een 'ja of nee'- antwoord op te geven, en voor een deel hangt de vraag naar evenredigheid samen met de onderbouwing van gemaakte keuzes bij de procesinrichting. Het start met een beoordeling van de effectiviteit van de verwerking, als de verwerking van persoonsgegevens niet bijdraagt aan het voorgenomen doel, is dit niet evenredig.

Daarnaast moet worden beoordeeld of aan de eisen van proportionaliteit en subsidiariteit wordt voldaan. Proportionaliteit verlangt dat de inbreuken op de belangen van betrokkenen in verhouding staan tot het doel van de verwerking. Subsidiariteit betreft de manier waarop de gegevens verwerkt worden; daarbij is het streven een werkwijze waar de privacyinbreuk zo minimaal mogelijk is. Alternatieve methoden die tot een vergelijkbaar of hetzelfde resultaat komen, moeten onderzocht en serieus overwogen zijn.

Effectiviteit

De inzet van camerabeelden kan enkel legitiem zijn, als deze ook daadwerkelijk bijdraagt aan de vooropgestelde, rechtmatige doelen zoals eerder beschreven. De werking van de camerabeelden is in Nederland meermaals onderzocht en is herhaaldelijk bestempeld als een effectief middel.

Het eerst aangetoonde effect dat is vastgesteld betreft *de-escalatie* bij inzet van bodycams door de politie. In opdracht van Politie & Wetenschap is dit onderzocht door wetenschapper Sander Flight[16]. Uit dit deelonderzoek blijkt dat in de basisteams waar bodycams werden gebruikt aanzienlijk minder geweld tegen politieambtenaren plaatsvond. De agenten die bodycams droegen, kregen minder vaak te maken met bedreigingen en lichamelijke agressie[17].

Voor wat betreft het *veiligheidsgevoel* blijkt uit de overige experimenten dat meer dan 80 procent van de agenten ervaart dat de bodycam de-escalerend (ofwel het veiligheidsgevoel verhogend) kan werken. Hoofdagent Nick van den Berge uit Den Haag legt uit: *'Vooral in situaties die uit de hand dreigen te lopen, kan het helpen als ik zeg dat ik opnames maak. Als er geen alcohol of drugs in het spel is, heeft de wetenschap gefilmd te worden vaak een positief effect op het gedrag van mensen.'*[18] Uit het onderzoek blijkt dat agenten de camera's vooral als nuttig ervaren in bekeuringssituaties. Van de dragers zegt 85 procent zich er *veiliger door te voelen* en 73 procent voelt zich gesteund in het werk.

Ook in de gemeentelijke context is de inzet van bodycams reeds getoetst, onderzocht en geëvalueerd. Pilots in Amsterdam en Rotterdam staven deze algemene bevindingen. In Amsterdam is er onderzoek gedaan naar de inzet van bodycams onder handhavers[19] .

Uit de pilot bleek dat het veiligheidsgevoel inderdaad toenam en dat het een effectieve vorm van bewijs leveren bleek. Ook is in Rotterdam in een vergelijkbare pilot gevonden dat agressie en geweld afneemt en veiligheidsgevoelens toenemen; met als kanttekening dat in het geval van fysiek geweld, wanneer mensen onder invloed zijn, minder goed lijkt te werken[20]. Verwacht mag worden dat de genoemde effecten ook op Voorne-Putten het geval zullen zijn.

Burgerpanel

Om evenredigheid van een verwerking te bepalen is *maatschappelijke acceptatie* een andere belangrijke graadmeter. Om de mening van de inwoners te peilen is er gebruik gemaakt van een

---

[16] De mogelijke meerwaarde van bodycams voor politieonderzoek. Flight, S. 2017. Politie & Wetenschap, Sander Flight Onderzoek en Advies
Zie: https://www.politieenwetenschap.nl/publicatie/politiewetenschap/2017/de-mogelijke-meerwaarde-van-bodycams-voor-politiewerk-283/

[17] Adviesrapport Landelijk Project Bodycams; Inzet van bodycams binnen het operationele politiewerk. 2018. Programma Sensing, Landelijk Project Bodycams.
Zie: https://www.politie.nl/binaries/content/assets/politie/nieuws/2019/00-km/eindrapport-inzet-van-bodycams-in-het-operationele-politiewerk.kader_geredigeerd.pdf

[18] Zie: https://www.politie.nl/nieuws/2019/april/23/00-bodycam-waardevol-voor-politie-op-straat.html

[19] Dit is gedaan in opdracht van Gemeente Amsterdam door de afdeling Informatie, Onderzoek & Statistiek. Zie voor meer informatie over hun bevindingen de volgende website: https://openresearch.amsterdam/nl/page/56605/evaluatie-pilot-bodycams/.

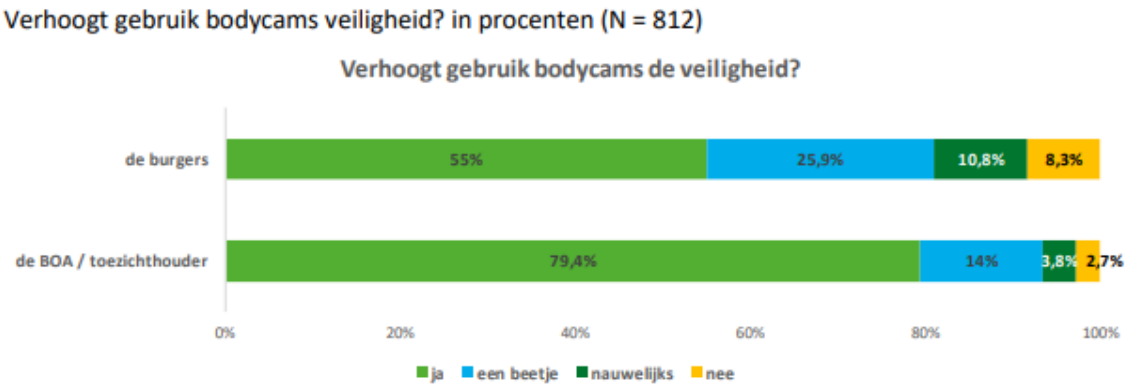
[20] Zie voor een volledig overzicht van de Rotterdamse pilot en de bevindingen: https://sanderflight.nl/wp-content/uploads/2020/01/Evaluatie-bodycams-handhavers-gemeente-Rotterdam-2019.pdf

burgerpanel. Gemeente Nissewaard heeft een enquête uitgezet bij haar burgerpanel over de inzet van bodycams. Hoewel dit niet herhaald is bij de andere gemeenten, geeft dit wel een indicatie van hoe de inwoners op Voorne-Putten denken over de kwestie.

Vergroten veiligheid

Een belangrijke eerste conclusie is dat uit deze enquête is gebleken men over het algemeen denkt dat bodycams de veiligheid vergroten (Figuur 1). Zo is 80% van de respondenten die de enquête hebben ingevuld van mening is dat bodycams de veiligheid van de BOA vergroot. Als je daarbij optelt dat 14% van mening is dat de veiligheid van de BOA 'een beetje' wordt vergroot, komt dat er steun is hiervoor onder ongeveer 94% van de respondenten.

Figuur 1



Een analyse van de antwoorden uit de open vragen wijst uit dat de overige groep (6%) die niet zo sterk gelooft dat bodycams de veiligheid bevorderden vooral denkt aan alternatieven. Zo wordt geantwoord dat BOA's over eigenlijk over nog zwaardere de-escalerende middelen dient beschikken. Hierbij kan je denken aan een wapenstok of pepperspray. Een andere opvatting die in die kleine groep leeft, is dat het dragen van een bodycam beter past bij de taken van de politie dan bij die van de BOA's.

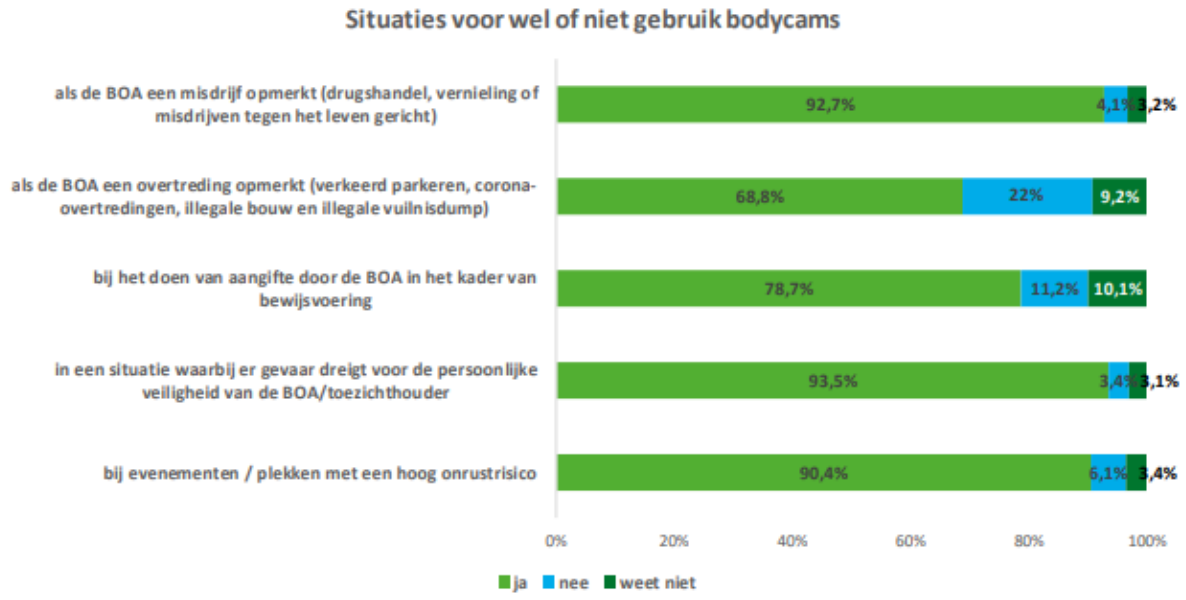
De laatste belangrijke conclusie over veiligheid en bodycams is dat rond de 80% van de respondenten denkt dat de bodycams bijdragen aan de publieke veiligheid (die van burgers).

