Edegem, 10 mei 2021

AANVRAAG VAN DE KORPSCHEF PZ HEKLA AAN DE GEMEENTERAAD VOOR HET VERKRIJGEN VAN EEN PRINCIPIËLE TOESTEMMING TOT HET GEBRUIK VAN MOBIELE CAMERA'S TYPE BODYCAM OP HET GRONDGEBIED DAT ONDER ZIJN BEVOEGDHEID VALT

De toestemmingsaanvraag in onderhavige document werd opgemaakt conform de voorwaarden van de Wet Politieambt en bevat volgende onderdelen:

1. Wettelijke en reglementaire basis voor de aanvraag;
2. Type camera;
3. Perimeter waarbinnen de mobiele camera's worden ingezet;
4. Doelstellingen;
5. Welke zijn de gebruiksmodaliteiten voor het gebruik van deze camera's;
6. Impact- en risicoanalyse op operationeel niveau;
7. Impact- en risicoanalyse op het vlak van de bescherming van de persoonlijke levenssfeer;
8. Aanvraag

1. Wettelijke en reglementaire basis voor de aanvraag

De Wet Politieambt en de uitvoeringsbesluiten ter zake regelen de plaatsing en het gebruik van camera's door de politiediensten.

Artikel 25/3 voorziet dat de politiediensten in het kader van hun opdrachten (mobiele) camera's die in voorkomend geval intelligent zijn, op **zichtbare** wijze kunnen gebruiken op het grondgebied van de politiezone in:

1. de niet-besloten plaatsen en de besloten plaatsen waarvan zij de beheerder zijn;
2. voor het publiek toegankelijke besloten plaatsen, waarvan zij niet de beheerder zijn tijdens de duur van een interventie;
3. niet voor het publiek toegankelijke besloten plaatsen, waarvan zij niet de beheerders zijn tijdens de duur van een interventie.

Artikel 25/4 Wet Politieambt bepaalt dat een politiedienst camera's kan gebruiken overeenkomstig artikel 25/3, op het grondgebied dat onder zijn bevoegdheid valt, na voorafgaande principiële toestemming van de gemeenteraad. De korpschef vraagt de toestemming aan de gemeenteraad. De toestemmingsaanvraag preciseert het type camera, de doeleinden waarvoor de camera's zullen worden geïnstalleerd of gebruikt en de voorziene gebruiksmodaliteiten. De aanvraag houdt rekening met een impact- en risicoanalyse op het vlak van de bescherming van de persoonlijke levenssfeer en op operationeel niveau, met name wat de categorieën van verwerkte persoonsgegevens betreft, de proportionaliteit van de aangewende middelen, de te bereiken operationele doelstellingen en de bewaartermijn van de gegevens die nodig is om deze doelstellingen te bereiken.

2. Type camera

De korpschef PZ HEKLA vraagt aan de gemeenteraad om het type body worn mobiele camera (*spreektaal: bodycam*), op **zichtbare** wijze te kunnen gebruiken.

Het betreft de onderstaande toepassing:

Zichtbaar gebruik van een **mobiele camera** die op de kledij wordt gedragen en in functie van de plaats, tijdstip, de gebeurtenis en/of de opdracht **op de plaats van een interventie** kan worden geactiveerd.

3. Perimeter waarbinnen de mobiele camera's (bodycams) worden ingezet

De politie vraagt om op het hele grondgebied dat onder haar bevoegdheid valt om mobiele camera's van het type bodycam op zichtbare wijze te kunnen gebruiken.

De politie wenst op **zichtbare wijze bodycams** te kunnen inzetten:

1. in de niet-besloten plaatsen;
2. In de besloten plaatsen waarvan politie de beheerder is;
3. in de voor het publiek toegankelijke besloten plaatsen, waarvan politie niet de beheerder is tijdens de duur van een interventie;
4. in de niet voor het publiek toegankelijke besloten plaatsen, waarvan wij niet de beheerders zijn tijdens de duur van een interventie;

Concreet:

Bodycam opnames kunnen gemaakt worden op het openbare domein (vb/ openbare weg, straten en pleinen, park,…). Bodycams kunnen ingezet worden in de gebouwen van de politie. Tijdens interventies kunnen ook bodycam opnames gemaakt worden in voor publiek toegankelijke besloten plaatsen waar diensten aan het publiek kunnen worden verstrekt (vb/ stations, voetbalstadia, horeca instellingen, winkels,…) of in niet voor publiek toegankelijke besloten plaatsen meer bepaald private plaatsen zoals de woning, appartementsgebouw, privédelen van een onderneming,… en dit tijdens de duur van de interventie.

Opgelet: de bodycam kan niet gebruikt worden op het grondgebied van een andere politiezone . Het gebruik van de bodycam voor interventies die gestart zijn op het grondgebied van de eigen zone vormt hierop een uitzondering. In dat verband moet artikel 25/4 WPA worden samen gelezen met artikel 45 WPA. Art. 45 WPA verwijst naar de territoriale bevoegdheid van de leden van het operationeel kader van de politie, van toepassing op het geheel van het grondgebied van het Rijk. Politieoperaties en politieoptredens laten zich nu eenmaal niet beperken door gemeentegrenzen of grenzen van politiezones. Concreet wil dit zeggen dat de politieambtenaar van de ene politiezone zijn

operationele opdracht moet kunnen verderzetten in een andere politiezone. De interventie waarbij een bodycam wordt gebruikt en die gestart is op het grondgebied van de PZ HEKLA kan, met gebruik van bodycam, rechtsgeldig worden verdergezet op het grondgebied van een andere zone.