Inzet bodycam

Het burgerpanel beoordeelt in een aantal geschetste situaties dat bodycams overwegend wél gebruikt kunnen worden. In sommige van de beschreven situaties is er zelfs meer dan 90% steun (zie Figuur 2). De situaties die op de meeste steun rekenen zijn:

1) De BOA een misdrijf opmerkt (zoals drugshandel, vernieling of misdrijven tegen het leven gericht),
2) In situaties waar gevaar dreigt voor de persoonlijke veiligheid van de BOA, en
3) Bij evenementen/ plekken met een hoog onrustrisico.

Figuur 2



Bovenstaande figuur laat zien dat het merendeel van de burgers in alle situaties wel een vorm van inzet van bodycams kan tolereren. Dat betekent dat de gemeenten kunnen rekenen op acceptatie voor de situaties waarin ze bodycams willen inzetten. Vooral met de 93,5% steun voor punt 2) *gevaar voor de persoonlijke veiligheid van de BOA* onderschrijft het Burgerpanel het primaire doel wat de gemeenten voor ogen hebben.

Opvallend is dat punt 1) *opmerken van misdrijf* (waarvoor de bodycams expliciet **niet** zullen worden ingezet) eveneens kan rekenen op maatschappelijke goedkeuring. Uiteraard is in deze korte situatieschetsen niet precies aan de burger uitgelegd hoe de bodycams precies gebruikt worden. In de huidige inzet (zoals beschreven in deze DPIA) is het niet logisch of makkelijker verenigbaar om de beelden voor het opmerken van misdrijven in te zetten.

Indien de bodycambeelden gebruikt gaan worden voor een van de andere doelen of situaties uit Figuur 2, verdient dat een nieuwe, eigen afweging. Dat zouden de gemeenten in een nieuwe DPIA moeten onderzoeken of als uitbreiding op de huidige DPIA toe moeten voegen.

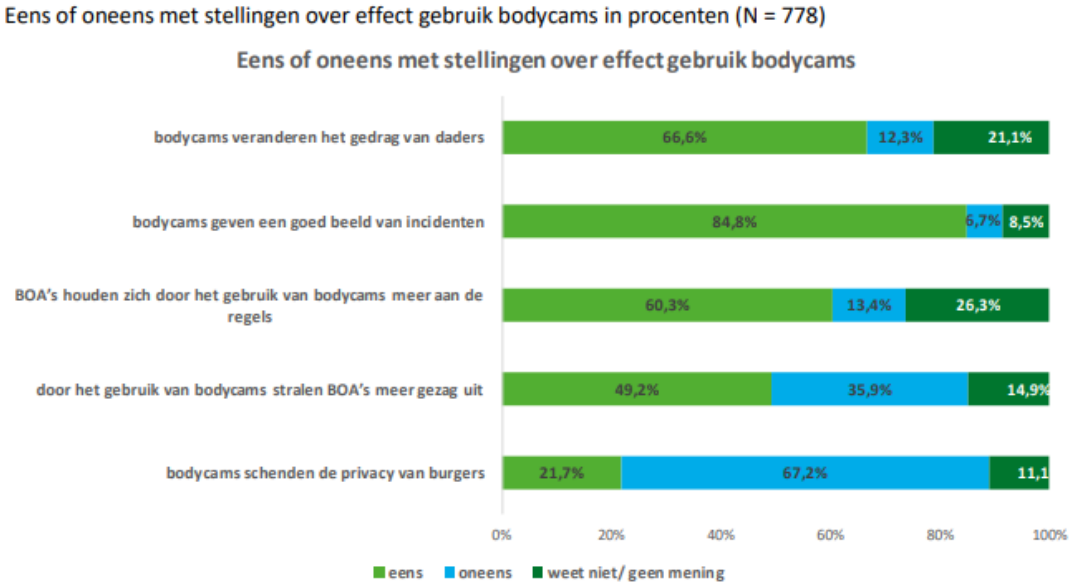
Effect bodycam

Het Burgerpanel is middels een aantal stellingen gevraagd wat zij denken dat het effect is van de bodycam (zie Figuur 3). De stellingen waarmee de hoogste percentages van de burgers instemmen (66,6% en 84,8%) zijn:

1) dat de bodycam een goed beeld geeft van incidenten; en
2) het gedrag beïnvloedende effect van de bodycam.

Figuur 3

Eens of oneens met stellingen over effect gebruik bodycams in procenten (N = 778)



Dit sluit goed aan bij de doeleinden die door de gemeenten zijn geformuleerd bij de voorgenomen inzet. De burgers verwachten effecten van de bodycams op het gebied van de preventieve de-escalerende werking (stelling over verandering van gedrag) en het versterken van bewijslast (stelling over een goed beeld). Een interessante overige bevinding voor de impact voor de burgers is dat een meerderheid van hen denkt dat de bodycams maken dat de BOA's zich beter aan de regels houden en zo de burgers eerlijker benaderen. Het burgerpanel is meer verdeeld over de vraag of de bodycams het gezaghebbende imago van de BOA verder helpen.

Tot slot toont Figuur 3 een significante algemene bevinding die cruciaal is voor de conclusies uit deze DPIA. Voor wat betreft de maatschappelijke acceptatie en de impact ofwel verwachte inbreuk op mensen rechten en vrijheden, laat bovenstaande stelling zien dat:

- slechts 22% van ondervraagde burgers vindt een bodycam een privacyschending van de burger.

Subsidiariteit en proportionaliteit

- De bodycam staat in beginsel uit en filmt dus niet de gehele dienst. In dat geval is er geen sprake van verwerking van persoonsgegevens.
- De bodycam wordt niet geïsoleerd ingezet. De BOA heeft in zijn standaarduitrusting al verschillende middelen tot zijn beschikking. Zo worden alle BOA's getraind op het toepassen van communicatievaardigheden, zoals omgaan met weerstand en agressie, verwarde personen of de-escalerend optreden;
- Bovendien zijn er diverse trainingen op het gebied van weerbaarheid en is er in sommige gemeenten een bikerstraining;
- Daarnaast dragen zij een portofoon om elkaar snel op de hoogte te kunnen stellen;
- een steekwerend vest;
- handschoenen;
- houden zij korte lijntjes met de politiecommandant;
- Voorts hebben de BOA's de mogelijkheid om ook RTGB-trainingen te volgen. Hierbij dient wel te worden opgemerkt dat nog niet elke BOA op Voorne-Putten de trainingen heeft voltooid, dan wel over een dergelijke bevoegdheid beschikt.

Zelfs met het nemen van deze maatregelen gebeuren er nog steeds met regelmaat incidenten waarbij de veiligheid van de BOA in het geding komt. De bodycam moet daarom worden gezien als een aanvullende maatregel om geweldloos op te treden en dat rechtvaardigt het gebruik van een bodycam. De bodycam onderscheidt zich immers van de andere middelen door zijn preventieve werking. Uit de onderzoeken is gebleken dat bodycams een de-escalerende werking hebben op het agressieve gedrag van burgers.

Ook de potentiële en beoogde dragers van de bodycam (BOA's domein 1) staan zelf achter dit middel. Zij hebben hun werkgever – de gemeenten – gevraagd of de bodycam aan hun uniform toegevoegd kan worden. Dit signaal is afzonderlijk van elkaar in de vier gemeenten afgegeven. De BOA's hebben een introductiebijeenkomst bijgewoond waar de bodycam en het gebruik ervan aan hen werd gedemonstreerd. Over het algemeen zijn de BOA's zelf ervan overtuigd dat het middel van toegevoegde waarde kan zijn om het veiligheidsgevoel te vergroten.

Daarnaast worden de bodycams binnen een gezamenlijk afgestemd kader ingezet, waarvoor de vier colleges afzonderlijk goedkeuring geven. De bodycam zal alleen worden aangezet als de situatie naar de mening van de BOA echt dreigend is en het inschakelen ervan agressie kan voorkomen. In de meeste gevallen zullen er ook geen opnamen worden gemaakt.

De opnames die wel gemaakt worden, zullen alleen maar worden bewaard voor zolang dat noodzakelijk is. De gemeente kan de beelden niet langer dan uiterlijk 28 dagen bewaren (of zij moet binnen die 28 dagen de beelden met een bepaalde doelstelling veiligstellen).

De gemeenten beschouwen de beelden als zeer gevoelige informatie en hechten dus waarde aan het treffen van de juiste informatiebeveiligingsmaatregelen conform de Baseline Informatiebeveiliging Overheid. Hierbij kun je denken aan aanvullende eisen voor toegang, strenge autorisaties, (automatische) logging en strikte eisen voor het inzien van beelden.

Daarnaast hebben de gemeenten aangegeven om de beelden niet voor andere doeleinden te gebruiken dan dat in de DPIA en het inzetkader/protocol Bodycams is beschreven. Bij gebruik van andere doeleinden is een nieuwe DPIA écht vereist.

Wij denken derhalve dat het praktisch gebruik van bodycams te rechtvaardigen is, mits er passende waarborgen (zoals beschreven in hoofdstuk 4) voor de rechten en vrijheden van burgers (zoals vastgesteld in het volgende hoofdstuk) worden getroffen. De legitimiteit kan door het recente handelen van de toezichthouders nog wel ter discussie staan (zie voor de uitleg en implicaties voor de organisatie de andere paarse tekstvakken eerder in hoofdstukken 2 en 4).

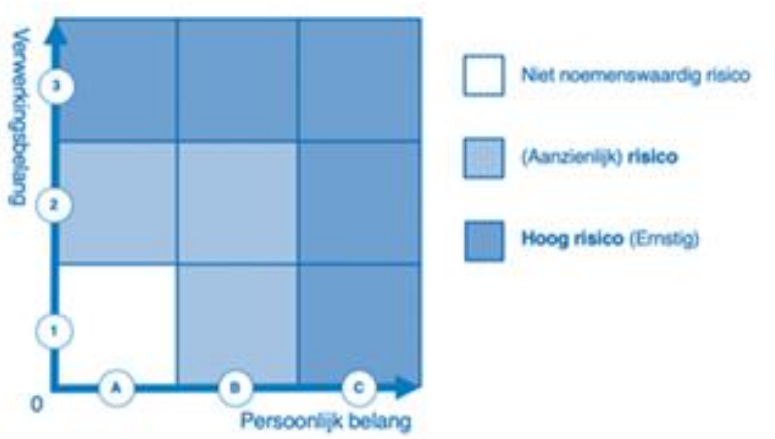
3 Risico's voor rechten en vrijheden

Op basis van de impactanalyse in de DPIA kan de zwaarte van benodigde beheersmaatregelen worden vastgesteld. Een impactanalyse is een beoordeling van de risico's en baten die er kleven aan de verwerking van persoonsgegevens. Aanvullend daarop nemen we de risico's voor de organisatie hierin mee. De AVG schrijft dit niet voor, maar dergelijke risico's zijn wel relevant voor de bepaling van beheersmaatregelen. Op basis van de impactanalyse kunnen passende beheersmaatregelen worden genomen.

3.1 Risicoclassificatie

Voor evenwichtige en rechtmatige inrichting van het proces dienen zowel de mogelijke privacyimpact voor betrokkenen als de organisatierisico's die aan het proces kleven inzichtelijk te zijn. Deze zijn bepalend voor hoe zwaar moet worden ingezet op beheersmaatregelen. Hoe groter de risico's, hoe robuuster die beheersmaatregelen dienen te zijn.

Voor verwerkingsprocessen in een organisatie maken wij gebruik van de hiernaast afgebeelde risicomatrix (*'De Schaal van Erg'*). Door risico's voor betrokkene en organisatie tegen de assen 'persoonlijke impact' en 'organisatie-impact' af te zetten, ontstaan er risico-scores op basis waarvan ten opzichte van elkaar beheersmaatregelen voor processen binnen een organisatie kunnen worden ingeschaald.



Bij het nemen van beheersmaatregelen als organisatie geeft de risicoscore van een proces een handvat voor de prioritering van het doorvoeren van maatregelen. Deze classificaties worden geduid met 0, of met A1 tot en met C3. De classificaties hangen samen met het gegeven dat de impact op vier niveaus kan worden ingeschat, namelijk geen impact ('0'), een geringe impact ('laag'), een substantiële impact ('midden'), of een ernstige impact ('hoog'). De mate van impact kan onevenredig zijn.

De risicoscore A3 duidt bijvoorbeeld op een ernstig organisatierisico, terwijl de persoonlijke risico's gering zijn. Hiervan kan bijvoorbeeld sprake zijn bij grote media-aandacht voor een blunder die door de gemeente begaan is zonder grote gevolgen voor de betrokkene. Om de risico-matrix voor de classificatie 'hoog' hier verder te verduidelijken:

- Ernstige persoonlijke risico's zijn een 'C' op de horizontale as. Het gaat om levensverwoestende risico's. Bijvoorbeeld ernstige persoonlijke beschadiging in sociale context (gevaren voor de persoonlijke veiligheid of gezondheid of ernstige financiële schade (faillissement));
- Ernstige organisatierisico's zijn een '3' op de verticale as. Het gaat bij deze risico's om grote imagoschade, wethouder of burgemeester die in opspraak komt, hoge kosten door het uitkeren van schadeclaims, juridische kosten of zware (bestuurlijke) handhavingsmiddelen van de Autoriteit Persoonsgegevens.

3.2 Risico's voor de rechten en vrijheden van betrokkenen

Hieronder treft u een overzicht van de mogelijke risico's aan. Deze risico's worden beschreven in de overwegingen 75 – 76 van de AVG. De AVG beschrijft in deze overwegingen het volgende:

'Het qua waarschijnlijkheid en ernst uiteenlopende risico voor de rechten en vrijheden van natuurlijke personen kan voortvloeien uit de gegevensverwerking die kan resulteren in ernstige lichamelijke, materiële of immateriële schade.'

Hieronder leest u in de tabel over de soorten schade die betrokkene kan overkomen:

Risico		Wat wordt hiermee bedoeld?
1.	***Bescherming van de lichamelijke integriteit***	Een persoon raakt gewond, zwaargewond of komt te overlijden. Maar denk hierbij ook aan psychische schade of depressies.
2.	***Misbruik van extra kwetsbare personen zoals ouderen, vluchtelingen of kinderen***	Er wordt misbruik van de zwakke situatie van deze personen gemaakt, waardoor deze personen door hun maatschappelijke positie/status in extra moeilijkheden dreigen te komen (ouderenmishandeling, uitzetting (politieke) of detentie vluchteling of kindermisbruik).
3.	***Financiële schade***	Een persoon lijdt op geld waardeerbare materiële of immateriële schade.
4.	***Sociale schade of carrière beschadiging***	Een persoon wordt gezien als het 'zwarte schaap' waardoor de persoon in kwestie in een sociaal isolement wordt geplaatst of er gevolgen voor zijn/haar carrière zijn.
5.	***Ongelijke behandeling***	Een persoon wordt gediscrimineerd, gestigmatiseerd of wordt gezien als een paria en wordt door die status ongelijk behandeld.
6.	***Uitsluiting van een recht of dienst***	Spreekt voor zich.
7.	***Inmenging in privéleven***	Er wordt inbreuk gemaakt op het gezinsleven, communicatiegeheim, huisrecht van een persoon.
8.	***Schending van het beroepsgeheim***	Een ambtenaar of arts maakt informatie bekend die hij uit hoofde van zijn beroep niet bekend mag maken.
9.	***Schending communicatiegeheim***	Met 'vertrouwelijk', 'intern' of 'geheim' geclassificeerde informatie is voor derden inzichtelijk. Denk hierbij ook aan het afluisteren door andere instanties.
10.	***Aanzienlijk economisch of maatschappelijk nadeel***	Een persoon raakt een geldbedrag kwijt, komt in de schuldhulpverlening terecht of raakt failliet. Een maatschappelijk nadeel heeft nadelige gevolgen voor de maatschappelijke positie die persoon bekleedt.

De waarschijnlijkheid en de ernst van het risico voor de rechten en vrijheden van de betrokkene moeten worden bepaald onder verwijzing naar de *aard*, het toepassingsgebied, *de context* en de *doeleinden van de verwerking*. Het risico moet worden bepaald op basis van *een objectieve beoordeling en vastgesteld* moet worden of de verwerking gepaard gaat met *een hoog risico voor de rechten en vrijheden van betrokkene(n)*. In de workshop zijn de risico's zoals hierboven beschreven ingeschat in samenspraak met de BOA's, afdelingsleiders, vertegenwoordigers van de OR en Syntrophos.

3.3 Scenario's

De risicoworkshop met de drie gemeenten[21] heeft een aantal scenario's opgeleverd. Binnen deze scenario's vormt gegevensbescherming een issue; daarbij is er een bepaalde impact als de verwerking zonder beheersmaatregel wordt uitgevoerd. Wij hebben deze scenario's uitgeschreven en gekoppeld aan de hierboven beschreven privacyrisico's. PMP kiest ervoor om vooral scenario's uit de praktijk in de risicobeoordeling mee te nemen. De theoretische scenario's die zich niet in het werkveld voortdoen, dan wel de scenario's die erg onwaarschijnlijk zijn, nemen wij niet mee in de risicobeoordeling.

[21] Brielle heeft de mogelijkheid om in deze versie nog een aantal scenario's toe te voegen.

Scenario 1: *Onvoldoende bewijs voor vervolging*

Een jeugdige is met een scooter wheelies aan het maken. De lokale BOA kiest ervoor om de jeugdige aan te spreken en te wijzen op mogelijke gevaren. Daarop vertoont de jeugdige verwerpelijk gedrag om de BOA uit te lokken. Dit escaleert en de scooterbestuurder rijdt met zijn scooter in op de BOA. Vanwege deze situatie komt er met spoed assistentie vanuit de hulpdiensten. Wanneer de jeugdige wordt verhoord ter zake poging van zware mishandeling tegen een buitengewone opsporingsambtenaar, geeft deze aan dat het inrijden op de BOA niet bewust is voorgevallen. De verbalisantenverplichting van de BOA bleek voor het Openbaar Ministerie onvoldoende bewijs voor het vervolgen van de jeugdige.

AVG-risico voor betrokkene(n)	**Gerelateerd aan:**
1. *Bescherming lichamelijke integriteit*	Er werd op de BOA ingereden, waardoor hij zwaargewond raakte.
2. *Beschadiging van carrière en/of sociale schade*	Door het inrijden en zijn verwondingen was de BOA in kwestie enkele weken uitgeschakeld.
3. *Aanzienlijk maatschappelijk nadeel*	Dergelijke incidenten zoals hierboven staan omschreven, dragen bij aan de verkeerde beeldvorming van de BOA.
4. *Inperking van het recht van werk*	Door dit ongeluk heeft de BOA niet kunnen werken.