4. Doelstellingen

Algemeen

De verwerking van de beelden omvat de doelstellingen conform art. 25/3 §2 Wet Politieambt. [1]

De mobiele camera's en de opnames worden gebruikt in uitvoering van de opdrachten van de politie, zoals bepaald in de Wet Politieambt. Het betreffen zowel opdrachten van bestuurlijke als gerechtelijke politie. Het gebruik van een bodycam dient steeds operationeel gemotiveerd te zijn. Het zichtbaar gebruik van de bodycam is onderworpen aan de wettelijke verplichting om mondeling een waarschuwing te geven. Dit impliceert dat de burger geïnformeerd is over de effectieve inzet van de bodycam. Enkele voorbeelden die de wetgever zelf aanhaalt in de memorie van toelichting m.b.t. het gebruik van mobiele camera's betreffen:

- handhaving en het herstel van de openbare orde in het kader van het genegotieerd beheer van de publieke ruimte;
- beheer van de mensenmassa's (crowdmanagement);
- voorbereiding en het uitvoeren van de politieoperaties, dit met het oog op het garanderen van de veiligheid van deze personen. Ongeacht het feit of het om operaties van bestuurlijke of gerechtelijke politie gaat, is het gebruik van camera's om de politieoperatie voor te bereiden, de veiligheid van het politiepersoneel en van derden te garanderen tijdens deze operatie of de operatie tactisch voor te bereiden, een handeling van bestuurlijke politie.

In concreto

- voorkomen en registreren van verstoringen van de openbare orde;
- voorkomen, vaststellen en registeren van strafbare feiten;
- openbare ordehandhaving (vb. voetbal, betogingen, evenementen, manifestaties, rampen, calamiteiten);
- beelden en -opnames ter operationele ondersteuning ('*situational awareness*' en '*common operational picture'*);
- gebruik opgenomen beelden als ondersteunend bewijsmateriaal;

[1] "het zichtbare gebruik van camera's voor het inwinnen van informatie van bestuurlijke politie bedoeld in artikel 44/5, § 1, is uitsluitend toegelaten in de gevallen bedoeld in artikel 44/5, § 1, eerste lid, 2° tot 6°. Wat artikel 44/5, § 1, eerste lid, 5°, betreft, kan dat gebruik bovendien alleen worden toegelaten ten aanzien van de categorieën van personen bedoeld in artikelen 18, 19 en 20."

- als hulpmiddel bij het afleggen van verantwoording met betrekking tot de aangeboden dienstverlening en/of een antwoord te formuleren in geval van klachten.
- identificeren van een dader, een verstoorder van de openbare orde, een getuige of een slachtoffer;
- interne opleidingsdoeleinden (didactische en pedagogische doeleinden zoals training en coaching van collega's).

5. De gebruiksmodaliteiten van deze camera's

- draagwijze: bevestigd op de kledij van de politieambtenaar, die hetzij herkenbaar is aan het politie-uniform, hetzij zich identificeert via de interventiearmband en/of de dienstidentiteitskaart;
- opname video en audio na een voorafgaande mondelinge waarschuwing. Het beeld en de audio worden 30 seconden voorafgaand aan het indrukken van de knop, bijkomend opgenomen;
- het feit dat de camera's het geluid kunnen opnemen, machtigt het lid van de politiediensten die deze camera's gebruikt niet om privégesprekken op te nemen waaraan hij niet deelneemt;
- de camera's mogen noch beelden opleveren die de intimiteit van een persoon schenden, noch gericht zijn op het inwinnen van informatie over de raciale of etnische oorsprong van een persoon, zijn religieuze of levensbeschouwelijke overtuigingen, zijn politieke opvattingen, zijn vakbondslidmaatschap, zijn gezondheidstoestand, zijn seksleven of zijn seksuele geaardheid.
- strikt beleid en uniforme procedures met betrekking tot het gebruik van de camera's en de opname. Standaardprocedure is dat de camera permanent in stand-by modus staat vanaf aanvang dienst en wordt geactiveerd in geval van een incident/interventie;
- geen live videoverbinding naar de lokale dispatch of een politiecomputer. De beelden worden automatisch opgeslagen op een beveiligde server van zodra het toestel in het dockingsstation wordt teruggeplaatst;
- beelden en audio worden opgenomen op een beveiligde server van de PZ HEKLA. De beelden zijn beveiligd;
- elke toegang tot de beveiligde server wordt bijgehouden zodat kan nagegaan worden wie wanneer toegang tot de beelden had (logging);
- gelet op de restricties van de camerawetgeving en de privacygevoeligheid bij het bekijken van camerabeelden, is de server enkel toegankelijk voor bevoegde personen. Deze toegang is geconfigureerd via een interface die toelaat de toegang tot data op het beheerssysteem van de politie te monitoren.

6. Impact- en risicoanalyse op operationeel niveau

Categorieën van verwerkte persoonsgegevens

De categorieën van persoonsgegevens die worden verwerkt met bodycams zijn enerzijds camerabeelden en anderzijds audio. De bodycam staat tijdens interventies op stand-by. Er is geen permanente opslag van beelden en audio. Om een effectieve opname te starten moet de medewerker steeds een knop op het toestel indrukken. PZ HEKLA werkt met een buffering van 30 seconden. Dit betekent dat ook het beeld en de audio 30 seconden voorafgaand aan het indrukken van de knop, bijkomend opgenomen worden. Hierdoor zal de noodzakelijke context en de voorafgaande waarschuwing steeds mee opgenomen zijn. De opname stopt pas zodra opnieuw een knop op het toestel wordt ingedrukt.

De beelden en de audio bevatten persoonsgegevens die het mogelijk maken om personen te identificeren. De betrokken personen zijn diegenen die op de beelden verschijnen. Ook de loggegevens van de verwerkingen (wie neemt op en wie raadpleegt de beelden, wie schrijft weg) worden bijgehouden.

De opnames worden bij het terugplaatsen van de bodycam in het docking station automatisch gedownload en weggeschreven naar een beveiligde server. De lokale opnames op het toestel worden automatisch gewist.

De camera's zullen noch beelden opleveren die de intimiteit van een persoon schenden, noch beelden opleveren die gericht zijn op het inwinnen van informatie over de filosofische, religieuze, politieke, syndicale gezindheid, etnische of sociale origine, het seksuele leven of de gezondheidstoestand van de gefilmde personen.

De opname van audio doet geen afbreuk aan de bepalingen van het Strafwetboek met betrekking tot het opnemen van privégesprekken (artikelen 259bis en 314bis SW). Het feit dat de camera's geluidsopnames mogelijk maken, betekent niet dat de leden van de politiediensten die ervan gebruikmaken privégesprekken mogen opnemen waaraan ze niet deelnemen.