Scenario 2: *Filmen op het strand*

Tijdens een hittegolf in de zomer is het druk op het strand. De bezoekers koelen af in het zand. Vanwege de drukte is er handhaving nodig. Wanneer een aantal BOA's een groep beschonken strandbezoekers vraagt hun rommel op te ruimen ontstaat er een dreigende situatie. Niet ver bij het incident vandaan ligt er een vrouw topless te zonnen. Een BOA besluit de camera aan te zetten en beelden op te vragen.

AVG-risico voor betrokkene(n)	**Gerelateerd aan:**
1. *Misbruik van kwetsbare personen zoals kinderen*	Voor de omstanders kan hun naaktheid of dat van hun kinderen erg kwetsbaar zijn. Wanneer daar opnamen van zijn, dan zou misbruik van die beelden kunnen leiden tot een andere interpretatie.
2. *Beschadiging van carrière en/of sociale schade/ financiële schade*	Het bestaan van beeldmateriaal van naakte personen kan veel belangstelling opwekken wanneer deze openbaar raken. Wanneer dergelijk beeldmateriaal eenmaal op internet rondzwerft is het erg moeilijk om het (rechtswege of überhaupt) te laten verwijderen. Dit kan gevolgen hebben voor het verloop van carrière of sociaal leven van die persoon.
3. *Schending van beroepsgeheim*	Het beeldmateriaal van naakte personen kan tevens binnen de gemeente tot interesse en nieuwsgierigheid leiden. In sommige gevallen zijn werknemers bereid gebleken om daarvoor hele strikte autorisatie-protocollen of beroepsgeheim te doorbreken[22].

[22] Zie de zaken van bijvoorbeeld tv-persoonlijkheid Barbie of profvoetballer Robin van Persie.

Scenario 3: *Herschrijven proces-verbaal*

Een BOA heeft een lange werkdag en kan zich niet meer herinneren wat er is voorgevallen. Er deed zich een situatie/ incident voor waartoe hij bevoegd is een boete uit te schrijven. Die bevoegdheid kent allemaal verplichtingen en een heel specifiek kader. Zo moet hij in verband met de verbalisantenverplichting een proces verbaal opmaken. Maar omdat hij geen zin heeft op dat moment zijn proces-verbaal op te stellen, zet de BOA dus zijn bodycam aan. Hij vraagt de volgende dag de beelden op en kan aan de hand van die beelden in alle rust het proces-verbaal schrijven.

AVG-risico voor betrokkene(n)	**Gerelateerd aan:**
1. *Ongelijke behandeling*	De privacy van mogelijke personen die op de beelden voorkomen is onrechtmatig geschonden. Er is namelijk geen rechtsgrond om in dit geval te filmen. Op deze manier worden zij onderworpen aan een ongelijke behandeling.
2. *Aanzienlijk maatschappelijk nadeel*	Oneigenlijk gebruik zoals hierboven beschreven draagt bij aan een negatief beeld van ambtenaren en vergroot wantrouwen in de (lokale) overheid.

Scenario 4: *BOA op huisbezoek*

Een BOA is een gerespecteerd en bekend gezicht in een wijk en kent veel van de spanningen en overlastsituaties die er spelen. Hij heeft met een aantal jonge wijkbewoners een persoonlijke en goede band. Het huisbezoek vormt een belangrijk onderdeel van het onderhouden van die band. Dankzij dit informele bezoek blijft de BOA op de hoogte van mogelijke problemen die bij de jongeren spelen. Wanneer de BOA op huisbezoek wil gaan bij één van de jongeren, schrikken zowel de vader als oudste zoon. 'Met die camera kom je niet binnen.'

AVG-risico voor betrokkene(n)	**Gerelateerd aan:**
1. *Inmenging in privéleven*	Het binnenstappen van een huis is het binnenkomen van een privédomein. Dat kan niet zomaar. Als dat informeel gebeurt, is daar wederzijds vertrouwen voor nodig. Dat vertrouwen is in geding als er een mogelijkheid bestaat dat er opnames gemaakt worden of als het onduidelijk is waarvoor die opnames zijn. De angst van de betrokkene is dat het privédomein publiek wordt.

Scenario 5: *Twijfelachtig functioneren van een medewerker*

Een Teamleider Toezicht en Handhaving maakt zich ernstige zorgen over het functioneren van één van de BOA's. De BOA lijkt steeds vaker dan andere BOA's in allerlei conflicten verzeild te raken. Tijdens het maandelijks 1-op-1 overleg houdt de BOA vol dat het toeval is. Verder vertelt hij dat zich altijd streng aan alle voorschriften en protocollen houdt. Het leidinggevende besluit om alle beelden in zien die de BOA heeft gemaakt. Zo krijgt de leidinggevende een eerlijk beeld van zijn functioneren en besluit de BOA hiermee te confronteren.

AVG-risico voor betrokkene(n)	**Gerelateerd aan:**
1. *Beschadiging van carrière en/of sociale schade*	Het verkeerd gebruik van het beeldmateriaal heeft negatieve gevolgen op de carrière van de BOA, als ook zijn/haar sociale positie binnen het team.

2. *Schending communicatiegeheim/ Beroepsgeheim*	Gegevens (beeldmateriaal) die duidelijk voor een bepaald doel verzameld zijn (veiligheid en aangifte), en dermate geclassificeerd waren en beperkt inzichtelijk, zijn ingezien door een partij die daar niet toe bevoegd was. De betrokkene op die beelden (BOA) had dit niet kunnen verwachten. Het vertrouwen in de bescherming van die beelden is geschonden.

3.4 Organisatierisico's

De potentiële impact van fouten of overtredingen met deze verwerking schatten we op het hoogste niveau in. Het ontstaan van onduidelijkheden of fouten in (of in sommige gevallen het niet uitvoeren van-) de verwerking van persoonsgegevens leidt namelijk tot ernstige gevolgen. Zoals:

- inbreuken op de lichamelijke integriteit of privésfeer, of
- sociale en financiële schade en carrière-beschadiging.

Bovendien kan er ongelijke behandeling van burgers door- of afname van vertrouwen in de (lokale) overheid ontstaan.

Daarbij kan er sprake zijn van maatschappelijke onrust en daaropvolgend een uitvergroting van incidenten in de media, waardoor imagoschade al snel een feit is. Daarnaast is het niet uitgesloten dat de Autoriteit Persoonsgegevens (AP) bij oneigenlijk gebruik (zoals bij *scenario 3*) een onderzoek start en/of andere (zware) handhavingsmiddelen inzet.

In de workshops hebben de deelnemers hun input gegeven aangaande de scenario's. Zij hebben daarbij benoemd wat zij in die gevallen als grootste organisatierisico's zien. Als belangrijkste noemen zij:

- Aansprakelijkheidsclaims
- Reputatieschade
- Klachten van de burger

Ontbreken grondslag/ legitimiteitsprobleem
In hoofdstuk 2.4 en bijbehorend tekstvak staat uitgeschreven hoe de juridische grondslag voor de verwerking vooralsnog voor de nodige discussie vatbaar is. De exercitie van een DPIA heeft tot doel heeft de concrete risico's voor de rechten en vrijheden van betrokkenen in beeld te brengen. Een grondslag die voor discussie vatbaar is, levert in beginsel geen (concrete, directe) risico's voor de betrokkene op. Behalve een overkoepelend democratisch risico dat overheden hun bevoegdheden op grond van het gerechtvaardigd belang ongecontroleerd uitbreiden.

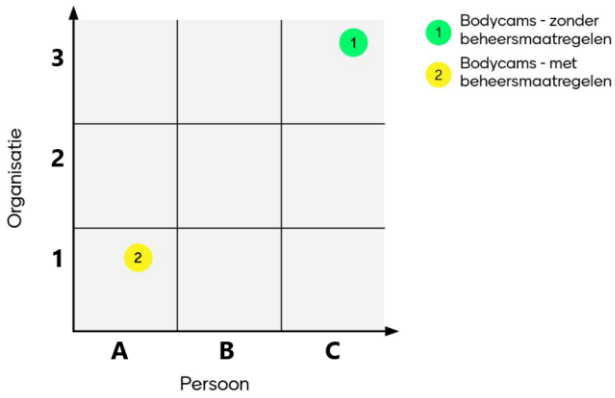
Voor wat betreft de organisatierisico's is er wel concrete aanleiding om te denken dat er negatieve gevolgen optreden. Met name in de handhavingslijn van de nationale toezichthouder is een duidelijk financieel risico te herkennen (zie bijvoorbeeld eerdere verwijzing in hoofdstuk 2 naar aanleiding van de boete voor Gemeente Enschede). Daartegenover staat dat de huidige toepassing van bodycams in andere gemeenten al doorgang heeft gevonden. Het ingrijpen van de AP is daar tot nu toe uitgebleven.

3.5 Risicoscore

Op basis van de risicoschatting en de uitgewerkte scenario's hebben de deelnemers aan de workshops het bodycam-proces een risicoclassificatie gegeven.

De deelnemers hebben het proces Bodycams geclassificeerd als een C3 op de Schaal van Erg. Deze score is vastgesteld op basis van het *bruto risico*. Een risicoscore is op haar beurt bepalend voor de evaluatiefrequentie en de mate van het treffen van passende beheersmaatregelen.

Als de gemeenten het risico met de beoogde maatregelen voldoende weet te verkleinen, dan zou het proces en het *netto-risico* een A1 op de Schaal van Erg kunnen scoren.



3.6 Risicobeoordeling Functionaris Gegevensbescherming

De FG's hebben in hun voorlopige zienswijze[23] zes specifieke risico's voorzien en beschreven. Hieronder hebben wij de FG-zienswijze letterlijk overgenomen. Puntsgewijs zijn de thema's waar volgens de FG's risico's te voorzien zijn:

- Heimelijk filmen
- Opnames verwerkt door onbevoegde gebruikers
- Hackers
- Inzet voor andere doeleinden
- Chilling effect
- Gezichtsherkenning

1) Heimelijk filmen
Het is verboden om heimelijk filmopnames te maken (art. 441b en 139f Sr). De AVG verplicht daarnaast om betrokkenen actief te informeren (transparantie) over de gegevensverwerking. De schade voor betrokkenen als er heimelijk wordt gefilmd kan ernstig zijn en de kans dat dit gebeurt is niet onaannemelijk: dus is sprake van een hoog risico.

[23] Zie zienswijze FG's Voorne-Putten op Quick Scan Inzet Bodycams d.d. 2 februari 2021

2) Opnames worden verwerkt door onbevoegde gebruikers
Onbevoegde medewerkers kunnen bijvoorbeeld over de schouder meekijken bij het terugzien van de beelden of hier zelfs een filmpje van maken met hun telefoon. De handhaver zou ook zelf een filmpje kunnen maken tijdens het terugzien. Ook kan de bodycam worden gestolen of kwijtraken. Beelden kunnen op social media worden geplaatst. Misbruik van opnames, afpersing of aantasting van de goede naam kunnen dan het gevolg zijn. Ook het vernietigen door onbevoegden kan schade opleveren, zeker als er mogelijk bewijs wordt vernietigd. Al met al ernstige scenario's die, zonder passende maatregelen, kunnen plaatsvinden en dus een hoog risico kunnen opleveren.

3) Hackers
Hackers kunnen toegang krijgen tot de opnames. De opnames zouden dan kunnen worden gebruikt om mensen af te persen of hun goede naam te schaden. In dat geval kan de schade voor betrokkenen of handhavers aanzienlijk zijn. De kans dat dit zich voordoet is weliswaar klein maar niet denkbeeldig. Er is een reële kans op schade wat een risico in de categorie 'gemiddeld' oplevert.

4) Inzet voor andere doeleinden
Bodycams kunnen ook voor andere doelen dan het vergroten van de veiligheid van de handhavers worden gebruikt. Dat wordt ook wel 'function creep' genoemd: na verloop van tijd wordt beschikbare technologie ook toegepast voor andere doelen. Dat zou zich bijvoorbeeld kunnen voordoen als handhavers APV-overtredingen gaan filmen met de bodycam om hiermee bewijsmateriaal te verzamelen. Het risico valt in de categorie 'gemiddeld', want de schade voor betrokkenen kan behoorlijk zijn als dit gebeurt en het is niet denkbeeldig dat het zich zal voordoen.

5) Chilling effect
Handhavers die een bodycam dragen kunnen hierdoor minder benaderbaar zijn; het zogenaamde chilling effect. Juist door een goed contact met burgers komen handhavers te weten wat er speelt op straat. Het is daarom belangrijk dat burgers zich vrij voelen om een praatje te maken met een handhaver zonder angst om gefilmd te worden. De kans dat dit scenario zich voordoet is reëel en de schade is aanzienlijk: het risico is hoog dus.

6) Gezichtsherkenning
De afspraak is dat bodycams geen bijzondere gegevens verwerken. Maar er zullen ongetwijfeld bodycams op de markt komen die gezichten kunnen herkennen en aan gemeenten aangeboden worden die bodycams gebruiken. Gezichtsherkenning is een vorm van biometrische gegevensverwerking die in beginsel verboden is. Omdat deze gegevens uniek zijn, net als vingerscans, leven ze een hoog risico op. De kans dat dit gebeurt is niet waarschijnlijk, maar de mogelijke schade is ernstig. Daarom levert dit een 'laag' risico op.

3.7 Risicoverkleinende maatregelen

Kijkend naar de pijnpunten die door de FG's zijn beschreven en de scenario's die in de risicoanalyse naar voren zijn gekomen, kunnen de benoemde risico's worden verkleind door:

1) Het duidelijk aan te geven waar je door de bodycam gefilmd wordt, dan wel aan te kondigen dat de camera wordt aangezet.
2) De gemeenten moeten duidelijke informatiebeveiligingsmaatregelen nemen. Die maatregelen zien vooral toe op toegang naar beelden, logging, bewustwording en autorisaties.
3) Om te voorkomen dat de gegevens voor andere doeleinden wordt gebruikt, dient de gemeente in haar protocol haar beoogde doelstellingen benoemen. Die doelstellingen omvatten ook de kaders wanneer de camera door de BOA wordt aangezet.

4) Om te voorkomen dat er een chilling effect zou kunnen plaatsvinden, dienen de BOA's af te wegen of in sommige situaties (zoals de huisbezoeken) de bodycam aangekondigd dient te worden. Een andere afweging kan zijn om de bodycam niet mee te nemen.
5) Leg geen databases van gezichten aan, zodat gezichtsherkenning nooit een rol of een argument bij de inzet van bodycams vormt.
6) Informeer de burger over hoe de gemeenten de bodycam zullen inzetten.

3.8 Mogelijke restrisico's

Als wij rekening houden met de handhavingslijn van de Autoriteit Persoonsgegevens in het Boetebesluit Wifi-tracking bij Gemeente Enschede[24], dan moeten gemeenten rekening met het feit dat ook andere zaken kunnen gebeuren waarin de inzet niet is voorzien. Het gaat hier om theoretische restrisico's, die zich kunnen manifesteren.

- De gemeenten vertrouwen bij de inzet van bodycams volledig op de professionaliteit van de BOA's. Je kan niet helemaal uitsluiten dat er BOA's zijn die het Protocol Bodycams niet zullen naleven;
- De BOA die besluit om zijn camera niet aan te zetten of op te spelden;
- Leidinggevenden die op basis van *'human bias[25]'* toch een beeld vormen van de professionele houding van de BOA.

[24] https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/boete-gemeente-enschede-om-wifitracking, geraadpleegd op 7 mei 2021. Het boetebesluit gaat uit van een boetebedrag van €600.000,- voor onrechtmatige wifi-tracking in de binnenstad van Enschede.

[25] Een vorm van vooringenomenheid, bevooroordeeld dan wel foutieve gedachtegang, omdat je dergelijke beelden ziet. Houd wel in de gaten dat het niet de bedoeling is dat deze beelden hierin een rol spelen.

4 Beheersmaatregelen

4.1 Inleiding

Na de bepaling van de privacyimpact en risico's in het vorige hoofdstuk, beschrijven wij in dit hoofdstuk de beheersmaatregelen. De beheersmaatregelen zijn nodig om de privacycompliance in het gebruik van bodycams te waarborgen. De analyse wordt gedaan aan de hand van de tien basisprincipes van privacy[26], waarbinnen de beheersmaatregelen worden genomen. Het gaat om de volgende tien principes:

Principes	AVG	(Waar)borging
1. Sturing & toezicht	IV	Bestuurlijk **artikel 24 AVG**
2. Risico management	IV	
3. Transparantie	II III	
4. Rekenschap	II IV	
5. Privacy-services	III	
6. Legitimiteit	II	Operationeel **artikel 25 AVG**
7. Doelbinding	II	
8. Proportionaliteit & opslagbeperking	II	
9. Informatiekwaliteit	II	
10. Informatiebeveiliging	II	

Deze beheersmaatregelen bieden bescherming tegen problemen die redelijkerwijs voorzienbaar zijn. Dat ze *passend* zijn houdt in dat ze daadwerkelijk effectief zijn, maar ook dat ze werkbaar en redelijk zijn. De DPIA betreft in eerste instantie een onderzoek op het operationele vlak (principes 6 t/m 10). Toch kan een DPIA ook bestuurlijke aanbevelingen (principes 1 t/m 5) bevatten, voor zover het ook een bestuurlijke aangelegenheid betreft.

[26] De meeste basisprincipes staan in hoofdstuk 2 AVG 'Beginselen over verwerking van persoonsgegevens, maar zijn ook elders terug te vinden. Vgl. OECD Privacy Guidelines. De Romeinse cijfers corresponderen met de hoofdstukindeling van de oorspronkelijke AVG-wettekst uit 2017.

Let op:
De beschreven beheersmaatregelen om volledig aan de wet te voldoen gaan uit van een degelijke juridische basis. Zoals al vaker in de paarse balken is opgemerkt; er valt hier over te discussiëren. Die discussie gaat nog meer op als een gemeente besluit om de bodycam voor Openbare Orde en veiligheid te gebruiken.

Mocht de afweging gemaakt worden dat er toch met de toepassing gestart wordt, dan zijn onderstaande maatregelen naar ons inzien voldoende voor een legitieme, praktische uitvoering. Voor volledige compliance aan de AVG en nationale wetgeving moet die juridische basis verbeteren. Dit kan onder andere doordat de AP met een zienswijze of boetebesluit een kader schetst. Anders bestaat er nog steeds een reëel risico op handhaving door de toezichthouder (zie hoofdstuk 3.4).

Wanneer er voor een verwerking van persoonsgegevens na de afwegingen gemaakt in een DPIA mét bijbehorende mitigerende maatregelen, steeds nog risico's of gaten in de juridische basis blijven openstaan dan schrijft de AVG een voorafgaande raadpleging bij de AP (artikel 36 AVG). In overleg met de AP kan besproken worden wat een acceptabel risico of correcte werkwijze is.

- Onze inschatting is dat in dit geval een voorafgaande raadpleging er toe leidt dat de AP de huidige grondslag niet zal accepteren. Het gevolg is dat het volledig stilleggen van de verwerking dan een kansrijke uitkomst is;
- Een andere optie is het afwachten tot dat er passende wetgeving is. De juridische basis voor de verwerking kan gecreëerd worden door een aanpassing/ aanvulling van de Gemeentewet (bijvoorbeeld in een nieuw art. 151 ca Gemeentewet). Hoelang het duurt voordat dit rond is, is moeilijk in te schatten;
- De laatste optie is met de verwerking starten. Hierbij dient u wel alle aanbevelingen uit dit rapport, in de wetenschap dat er over de grondslag valt te discussiëren, wel overnemen. Bij inmenging van de AP adviseert PMP ook om op te trekken met de andere gemeenten die de bodycams hebben geïmplementeerd.