Het gebruik van bodycams met geluidsopname is enkel toegelaten als de leden aan het opgenomen gesprek deelnemen. De geluidsopname kan dan aantonen dat de leden van de politiediensten de burgers op voorhand over het gebruik van camera's hebben ingelicht.

Operationele doelstellingen

Het dragen van een bodycam beoogt volgende doeleinden:

- Het preventief de-escaleren van een risico-interventie door helder te communiceren dat de hele gebeurtenis wordt gefilmd (internationaal onderzoek bevestigt deze stelling[2]).
- Het vastleggen van gebeurtenissen om te kunnen dienen als bewijsmateriaal (waarheidsvinding, bewijs, reconstructie na incidenten) – zowel in een gerechtelijk als

1. [2] S. FLIGHT, Evaluatie pilot bodycams Eenheid Amsterdam 2017-2018, *Politie & Wetenschap* 2019, 187-190.

administratief onderzoek – en dit ondersteunend aan de vaststellingen van de politie-ambtenaar.
- Gebruik van geanonimiseerde beelden voor opleidings- en trainingsdoeleinden bij politiemedewerkers.

Proportionaliteit van de aangewende middelen

Het gebruik van de mobiele camera's zal steeds kaderen binnen het uitvoeren van taken van bestuurlijke en gerechtelijke politie, en in het bijzonder op het vlak van 'toezicht' en 'opsporing'. Het spreekt voor zich dat het gebruik van mobiele camera's als intrusief kan ervaren worden. Het is daarom van essentieel belang te waken over het evenwicht tussen de behoeften van de politiediensten in het raam van hun opdrachten en het recht op privacy van de betrokkenen. Cruciaal daarbij is enerzijds het ontwikkelen van strikte en uniforme procedures met betrekking tot het gebruik en de inzet van de camera's en anderzijds de training van politiemedewerkers in de manier waarop ze de camera gebruiken.

Een officier bestuurlijke politie is organisatorisch belast met de naleving van de regelgeving en een goede implementatie van de technologie.

De bodycam wordt prioritair meegegeven aan medewerkers voor opdrachten met een verhoogd risico op incidenten of heterdaadvaststellingen (niet exhaustief: interventiemedewerkers, bijstand deurwaarders, verkeerscontroles, huiszoekingen, …).

De politie is gebonden aan een strikt regelgevend kader. De verschillende verwerkingen met bodycams (opslag, het beheer, loggegevens bijhouden) kaderen allemaal binnen een wettelijke opdracht. De rechtmatigheid van de verwerking situeert zich binnen de opdrachten van bestuurlijke en gerechtelijke politie. De wettelijke bepalingen die van toepassing zijn op de politiediensten inzake de verwerking van persoonsgegevens bevatten waarborgen tegen misbruiken.

In concreto is dit:

- maken van een impact- en risico analyse op het vlak van de bescherming van de persoonlijke levenssfeer;
- camera 's zullen gebruikt worden voor duidelijk omschreven en gerechtvaardigde doeleinden. De WPA voorziet dat politiediensten camera's kunnen inzetten in het kader van opdrachten van bestuurlijke EN gerechtelijke politie (artikel 14 en 15 WPA);
- opname video en audio pas na een voorafgaande mondelinge waarschuwing;
- servers bevinden zich in beveiligde politielokalen. Deze lokalen beantwoorden aan de vigerende beveiligingsstandaarden;
- geregistreerde gegevens zijn niet zonder grondige reden raadpleegbaar. Er moet een concrete politionele behoefte bestaan in het raam van de bestuurlijke of de gerechtelijke politie;
- geregistreerde gegevens zijn enkel raadpleegbaar door gemandateerden. Het is de korpschef die beslist of de medewerker toegang krijgt tot de applicatie, en dit op basis van de uitgeoefende functie en het noodzakelijke profiel;

- elke raadpleging + de reden van raadpleging wordt gelogd;
- de gegevens zijn enkel raadpleegbaar conform de toegangsregels van de WPA
- derden kunnen hun recht op toegang uitoefenen via de vigerende regelgeving
- verschillende vormen van intern en extern toezicht: intern is dit de functionaris voor de gegevensbescherming (DPO) en intern toezicht. Volgende overheden kunnen een controlebezoek uitvoeren: Controleorgaan van het politioneel informatiebeheer (COC), Comité P, de Algemene Inspectie van de Federale Politie en van de Lokale Politie.

Bewaartermijn en toegang tot de beelden

De beelden worden automatisch opgenomen op een beveiligde server van de politiezone. Lokale opslag op een gegevensdrager in het toestel wordt toegepast tijdens het dragen, maar wordt automatisch verwijderd na 'docking' van de camera. In voorkomend geval worden beelden toegevoegd als bewijsmateriaal. De politiediensten mogen de verzamelde gegevens niet meer dan twaalf maanden bewaren na de registratie. Enkel de relevante camerabeelden worden 12 maanden bewaard. Indien bodycam opnames niet werden gemarkeerd als 'te bewaren' worden deze na 90 dagen verwijderd

De toegang tot de gegevens door politiemensen is beperkt tot één maand na de registratie, behalve voor een raadpleging in het kader van een opdracht van gerechtelijke politie of voor didactische doeleinden.

Binnen de 1ste maand na registratie: bevoegdheid korpschef van de politiezone

- De gefilmde persoon richt zich binnen de 1ste maand na registratie met voldoende gedetailleerde aanwijzingen inzake lokalisatie van de beelden tot de korpschef als verantwoordelijke van de verwerking. Deze laatste voorziet in voorkomend geval een directe toegang, waarbij het COC als beroepsinstantie kan optreden t.a.v. zijn beslissing. De toegang tot de beelden is afhankelijk van de beoogde finaliteit (een concreet operationeel belang), de traceerbaarheid (audit trail) en de uitoefening van een welbepaalde opdracht (motivatie).
- Elke medewerker van de politiezone heeft, buiten zijn wettelijke opdrachten van gerechtelijke en bestuurlijke politie, ook het recht om kennis te nemen van het beeldmateriaal en elk ander gegeven dat verzameld wordt door de bodycams en hem/haar aanbelangt. (zelf opgenomen of ook door collega?) De betrokken medewerker kan daarbij de verwijdering verzoeken van alle hem/haar betreffende persoonsgegevens die onvolledig, of niet ter zake dienend zijn, of waarvan de registratie, de mededeling of de bewaring verboden zijn, of die na verloop van de toegestane duur zijn bewaard.
- Klachten worden behandeld overeenkomstig de richtlijnen van de bevoegde tuchtoverheid.