Het is dus aan ieder college afzonderlijk om hierin een keuze te maken.

Wij adviseren daarom de volgende aandachtspunten in stand te houden:

- De gemeenten hebben al een protocol voor het gebruik van bodycams geschreven;
- Blijf de BOA's betrekken bij het maken van beleidsmatige instructies;
- De gemeenten beschikken over afdoende controlemechanismen om het nieuwe proces verder goed vorm te geven.

En adviseren om de volgende aandachtspunten in het verbeterproces mee te nemen:

- De gemeenten beschikken nog niet over een duidelijk en concreet werkproces 'Verwijdering Bodycambeelden' en 'Verstrekkingen aan politie en/of OM';
- Ga aan de slag met de aandachtspunten m.b.t. de bewaartermijnen;
- Maak een toevoeging op het huidige Privacy Services-protocol m.b.t. camerabeelden;
- Breng het proces verder in lijn met de verplichtingen rondom informatiebeveiliging;
- Ga aan de slag met de aandachtspunten m.b.t. informatieverplichtingen.

4.2 Aanbevelingen met bestuurlijke borging

Bestuurlijke transparantie

Beleidstransparantie hangt samen met Sturing en Toezicht en Rekenschap. Bij beleidstransparantie gaat het over het transparant zijn over de gegevensverwerkingen binnen het proces Bodycams en met welke privacywaarborgen de verwerkingen zijn omkleed. Door de betrokkenen hierover adequaat te informeren, wordt het draagvlak onder hen vergroot en kunnen toekomstige discussies of misvattingen over het gebruik van bodycams worden voorkomen.

1. Verbeter het huidige protocol Bodycams. De verbeterede versie moet onderdelen bevatten over: Hoe gebruik je de bodycams? Wanneer zet je ze aan? Wanneer niet? Op welk moment zet je de camera weer uit? Hoe waarschuw je betrokkenen? Hoe bewaar je de bodycam buiten gebruik? Wat voor afspraken zijn er rondom opslag/ opladen van de bodycam? Hoe stel je de beelden veilig en in welke gevallen?

   Hieronder beschrijven wij tien verbeteringen voor het huidig protocol:

   - Breng het juridisch verhaal geheel in lijn met het juridisch verhaal uit de DPIA (Doelstellingen en juridische termen zoals zij in hoofdstuk 2 zijn benoemd). Dus enkel gebruik voor het vergroten van de veiligheid en versterking van de bewijspositie van de BOA;
   - Beschrijf nadrukkelijk de instructies voor BOA's/ dragers van die bodycam;
   - Beschrijf nadrukkelijk de rollen- en verantwoordelijkheden van de actoren (Teamleiders, BOA's, FG/Privacy Officer);
   - Leidinggevenden Veiligheid, Toezicht en/of handhaving (Proceseigenaren) zijn verantwoordelijk voor het naleven van dit protocol, maar beschikken niet rechtstreeks over de beelden. Richt daarvoor een aparte functie in.
   - Leg in het protocol vast dat de camera standaard op stand-by staat;
   - Aanzetten bij dreigende situatie – wanneer veiligheidsgevoel in geding komt;
   - Definieer de term 'dreigende situatie' aan de hand van de scenario's[27], maar leg ook uit dat de afweging;
   - Beschrijf de instructies voor de BOA nadrukkelijk in dit protocol. Waarschuw dat je hem aanzet, in het proces-verbaal staat genoteerd dat er camerabeelden zijn enzovoorts.
   - Bekijk hoe de BOA en/of gemeente gefilmde betrokkenen achteraf informeert. Een visitekaartje als ze gefilmd zijn, kan een uitkomst zijn. Op het visitekaartje is dan een instructie voor de betrokkene(n) en/of QR-code vermeld.
   - Beschrijf in het protocol aanverwante processen: het inzien van beelden, proces van veiligstellen en doorgifte(n) van die beelden in hoofdlijnen werkt.

2. Voor de FG, CISO en Privacy Officer(s): Adviseer de proceseigenaren bij het vormgeven van het gehele verbeterproces.
3. Laat het protocol voor één jaar vaststellen door ieder college afzonderlijk en informeer de overige stakeholders (Raad, OR en Burgemeesters). Laat daarnaast de OR ook in het kader van het instemmingsrecht ook instemmen over het gebruik van bodycams, aangezien de bodycam ook als een personeelsvolgsysteem kan worden gebruikt.
4. Beschrijf in je protocol nadrukkelijk hoe het proces wordt geëvalueerd en zo nodig wordt verbeterd. Wij stellen voor dat de gemeenten over 6 maanden een evaluatie van de bodycams (zoals in gebruik en gevoel bij de BOA's) doen.

[27] Mail van Linda van der Lugt (Gemeente Nissewaard) over de noodzaak van bodycams d.d. 9 juli 2020. Haar mail biedt hiervoor een goede basis. Soortgelijke incidenten zullen per gemeente ook voor handen zijn.

5. Bespreek het gebruik van bodycams door gemeentelijke BOA's ook met overige stakeholders (voornamelijk OM en Politie). Maak met hen duidelijke afspraken over het gebruik van bodycambeelden (zie aanbeveling 20).

Informatieverplichting

De AVG verplicht dat de vier gemeenten de betrokkenen actief informeren over de gegevensverwerkingen binnen haar proces Bodycams conform artikelen 12 en 13 of 14 AVG. Het actief informeren dient o.a. op de gemeentelijke website (in de privacyverklaring) te gebeuren, maar ook op andere manieren. Op dit moment gaat het informeren over privacy veelal middels de gemeentelijke website.

Op basis van de enquête heeft het burgerpanel aangegeven hoe zij wenst te worden geïnformeerd. Het burgerpanel geeft aan dat de belangrijkste vorm van informeren (60% steun) die in de fysieke situatie (aanbeveling 6) is. Andere geprefereerde informatiekanalen veel genoemd worden (aflopend in populariteit):

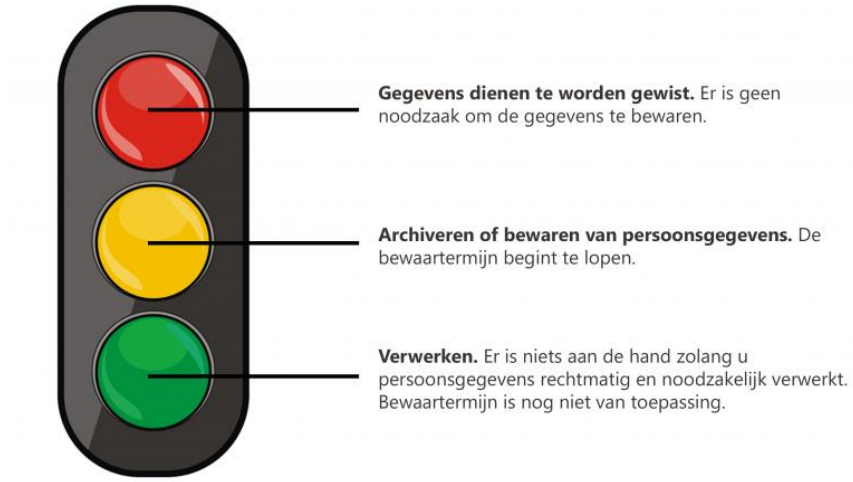
a. een officiële publicatie op de website (34 % steun, aanbeveling 7)
b. informatie via het gemeenteblad (30%), en
c. informatie op (tijdelijke) verkeersborden (29,1%)

Wij adviseren daartoe het volgende:

6. BOA's dienen voorafgaand het filmen aan te kondigen dat zij de bodycam gaan aanzetten. Dit gaat echter niet op in situaties waarin dit niet mogelijk blijkt te zijn.
7. Publiceer op de gemeentelijke website een privacyverklaring omtrent het gebruik van bodycams[28]. Houd rekening met de werking van artikel 12 AVG. Dat benoemt een aantal eisen m.b.t. de publicatie en de vorm.
8. Publiceer ook in hoofdlijnen: de werking van de camera, het inzetkader (wanneer mag de camera draaien), de gemeentelijke doelstellingen van de bodycam, de instructie van de BOA en op welke wijze een betrokkene de beelden kan inzien.

Proportionaliteit en opslagbeperking

De bewaartermijn gaat in na het aflopen van de gebruikstermijn. De gebruikstermijn stopt zodra de dienstverlening is beëindigd. Vanaf dat moment begint een bewaartermijn te afgelopen, begint een bewaartermijn te lopen. Binnen een bewaartermijn kunnen de gegevens nog in zijn huidige vorm worden bewaard. Als de bewaartermijn is afgelopen en er geen redenen zijn om de gegevens te bewaren, dan dienen de gegevens te worden vernietigd. **(Opslagbeperking).**



[28] Gebruik www.nissewaard.nl/privacy of www.zaanstad.nl/bodycam als voorbeeld hoe de gemeenten dat kunnen vormgeven.

9. De gemeenten hebben in hun protocol vrij algemeen benoemd dat hun beelden voor 28 dagen zullen zijn opgeslagen. Wij stellen echter een verscherping voor: de gemeente doet binnen 28 dagen aangifte, en stelt dus binnen die termijn de beelden veilig (mochten zij langer nodig zijn).
10. Die termijn van 28 dagen is niet strijd met de wet of Nederlandse opvattingen van de AVG[29], maar op Europees niveau wordt de zienswijze niet gedeeld[30]. Daarom dienen de gemeenten te onderzoeken of het bewaren van de bodycambeelden korter kan.