In voorkomend geval kan de medewerker schriftelijk op de hoogte worden gebracht opdat hij/zij ook kennis kan nemen van de zo verkregen informatie.

Na de 1ste maand na registratie: bevoegdheid procureur des Konings

- Onverminderd zijn verantwoordelijkheid in lopende opsporingsonderzoeken en de richtlijnen inzake inbeslaggenomen overtuigingsstukken, richten de politieambtenaar met individuele toegangsrechten zich na de 1ste maand na registratie tot de procureur des Konings. Deze laatste beslist op schriftelijke en gemotiveerde beslissing over de toegang.

Beelden voor didactische doeleinden worden geanonimiseerd. Elke lees- en schrijfbeweging op de beveiligde server wordt gelogd.

De politiezone zal een register van gebruik bijhouden.

De camera's worden gebruikt conform de voorwaarden van de Wet Politieambt.

7. Impact- en risicoanalyse op het vlak van de bescherming van de persoonlijke levenssfeer (DPIA)

Betrokken actoren

- Naam verwerkingsverantwoordelijke: HCP Ivo VEREYCKEN, Korpschef
- Contactpunt voor het recht van toegang op de beelden: contact@politiehekla.be
- Contactpunt voor informatievragen: contact@politiehekla.be Tel: 03.444.00.00
- De flowchart en de criteriamatrix werd geanalyseerd door:
  - De Data Protection Officer van PZ HEKLA
  - Korpsleiding PZ HEKLA.

Beschrijving van de gegevensstroom

De categorieën van persoonsgegevens die worden verwerkt zijn:

Algemeen:

- camerabeelden en audio-opnames (mobiele body worn camera):
  - beelden en geluiden;
  - de metagegevens gelinkt aan deze beelden/geluiden:
    - tijdsbepaling (dag en de uurvorken van deze opnames
    - identificatie van het lid van het operationeel kader die drager is van de camera tijdens de opname van gegevens (voorafgaandelijk registratie van het gebruik door het personeelslid);
    - de plaats waar de gegevens werden verzameld.
- logginggegevens van de verwerkingen (mobiele body worn camera):;
- pre-recording functionaliteit die data buffert (30 seconden). Wanneer een politieambtenaar een opname effectief start, wordt de betrokken buffer van 30 seconden die voorafgaat aan z'n opname ook bewaard. Zo zal men met de geluidsopname kunnen aantonen dat er mondeling werd aangekondigd dat er wordt gefilmd. De bodycam staat hiervoor steeds in standby modus.

De volgende categorieën met gegevens met een persoonlijk karakter kunnen het voorwerp uitmaken van de opnames:

- algemene persoonlijke gegevens die toelaten om rechtstreeks of onrechtstreeks iemand te identificeren. In het kader van het vaststellen van inbreuken en/of het niet respecteren van bepalingen aangaande politiereglementen, kan een identiteit gekoppeld worden aan een opname met (naam, de voornaam en de geboortedatum van de betrokken personen op de beelden). Dit kunnen politiemedewerkers zijn, daders van inbreuken, de slachtoffers, de getuigen of relevante derden;
- gevoelige gegevens kunnen voorkomen op de beelden (bv/ zichtbare karakteristieken van de gezondheidstoestand). Dit is geen finaliteit. De verwerking van gevoelige persoonsgegevens mag alleen plaatsvinden in aanvulling op de verwerking van andere politiegegevens en alleen voor zover dit voor het doel van de verwerking onvermijdelijk en strikt noodzakelijk is.

Functioneel:

- Elke operationele medewerker kan een bodycam meenemen op dienst door zijn/haar individuele badge op de RFID-reader (radio frequency identification) te plaatsen. De interventieploegen nemen per ploeg verplicht één bodycam mee.
- De bodycam dient steeds in stand-by modus te staan, met een pre-recording functie actief;
- Uiterlijk bij einde dienst wordt de bodycam opnieuw ingeleverd op de door de RFID-reader toegewezen locatie in het docking station.
  Via het docking station worden de bodycam opnames afgeladen naar het bodycam systeem. Eens afgeladen zijn de bodycam opnames beschikbaar in het systeem, en raadpleegbaar afhankelijk van gebruikersrechten.
  Op de bodycam vindt een simultane verwijdering van de gegevens plaats

Persoonsgegevens zijn toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt:

<u>Finaliteit van de verwerking (ook cf. supra)</u>

De camera's worden zichtbaar gebruikt op het grondgebied van de PZ HEKLA in uitvoering van art 25/3 wet Politieambt en ter ondersteuning van de opdrachten van de politie, zoals bepaald in de Wet Politieambt. Het betreffen zowel opdrachten van bestuurlijke politie (artikel 14 Wet Politieambt) als opdrachten van gerechtelijke politie (artikel 15 Wet Politieambt). Met de bodycam wordt aan de operationele terreinmedewerkers een tool aangeboden die hen ondersteunt in hun reguliere werking. De verwerking van de data moet leiden tot een betere besluitvorming op het terrein, het handhaven van de openbare orde en veiligheid, het verbeteren van heterdaadkracht en opsporing en het bijdragen aan bewijsvoering.

Wie bekijkt de beelden? (ontvangers)

Het camerasysteem functioneert onder de operationele verantwoordelijkheid van de politieambtenaar bedoeld in de artikelen 7 tot 7/3 WPA die waakt over de naleving van de proportionaliteits- en subsidiariteitsbeginselen. De bediening en het gebruik van de apparatuur gebeurt door bevoegd politiepersoneel. De politieambtenaren zullen voorafgaandelijk een opleiding krijgen en worden aangeduid door de korpschef.

De toegang tot de opgenomen beelden is strikt geregeld en uitvoerig beschreven in artikel 25/7 van de WPA.

Consultatie is toegelaten op voorwaarde dat het operationeel gemotiveerd is en dat het noodzakelijk is voor de uitvoering van een welbepaalde opdracht.

De toegangstermijn tot de opgenomen beelden is afhankelijk van de bestuurlijke of gerechtelijke finaliteit van de opdracht die de toegang vereist:

- In het kader van bestuurlijke politie zijn beelden opvraagbaar tot maximum één maand na opname;
- In het kader van gerechtelijke politie zijn beelden opvraagbaar tot maximum 12 maanden na opname. Zodra er echter toegang nodig is tot de beelden na de eerste maand, is deze toegang steeds onderworpen aan een schriftelijke en gemotiveerde beslissing van de procureur des Konings (kantschrift).

Worden de beelden opgenomen?

Ja.

Op welke wijze worden de beelden opgeslagen?

Het beeldmateriaal wordt op een beveiligde server opgeslagen. De beelden zijn enkel toegankelijk voor bevoegde politieambtenaren en de systeemverantwoordelijke(n). Deze toegang hebben ze via een systeem dat toelaat de data te monitoren. Bevoegde personen zullen een login en paswoord moeten gebruiken. Alle handelingen die zij stellen worden gelogd. De korpschef duidt een officier aan, verantwoordelijk voor het toezicht en het gebruik van de gegevens die door de camera's worden gegenereerd. Deze aangeduide officier waakt erover dat onbevoegde personen geen toegang hebben tot de camerabeelden en -data.

Hoelang worden de opgeslagen beelden bewaard?

De opgenomen beelden worden niet langer bijgehouden dan noodzakelijk. De duur van de bewaring van de gegevens is wettelijk bepaald. De gegevens mogen zoals bepaald in artikel 25/6 van de WPA maximum 12 maanden worden bewaard. Na deze termijn worden de beelden automatisch gewist.

Alleen het beeldmateriaal dienstig voor een opsporingsonderzoek van de politie of dienstig als bewijsmateriaal tijdens een rechtszitting kan langer worden bijgehouden. De gegevens worden in dat geval bewaard totdat het opsporingsonderzoek en de gerechtelijke procedures zijn afgerond.

Hoe wordt de toegang tot de beelden beveiligd?

PZ HEKLA neemt alle nodige en passende voorzorgsmaatregelen ten einde de toegang tot de beelden te beveiligen tegen toegang door onbevoegden. De personen die toegang hebben tot de beelden hebben een discretieplicht omtrent de persoonsgegevens die de beelden opleveren. Dit impliceert dat:

- de beheerders en de personen die onder hun gezag handelen worden geresponsabiliseerd in het kader van de bescherming van de privacy;
- principieel vreemden aan de dienst geen toegang hebben tot de meldkamer en serverlokalen;
- enkel politie- en onderhoudspersoneel toegang hebben. De toegang van politiepersoneel, vreemd aan de eigen dienst, wordt tot een minimum beperkt in functie van het operationeel nut of de deelname aan vergaderingen in de vergaderzaal. Onder onderhoudspersoneel wordt verstaan: personeel belast met het onderhoud;
- de toegangsdeur tot de lokalen afgeschermd wordt met een elektronisch slot. De toegangsdeur moet zich permanent automatisch vergrendelen. Iedere andere bezoeker, die niet behoort tot het politiekorps van HEKLA, moet zich vooraf laten verifiëren of registreren;
- de uitzonderlijke toegang van derden tot de lokalen enkel is toegestaan onder het toezicht van een vast personeelslid;
- een officier organisatorisch is belast met de naleving van deze regelgeving.

Worden de beelden in real-time bekeken?

Neen.

Register

De PZ HEKLA houdt een digitaal register bij, zoals bepaald in art. 25/8 Wet Politieambt, opdat het gebruik van de camera's worden gelogd.

Kennisgevingen

De PZ HEKLA neemt volgende maatregelen om het gebruik van de camera's aan de informatieplicht en het nodige toezicht te onderwerpen:

- kennisgeving van de principiële toestemming door de gemeenteraad via de website van de gemeenten van de politiezone;
- kennisgeving van de principiële toestemming door de gemeenteraad aan de procureur des Konings;
- kennisgeving aan het Controleorgaan op de politionele informatie (COC) via REGPOL.

Informatieplicht

In overeenstemming met de wet op het politieambt is het gebruik van mobiele camera's zichtbaar door een mondelinge verwittiging komende van de leden van het operationeel kader van de politiediensten herkenbaar in die hoedanigheid. Om beschouwd te kunnen worden als herkenbaar, moet het lid van het operationeel kader drager zijn van zijn uniform of tussenkomen in burgerkledij EN drager zijn van zijn interventiearmband of duidelijk zijn legitimatiekaart tonen. De politieambtenaar zal verplicht en voorafgaandelijk betrokkenen informeren van het gebruik van de camera, onmiddellijk na het starten van de registratie. Om een bewaring te hebben van deze verwittiging wordt hierbij rekening gehouden met een buffer van 30 seconden, d.w.z. dat er 30 seconden voorafgaand aan het indrukken van de opnameknop reeds wordt opgenomen.

Er zal specifieke communicatie gebeuren naar het personeel:

- via BOC
- door de verspreiding van een interne richtlijnen
- door verplichte training.

Rechten van de betrokkene

Deze rechten zullen kunnen uitgeoefend worden conform de nationale regelgeving ter zake (Wet 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens).

Inzage kan via het functioneel e-mailadres van PZ HEKLA. Het verzoek moet voldoende gedetailleerd zijn om de data precies te kunnen terugvinden. Men moet ook een reden opgeven voor het verzoek. De functionaris voor gegevensbescherming weegt vervolgens af of het verzoek tot toegang kan ingewilligd worden. Hij houdt hierbij rekening met de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens. De uitoefening van dit recht mag geen afbreuk doen aan de rechten en vrijheden van anderen. Toegang kan worden verleend maar ook geweigerd om de privacy van derden te beschermen of omwille van de openbare veiligheid. We geven nooit een kopie van beelden mee. Betrokkenen kunnen beelden wel komen inzien. Voor we aan het verzoek voldoen, zullen wij vragen om een identiteitsbewijs voor te leggen. uitgeoefend worden conform de nationale regelgeving ter zake.