    Twee weken (14 dagen) is een andere termijn die binnen de workshops besproken is. Nadat er een tijd is gewerkt met de originele bewaartermijn van 28 dagen, en er ervaring is met de tijdsduur en het verloop van het aangifteproces, moet er een evaluatie plaatsvinden of de termijn verkort kan worden (tot bijvoorbeeld die 14 dagen).
11. Op het moment dat de beelden zijn veiliggesteld, dient de gemeente de beelden te bewaren zolang het nog nodig is. Het stoplicht staat dan op geel. De noodzakelijkheid zit hem dan vooral in de strafrechtelijke bewijsvoering.
12. Als de strafrechtelijke verplichtingen hebben plaatsgevonden en beelden verder geen nut meer hebben, dan dienen de gemeenten de beelden binnen afzienbare tijd te verwijderen. Het stoplicht staat dan op rood.

Rechten van betrokkene(n)

Betrokkenen moeten op een laagdrempelige manier privacyrechten ('privacy services') kunnen uitoefenen en dit moet op adequate wijze worden ingeregeld. Hierbij dient te worden afgewogen of een aanvullende procedure nodig is om te kunnen voldoen aan de vereisten die de AVG hieraan stelt. De volgende (relevante zaken) zijn (deels) al geborgd bij de vier gemeenten op Voorne-Putten:

I. Facilitering van het recht op informatie;
II. Facilitering van het recht op inzage;
III. Facilitering van het recht op aanvulling, correctie;
IV. Facilitering van het recht op verzet (bezwaar);
V. Facilitering van het recht op schadevergoeding bij gebrekkig privacymanagement[31];
VI. Facilitering van beroep bij de Functionaris Gegevensbescherming (ombudsfunctie).

13. De AVG beschrijft het recht van inzage, aanvulling en correctie. De vier gemeenten beschikken al (deels) over dit proces. Maar binnen het proces is het voorzienbaar dat er betrokkene(n) en derde partijen (zoals de politie en OM) om de bodycambeelden vragen. Hoe ga je daar mee om? Zorg daarom voor een goede werkwijze om het in behandeling nemen van dergelijke verzoeken soepel te laten lopen.
14. Het is op grond van de AVG toegestaan om bodycambeelden in te laten zien. Dat betekent echter niet dat het logisch is om de bodycambeelden zonder meer te verstrekken. Een verstrekking is onder het inzagerecht niet mogelijk aan advocaten of betrokkene(n). Wel kunnen beelden worden gedeeld met politie en OM, zij hebben op grond van artikel 30, 31 en 32 Sv het recht om een afschrift van de processtukken van de officier van justitie te ontvangen.
15. Ondanks bovenstaande mag de gemeente echter geen afbreuk aan het inzagerecht doen. Dus hoewel inzage mogelijk moet kunnen zijn, en de AVG omschrijft dat bij het inzagerecht een afschrift of kopie verstrekt moet worden, resulteert dat er niet in dat de beelden één op

[29] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/cameratoezicht/melden-van-cameratoezicht, geraadpleegd op 14 maart 2021. En de AP-beleidsregels cameratoezicht onder Wpb en Wpg 9 februari 2016 (oud, maar nog steeds bruikbaar als een richtsnoer).

[30] European Data Protection Guidelines 3/2019 on processing of personal data through the use of video devices.

[31] Artikel 82 AVG i.c.m. 6:162 BW.

één verstrekt kunnen worden. Wij adviseren in dergelijke situaties dat de beelden *tekstueel* worden verstrekt. Indien er sprake is van een legitieme uitoefening van het inzagerecht, kunnen de beelden bij de gemeente worden ingezien (zoals in punt 15), hiervan worden geen kopieën verstrekt[32]. Wel kan er bijvoorbeeld een afschrift worden gegeven met daarop een korte situationele schets van wat er op de beelden te zien is (een weergave van de gebeurtenissen, geen uitgebreid transcript).

16. Dit proces dient ook een aantal werkafspraken met de Privacy Officer en FG te bevatten. Bijvoorbeeld in welke gevallen de FG betrokken dient te worden, wie de regie heeft en wanneer advies van Privacy Officer gewenst is. Bespreek vervolgens een aantal kaders af. Deze kaders dienen antwoord op de volgende vragen te geven: wat is er technisch en organisatorisch mogelijk om dit recht te kunnen uitoefenen, wat is het tijdspad en welke escalatiemogelijkheden zijn er, enzovoorts.
17. Documenteer de behandelde verzoeken in een register. Maak daarbij ook afspraken over wie het register bijhoudt en bijwerkt.

4.3 Aanbevelingen met operationele borging

Legitimiteit

18. Wij zien in het proces dat er mogelijk 1 verwerker is, Syntrophos. Met Syntrophos moet een verwerkersovereenkomst worden afgesloten (art. 28 lid 3 AVG), indien Syntrophos persoonsgegevens in het kader van de bodycam zal gaan verwerken. Hier moet nog een besluit over worden gevormd. Hierbij kunnen de FG's, CISO en Privacy Officer ondersteuning bieden. **(Sluit een verwerkersovereenkomst met Syntrophos)**.
19. Ook in de beperkte inzet van bodycams uit arbeidsrechtelijke overwegingen, kunnen OM en politie in sommige gevallen beelden opvragen. Het is verstandig met hen af te bespreken wanneer dit wél, maar vooral wanneer dit niet logisch is. Maak heldere afspraken over de gegevensverstrekking tussen verwerkingsverantwoordelijken. De afdeling juridische zaken, FG, CISO en Privacy Officer moeten een rol spelen bij de totstandkoming daarvan **(Maak uitwisselingsafspraken met politie en OM over de bodycambeelden)**.

Informatiebeveiliging

Informatieveiligheid is een basisvereiste voor het voldoen aan de AVG en internationale beveiligingsnormen. De AVG stelt summiere beveiligingseisen, onder meer aan de beveiliging van gegevens, kort gezegd dat de vier gemeenten moeten zorgen voor een passend beveiligingsniveau (art. 32 AVG). Hierbij dienen de gemeenten rekening te houden met belangrijke informatiebeveiligingsbeginselen: **Beschikbaarheid, Integriteit en Vertrouwelijkheid.** Wij adviseren in het kader van informatieveiligheid daarom het volgende:

20. Breng de rollen en verantwoordelijkheden nader in kaart.
    Privacy Officer en/of Functionaris Gegevensbescherming: Deze functies hebben geen bevoegdheid om zomaar beelden in te zien. Zij hebben vooral een toetsende rol in dit proces en houden toezicht of er correct met de gegevens wordt omgegaan en de rechten van de betrokkenen worden gewaarborgd. Daarnaast dienen zij ook betrokken te worden wanneer er een inzage vraag is vanuit de Teamleider, BOA, Politie/OM of betrokkene.

    CISO: De informatiebeveiligingsfunctionaris stelt de autorisatiematrix vast. Hij toetst en houdt toezicht op de naleving van de autorisatiematrix en er geen onbevoegden toegang tot de beelden hebben.

    Beleidsmedewerker Openbare Orde: Deze ambtenaren hebben in principe ook geen reden om de beelden op te zoeken en in te zien. Zij stellen immers beleid op. Er zou eventueel

[32] Onder andere om de privacy te waarborgen van mogelijke andere betrokkenen die op de beelden te zien zijn te waarborgen.

nagedacht kunnen worden of beeldmateriaal gebruikt kan worden als leermateriaal, zodat het beleid rondom bodycams verbeterd kan worden. Het beeldmateriaal dient dan gekozen te worden door iemand die hier bevoegd voor is, zoals de Teamleider.

Teamleider/Teamhoofd Openbare Orde: Bij gegronde reden, zoals wanneer een incident heeft plaatsgevonden, kan de Teamleider de beelden inzien. Hierbij dient nagedacht te worden onder welke voorwaarden dit gebeurt. Denk bijvoorbeeld aan aangifte wanneer een BOA psychisch of fysiek letsel heeft opgelopen. Het beeldmateriaal kan dan de aangifte versterken in bewijs. Ook wanneer er een ernstige klacht vanuit een burger binnenkomt, zouden beelden ter aanvulling ingezien kunnen worden. In beide varianten van belang om eerst zoveel mogelijk te verklaren en op papier te krijgen zonder beeldmateriaal, dit is enkel ter aanvulling.

BOA: De BOA heeft in principe geen toegang tot de beelden. In het geval van een incident waarbij de BOA is betrokken en aangifte wens te doen of bij een ernstige klacht van een burger, kan de betrokken BOA samen met de Teamleider Openbare Orde deze beelden inzien. De beelden kunnen dan bij de eigen aangifte worden bijgevoegd.

Inwoner/Betrokkene: Een betrokkene heeft recht op inzage bij gegronde reden. Een inwoner die niet betrokken is geweest en niet op de beelden staat, heeft geen recht op inzage.

Politie/OM: Deze partijen hebben een vordering nodig om de beelden op te vragen. Daarnaast kunnen de gemeenten bodycambeelden verstrekken bij het doen van aangifte.

21. Maak een plan om de opslag en het inzien van die beelden aan de geldende informatiebeveiligingsnormen – waaronder de Baseline Informatiebeveiliging Overheid (BIO) – te laten voldoen **(Baseline Informatiebeveiliging Overheid)**. Kijk naar de controls uit de BIO en de bijbehorende passende beveiligingsniveaus. **Wij adviseren om de beelden op minimaal BBN-2 niveau te beveiligen, met een aantal aandachtspunten op BBN-3, en daartoe passende maatregelen te treffen**. Binnen deze maatregelen dient men ook (automatische) *logging* toe te passen.