Risicobeoordeling

Geplande of bestaande richtlijnen cf Korpsnota PZ5349/OPS/2021-004

- Elke operationele dienst die bodycams krijgt toegewezen, staat in voor het correct beheer van de bodycams, het docking station en de meegeleverde hard- en software. De operationele reservestock wordt beheerd door de dienst OCS – in geval van nood bereikbaar voor de OGP wacht.
- Het strategisch beleid rond de mobiele camera's als onderdeel van een breder perspectief inzake cameramiddelen wordt beheerd door de directeur operaties als dossierbeheerder;
- De eindverantwoordelijkheid van de verwerking ligt bij de korpschef;
- Het gebruik van bodycams uit de operationele reserve bij geplande acties en evenementen dient via de dienst OCS te worden aangevraagd indien de eigen capaciteit niet volstaat. Dit om te vermijden dat de bodycams niet beschikbaar zouden zijn bij operationele noodwendigheden;
- De directie bedrijfsvoering neemt kennis van eventuele defecten aan de hardware via de helpdeskmodule (intranet), opdat er snel kan worden teruggekoppeld met de leverancier;
- De dienst ICT is beschikbaar voor de coördinatie m.b.t. de toegangsrechten van de gebruikers (incl. de integratie van RFID), voor technische ondersteuning of opzoekingen in de audit trail;
- Elke bodycam wordt aan het einde van de dienst in het docking station geplaatst waarna de gegevens automatisch worden overgezet naar een beveiligde server in de politiezone zonder externe toegang;
- Privacy by design: de PZ HEKLA ambieert een product aan te kopen waarbij de bescherming van de privacy maximaal wordt gewaarborgd door de constructie van het toestel. Vereisten zijn onder meer:
    - Bij het terugplaatsen worden de beelden automatisch en gecrypteerd opgehaald van de bodycam en op de server van de politie bewaard. Daarna kunnen de beelden niet meer op de bodycam zelf gerecupereerd worden. Ter preventie van datalekken moet (bijhorende) software worden bijgeleverd die voorziet in multi factor authentification, verschillende autorisatieniveaus in een beveiligd politiecommissariaat, de optie om verboden beelden te blurren, …
    - Van alle bodycam opnames moet automatisch een digitaal register worden bijgehouden in de politiezone door middel van een audit trail: wie de opnames gemaakt heeft, wanneer, op welke locatie, …
    - Aan de verplichtingen inzake derde verwerkersovereenkomst en het voeden van het register verwerking persoonsgegevens geïntegreerde politie (RegPol) moet worden voldaan.

- Het recht om vergeten te worden:
    - De informatie en persoonsgegevens die verzameld worden door middel van camera's kunnen wettelijk worden geregistreerd en bewaard voor een duur van niet meer dan twaalf maanden, te rekenen vanaf de dag van de opname. Indien de bodycam opnames terug worden bekeken om vaststellingen te vervolledigen dan wordt dit steeds vermeld in de voorziene ISLP-module, een PV en/of een bestuurlijke akte.
    - Relevante camerabeelden dienen in voorkomend geval in het systeem gemarkeerd te worden als 'te bewaren' door de dossierbeheerder. Indien bodycam opnames niet werden gemarkeerd als 'te bewaren' worden deze in de politiezone HEKLA standaard na 3 maanden (90 dagen) verwijderd omwille van de opslagcapaciteit op de lokale server. Het is in geen enkel geval toegelaten (of zelfs mogelijk) om zelf bodycam opnames te verwijderen en politieambtenaren kunnen op eigen initiatief slechts 1 maand terug in de tijd (zie verder).
- Volgende autorisatieniveaus worden binnen de zone gehanteerd:

ROL	AUTORISATIE	BELEIDSKEUZE
System Administrator	Recorder en Manager administrators	Diensthoofd ICT
Device operators	Kan toegewezen worden aan recorders	Alle Ops. medewerkers
Manager	Eigen beelden, die van supervisor en anderen bekijken	KC - DirOps - DPO - COC
Supervisor	Eigen beelden en beelden toegewezen medewerkers bekijken	Teamchefs
Gebruiker	Eigen beelden bekijken en beelden met hen gedeeld	Alle ops. medewerkers

- De gegevens kunnen na anonimisering ook worden gebruik t.v.v. vorming binnen de politiediensten
- Het recht op toegang
    - Voor het exploiteren van de beelden van de bodycams is het wettelijk kader op verwerking van politiegegevens van toepassing. We onderscheiden enerzijds de individuele toegangsrechten van de politieambtenaar tijdens zijn/haar wettelijke opdrachten van bestuurlijke en/of gerechtelijke politie (vb. kwaliteitszorg, rechtstreeks leidinggevende, de dossierbeheerder, …) en anderzijds het principieel recht van iedere gefilmde persoon. De wet maakt een verschil tussen de 1ste maand na registratie en daarna:

- Binnen de 1ste maand na registratie: bevoegdheid korpschef van de politiezone.
    - De gefilmde persoon richt zich binnen de 1ste maand na registratie met voldoende gedetailleerde aanwijzingen inzake lokalisatie van de beelden tot de korpschef als verantwoordelijke van de verwerking. Deze laatste voorziet in voorkomend geval een directe toegang, waarbij het COC als beroepsinstantie kan optreden t.a.v. zijn beslissing. De toegang tot de beelden is afhankelijk van de beoogde finaliteit (een concreet operationeel belang), de traceerbaarheid (audit trail) en de uitoefening van een welbepaalde opdracht (motivatie).
    - Elke medewerker van de politiezone heeft, buiten zijn wettelijke opdrachten van gerechtelijke en bestuurlijke politie, ook het recht om kennis te nemen van het beeldmateriaal en elk ander gegeven dat verzameld wordt door de bodycams en hem/haar aanbelangt. (zelf opgenomen of ook door collega?) De betrokken medewerker kan daarbij de verwijdering verzoeken van alle hem/haar betreffende persoonsgegevens die onvolledig, of niet ter zake dienend zijn, of waarvan de registratie, de mededeling of de bewaring verboden zijn, of die na verloop van de toegestane duur zijn bewaard.
    - Klachten worden behandeld overeenkomstig de richtlijnen van de bevoegde tuchtoverheid. In voorkomend geval kan de medewerker schriftelijk op de hoogte worden gebracht opdat hij/zij ook kennis kan nemen van de zo verkregen informatie.
- Na de 1ste maand na registratie: bevoegdheid procureur des Konings
    - Onverminderd zijn verantwoordelijkheid in lopende opsporingsonderzoeken en de richtlijnen inzake inbeslaggenomen overtuigingsstukken, richten de politieambtenaar met individuele toegangsrechten zich na de 1ste maand na registratie tot de procureur des Konings. Deze laatste beslist op schriftelijke en gemotiveerde beslissing over de toegang.
- Toegang tot de geregistreerde gegevens op de beveiligde server is gelimiteerd tot de personen gemachtigd door de korpsnota;
- Logging van de toegang tot de gegevens is voorzien
- de gegevens worden op een beveiligde server bewaard. De server bevindt zich on site (binnen het gebouw van de politie).
- de fysieke toegang tot de infrastructuur is beveiligd
- het politiegebouw is uitgerust met branddetectie

- Overeenstemmend met de wettelijke bepalingen en reglementen, heeft PZ HEKLA een DPO aangeduid
- Er bestaan verschillende vormen van intern en extern toezicht die controles kunnen uitvoeren om na te kijken of de richtlijnen worden gerespecteerd. Intern is dit de functionaris voor de gegevensbescherming (DPO) en intern toezicht. Volgende overheden kunnen een controlebezoek uitvoeren: Controleorgaan van het

politioneel informatiebeheer (COC), Comité P, de Algemene Inspectie van de Federale Politie en van de Lokale Politie.

- De implementatie van de bodycam maakt het voorwerp uit van een Korpsnota en een interne richtlijn met betrekking tot de finaliteiten, het wettelijk gebruik (enkel op zichtbare wijze en na een voorafgaandelijke verwittiging en de toegangsrechten, de opslag en de duur van de bewaring van de gegeven. Er is een voorafgaandelijke opleiding van de gebruikers.

RISICO: Onrechtmatige toegang tot de gegevens

- **Gevolgen voor de betrokken personen indien dit risico zich voordoet:** onrechtmatige raadpleging door onbevoegde personen, onrechtmatige verspreiding van persoonsgegevens, data wordt publiek gemaakt, verspreiding via sociale media,…, imagoschade voor het korps, schade aan het geheim van het strafrechtelijk onderzoek, misbruik van gegevens, betrokken persoon stelt zich burgerlijke partij tegenover de politiediensten.
- **Belangrijkste bedreigingen die dit risico zouden kunnen doen ontstaan:** Binnendringen in politiegebouwen, hacking IT-systemen, verlies bodycam, schending beroepsgeheim, misbruik van de beoogde verwerkingen in het systeem
- **Welke bronnen van risico kunnen hierbij aan de grondslag liggen?** Onvoldoende veiligheid toegang tot politiegebouw, onveiligheid van de toegang tot de server, nalatige of malafide medewerker, hacker.
- **Welke maatregelen dragen bij om dit risico te remediëren?** Server in een beveiligd politiecommissariaat, geen leesbare data op bodycam zelf, cryptografie, multi factor authentification, verschillende autorisatieniveaus, logging, netwerkbeveiliging, registratie van personen die toegang hebben tot gebouw, controle van de logische toegangen, interne richtlijnen, interne en externe controles, opleidingen, sensibiliseren.
- **Hoe wordt de ernst van het risico ingeschat, in functie van de mogelijke impact en de effecten?** Groot immers, imagoschade, schending geheim van het strafrechtelijk onderzoek, schending van recht op afbeelding van betrokkene, misbruik van gegevens.
- **Hoe schat u de waarschijnlijkheid van het risico, vooral met betrekking tot bedreigingen, risicobronnen en geplande controles?** Klein tot verwaarloosbaar. Er zijn voldoende maatregelen en controles bepaald om het risico zoveel mogelijk te beperken: versterking van de toegangscontrole, beveiligd gebouw (badge), opleiding en sensibilisering mbt maatregelen op vlak van security/safety, toegang tot de lokalen met de servers gelimiteerd, netwerk beveiliging tegen ongewenste externe indringing, laden van de beelden is geïnstalleerd in een dockstation, logging wie, wat, wanneer, geen lezen van de beelden mogelijk vanaf de bodycam, technische en organisatorische maatregelen om politiegegevens afkomstig van bodycams te beveiligen tegen verlies of vormen van onrechtmatige verwerking door op de opnames data encryptie toe te passen en medewerkersgegevens aan de opnames te koppelen.

RISICO: het ongewenst wijzigen van gegevens

- **Wat zouden de voornaamste gevolgen zijn voor de betrokken personen indien dit risico zich voordoet?** Imagoschade, manipulatie van de bewijslast,
- **Belangrijkste bedreigingen die dit risico zouden kunnen doen ontstaan:** misbruik of foutief gebruik door medewerkers, hacking.
- **Welke bronnen van risico kunnen hierbij aan de grondslag liggen?** Nalatige of malafide medewerker, incident op de infrastructuur, hacker, malafide toegang door leverancier van het systeem.
- **Welke maatregelen dragen bij om dit risico te remediëren?** Netwerk veiligheid, fysieke toegangscontrole, traceerbaarheid (logging), operationele beveiliging, overeenkomsten met derden, interne en externe controles, interne richtlijn, opleiding, een geheimhoudingsverplichting en verwerkersovereenkomst ondertekend door de firma Securitas.
- **Hoe wordt de ernst van het risico ingeschat, in functie van de mogelijke impact en de effecten?** Mogelijke impact op de uitoefening van de strafvordering en de bewijslast maar het feit dat de beelden van een incident niet verplicht wettelijk zijn en enkel een bijkomende aanwijzing zijn, verkleint de ernst van het risico.
- **Hoe schat u de waarschijnlijkheid van het risico, vooral met betrekking tot bedreigingen, risicobronnen en geplande controles?** Klein tot verwaarloosbaar, voldoende beveiligingsmaatregelen (toekennen rechten, logisch toegangsbeleid), pogingen tot wijziging van de beelden laten sporen na.