22. In het plan dient ook naar de autorisaties te worden gekeken. Maak daarom een autorisatiematrix voor het toegang tot de beelden.
23. Bepaal wat **de organisatorische maatregelen** zijn bij het inzien van de beelden. Houd daarbij rekening met in elk geval de volgende aspecten:
    a. Verzwaarde geheimhoudingsafspraken met de diegene die beelden rechtstreeks kan inzien;
    b. Verzwaarde geheimhoudingsafspraken met de betrokkene(n) en hun gemachtigde[33];
    c. Maak een kamer/plek voor het uitlezen van die beelden;
    d. Voorafgaand het uitlezen dienen alle apparaten en gegevensdragers te worden ingeleverd. Na afloop van het uitleesmoment kunnen de apparaten weer worden teruggegeven verstrekt;
    e. Houd ook rekening met de beveiligingsmaatregelen voor fysieke veiligheid.

Einde rapport

[33] Dat geldt niet voor advocaten. De gedragsregels advocatuur vereist geheimhouding voor advocaten.

Bijlage 1 Verenigbaarheidstoets Scholing en opleiding

Het verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld, en de doeleinden van de voorgenomen verdere verwerking

Het doeleinde waarvoor de beelden worden gemaakt c.q. verkregen, is omschreven in hoofdstuk 2 van dit document. Dit doeleinde is omschreven als de verplichting om zich als een goed werkgever te gedragen die op de gemeenten rust. Dat is de motivatie voor de gemeenten om de bodycam voor hun werknemers (de BOA's) aan te schaffen o.a. op de verplichtingen om daarmee een veilige werkplek te zorgen[34].

De doeleinden van de voorgenomen verdere verwerking zijn het evalueren van de eigen handelingen of die van zijn collega's binnen de kaders van scholing, training en opleiding die de veiligheid van BOA dient te versterken. Deze doelen liggen in het verlengde van het verzameldoel. Een goed werkgever faciliteert ook de training, opleiding en scholing van de BOA's. Die trainingen kunnen gaan over het toepassen van gesprekstechnieken en escalatieladders om de communicatie en/of gedrag te kunnen beïnvloeden. In die trainingen wordt soms het eigen handelen van de BOA gereflecteerd, waardoor de BOA meer handvatten krijgt om zijn vak beter te verstaan. In dat laatste ligt immers ook als doel besloten om voor een veilige werkplek te zorgen.

Het kader waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkenen en de verwerkingsverantwoordelijke betreft

De BOA's maken deze beelden zodra zij zich fysiek of verbaal onveilig voelen en kunnen de beelden gebruiken om de eigen aangifte nader te onderbouwen. De gemeenten slaan de beelden op en kunnen zelf ook aangifte doen. De persoonsgegevens worden alleen verder gebruikt als steunbewijs. Er is dus wel sprake van een directe relatie tussen de verwerkingsverantwoordelijke voor het verdere gebruik en de BOA. Op die beelden staan ook betrokkene(n) die verbaal of fysiek geweld hebben toegepast.

De aard van de persoonsgegevens met name of bijzondere categorieën van persoonsgegevens worden verwerkt, overeenkomstig art. 9 AVG, en of de persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten worden verwerkt, overeenkomstig art. 10 AVG.

Het gaat niet om bijzondere gegevens, noch om gegevens over strafrechtelijke beoordelingen. Het gaat hier wel om strafbare feiten (mishandeling, geweld tegen ambtenaar in functie, belediging en/of bedreiging van een buitengewone opsporingsambtenaar in functie).

De mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen

Met de voorgenomen verdere verwerking worden voor de betrokkenen (in dit geval de BOA) slechts voor hen gunstige gevolgen beoogd. Bij het gebruiken van de bodycambeelden heeft de BOA ook direct context en inzicht in zijn eigen handelen. De negatieve gevolgen kunnen leiden tot negatieve gedachten bij het tonen van de beelden, schaamte voor het eigen gedrag en/ of handelen.

Het bestaan van passende waarborgen

Dit laatste criterium is van een ander karakter dan de eerste vier, doordat het de mogelijkheid creëert om verenigbaarheid te bevorderen door het nemen van maatregelen. Wanneer we naar de eerste vier criteria kijken, dan pakken deze in het algemeen voor verenigbaarheid neutraal of positief uit.

---

[34] Arbeidsomstandighedenwet

Dat laatste vereist dat er extra zorgvuldig met de gegevens wordt omgegaan, en specifiek (mocht dat aan de orde zijn) dat gebruik van de gegevens wordt vermeden dat niet in lijn ligt met de basis waarop ze zijn verkregen. Waarborgen waaraan gedacht kan worden zijn bijvoorbeeld om extra aandacht te besteden aan:

1. het uitgebreid informeren van de BOA over deze mogelijkheden;
2. pseudonimiseren of vervormen van beelden;
3. opslag van die beelden binnen aparte beveiligde omgeving
4. en om de BOA's een laagdrempelige mogelijkheid te bieden om in te stemmen met het gebruik van dergelijke beelden met een specifiek persoonlijk training – of opleidingsdoelstelling wat bij de toekomstige uitvoering van zijn BOA-taak zal helpen.

Met inachtneming van bovenstaande maatregelen beoordelen wij het beoogde gebruik van de bodycam beelden met betrekking tot individuele scholing of opleiding verenigbaar met de oorspronkelijke verzameldoeleinden.

Privacy
Management
Partners
Coöperatie UA

adres
Vondellaan 58
3521 GH Utrecht

telefoon
+31 85 401 38 66

e-mail
info@pmpartners.nl

website
www.pmpartners.nl

Aan de Colleges van burgemeester en wethouders van de gemeenten
Brielle
Hellevoetsluis
Nissewaard
Westvoorne

Betreft: FG-advies bij de DPIA bodycams voor BOA's, versie 1.0, 12 juli 2021

Datum: 8 september 2021

Geachte colleges,

In vervolg op onze eerdere adviezen op de - nu voorgelegde definitieve versie van de - DPIA, komen wij tot de volgende opmerkingen.

De FG's merken op dat de DPIA tegenstrijdigheden bevat. Met name de in paars aangegeven teksten kunnen bij gemeenten tot verwarring leiden. Deze verwarring is ons inziens niet nodig.

PMP stelt enerzijds dat de bodycams kunnen worden ingezet als preventief middel, ter deëscalatie van een situatie waarin de BOA zich onveilig voelt, en als dit niet helpt mag de bodycam worden aangezet en de beelden worden gebruikt als bewijs bij de aangifte bij de politie. Dit is toegestaan op grond van het "gerechtvaardigde belang" van het college als goed werkgever van de BOA.

Anderzijds stelt PMP dat de bodycams worden ingezet bij de uitoefening van een openbare taak en dat dus de grondslag "gerechtvaardigd belang" niet mag worden gebruikt. Overheden mogen zich niet op deze grondslag beroepen.
De FG's zijn van oordeel dat de laatste stelling elke grond mist. Een overheidsinstantie mag zich in het kader van de uitoefening van haar taken niet beroepen op de grondslag 'gerechtvaardigd belang' ex artikel 6, eerste lid, laatste volzin, AVG, maar dat is hier niet aan de orde. Het gaat immers uitsluitend om privaatrechtelijk handelen als goed werkgever. Daarvoor is wel degelijk een goede grondslag aanwezig.

Juist in de situatie dat het voor gemeenten heel verleidelijk kan zijn om de bodycam ook voor andere doeleinden in te zetten, zoals bij de handhaving van de openbare orde, achten de FG's het heel belangrijk hier een duidelijk signaal af te geven:

Inzet van de bodycam bij de handhaving van de openbare orde is niet toegestaan. De bodycam mag uitsluitend worden ingezet als (preventief) middel om de eigen werknemers te beschermen, uit hoofde van goed werkgeverschap van het college.
Grondslag: gerechtvaardigd belang van het college als goed werkgever.

PMP komt naar aanleiding van bovenbeschreven tegenstrijdigheid tot de volgende afsluitende conclusie (zie pagina 33 van de DPIA):

- Onze inschatting is dat voorafgaande raadpleging door de AP ertoe leidt dat de huidige grondslag (gerechtvaardigd belang) niet zal worden geaccepteerd. Het gevolg is dat het volledig stilleggen van de verwerking dan een kansrijke uitkomst is;
- Een andere optie is het afwachten tot dat er passende wetgeving is. De juridische basis voor de verwerking kan gecreëerd worden door een aanpassing/aanvulling van de Gemeentewet (bijvoorbeeld in een nieuwe art. 151ca Gemeentewet). Hoelang het duurt voordat dit rond is, is moeilijk in te schatten;
- De laatste optie is met de verwerking starten. Hierbij dient u wel alle aanbevelingen uit dit rapport, in de wetenschap dat er over de grondslag valt te discussiëren, wel over te nemen. Bij inmenging van de AP adviseert PMP ook om op te trekken met de andere gemeenten die de bodycams hebben geïmplementeerd.

Het is dus aan een ieder college om hierin een keuze te maken.

PMP heeft een jaar lang aan een DPIA gewerkt die feitelijk tegen gemeenten zegt:
“De grondslag voor de inzet van bodycams is te wankel, dus wij adviseren een voorafgaande raadpleging door de AP. Deze zal waarschijnlijk leiden tot het niet mogen inzetten van de bodycams.”

De FG’s zijn het niet met deze conclusie eens.

Wij adviseren positief over de inzet van de bodycams, mits:

- deze berust op de door ons geadviseerde grondslag
- deze uitsluitend wordt ingezet voor het doel van het bieden van een veilige werkplek voor de BOA, en
- de in de DPIA genoemde passende maatregelen zijn genomen.

Hoogachtend,

Mw. Mr M. Hoff
Functionaris voor de Gegevensbescherming
Gemeente Nissewaard

Dhr. S. van Merode
Functionaris voor de Gegevensbescherming
Gemeenten Brielle, Westvoorne en Hellevoetsluis