RISICO: het verdwijnen van gegevens

- **Wat zouden de voornaamste gevolgen zijn voor de betrokken personen indien dit risico zich voordoet?** Onvolledigheid en onbetrouwbaarheid van het beeldmateriaal, effect op de bewijslast door onmogelijkheid om de gegevens te gebruiken of de wettelijkheid te betwisten en/of te bevestigen.
- **Belangrijkste bedreigingen die dit risico zouden kunnen doen ontstaan:** misbruik of foutief gebruik door medewerkers, technologisch falen, hacking, accidenteel wissen van de gestockeerde gegevens
- **Welke bronnen van risico kunnen hierbij aan de grondslag liggen?** Incident op de infrastructuur (bv brand), nalatige of malafide medewerker, hacker
- **Welke maatregelen dragen bij om dit risico te remediëren?** Netwerk veiligheid, fysieke toegangscontrole, traceerbaarheid (logging), operationele beveiliging, , interne en externe controles, interne richtlijn, opleiding.
- **Hoe wordt de ernst van het risico ingeschat, in functie van de mogelijke impact en de effecten?** Afhankelijk van de positie van de betrokkene kan het een positief of negatief effect hebben. Mogelijke impact op de uitoefening van de strafvordering en de bewijslast, maar het feit dat de beelden van een incident niet verplicht wettelijk zijn en enkel een bijkomende aanwijzing zijn, verkleint de ernst van het risico.
- **Hoe schat u de waarschijnlijkheid van het risico, vooral met betrekking tot bedreigingen, risicobronnen en geplande controles?** Klein tot verwaarloosbaar, voldoende beveiligingsmaatregelen (toekennen rechten, logisch toegangsbeleid,

logging), pogingen tot wijziging van de beelden laten sporen na, beveiliging van de toegangen van de lokalen en servers, gebruik van antivirus, regelmatige update van windows en software, up-to-date houden van de netwerkveiligheid

SAMENVATTEND

Criteriamatrix

Verwerkingen en de verwerkingsdoeleinden			
Beoogde verwerkingsdoeleinden	**Middelen**	**Finaliteiten**	**Wettelijke basis**
Beeldopnames en opname audio met oog op: -bewaking en toezicht; -handhaving openbare orde; -objectieve waarneming interactie politie-burger; -preventie en de-escalatie; -bepalen politie-inzet; -registreren en terugdringen geweld tegen politie; -objectieve weergave van het politieoptreden in kader van klachtenbehandeling; -beschermen van politieambtenaren en bevorderen veiligheidsgevoel politieambtenaren; -interne opleidingsdoelei	Inzet en gebruik mobiele camera's op het grondgebied van PZ HEKLA (bodycam).	De verwerking gebeurt in toepassing van de wet op het politieambt met het oog op de uitoefening de opdrachten van bestuurlijke politie (artikel 14 van de wet op het politieambt) en de opdrachten van gerechtelijke politie (artikel 15 van de wet op het politieambt).	Wet van 5 augustus 1992 op het politieambt Europese Richtlijn Politie-Justitie (DAPIX) Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *B.S.* 5 september 2018.

nden (training en coaching van collega's).			
Beheer van camerabeelden	Standaardwerkwijze is dat de mobiele camera tijdens dienst in “stand-by modus staat, met een mogelijkheid dit door een eenvoudige handeling te activeren. Deze opnames worden weggeschreven naar een beveiligde server en van het toestel verwijderd van zodra de camera in het docking station wordt geplaatst. De beelden worden maximaal bijgehouden voor een termijn van 1 jaar indien zij geen bijdrage leveren tot het bewijzen van een misdrijf of van toegebrachte schade of tot het identificeren van een dader, een ordeverstoorder, een getuige of slachtoffer. De beelden mogen enkel worden bekeken door bevoegde personen in kader van een gericht dossier. De camera’s worden alleen gebruikt conform de voorwaarden van de WPA. Dienstige beelden worden geëxporteerd naar	idem	Idem

	een externe drager, gevoegd aan het proces-verbaal en neergelegd op de griffie. Beelden voor opleidingen worden geanonimiseerd.		
Raadpleging van beeldopnames door bevoegde personen op basis van een reden die verplicht dient te worden ingevuld en die moet verwijzen naar een concreet en identificeerbaar dossier van bestuurlijke of gerechtelijke politie. De resultaten van de bevraging kunnen geëxporteerd worden naar een externe drager. Elke bevraging wordt gelogd.	Queries in beeldopnames via cameramanagementinformatiesysteem (interface). Bodycam opnames kunnen worden opgezocht op basis van verschillende zoekcriteria: auteur, datum en tijdstip opname, bodycam toestel, eventueel gelinkt pv-nummer.	Idem	Idem
Logging: -raadpleging van een gebruiker -actie van een gebruiker		Controle en monitoring van gebruiksprocedures Rapportering resultaten	Idem
Rechten- en profielbeheer: elke mogelijke actie op de backoffice kan als recht toegekend worden aan een	Organisatorisch via beheersmaatregel	De handelingen die elke gebruiker kan uitvoeren beperken tot wat hij nodig heeft, afhankelijk van de functie die hij uitoefent.	Idem

profiel. Enkel personen met het daartoe voorziene profiel kunnen de camera's gebruiken/hanteren.			
Toegang op afstand door leverancier van het systeem.		Het uitvoeren van bepaalde technisch noodzakelijke handelingen vanop afstand, op afroep, en onder supervisie van de politiebeheerder.	Idem

Beoordeling van de noodzaak en de evenredigheid			
Noodzaak		Doeltreffendheid	Evenwicht belangen
Van de verwerking	Van elk van de verwerkingen		
• fenomenen kunnen voorkomen, vastgesteld of opgespoord worden; • bijdragen aan bewijsvoering; • verhogen van de pakkans verbeteren van heterdaadkracht en opsporing. • escalatie voorkomen • toezicht efficiënter en kwaliteitsvoller door betere besluitvorming (*situational awareness/common operational picture*). • Training- en coachingsdoeleinden (geanonimiseerd)	• Beeldopname: uitoefening de opdrachten van bestuurlijke politie (artikel 14 van de wet op het politieambt) en de opdrachten van gerechtelijke politie (artikel 15 van de wet op het politieambt) • Beheer: idem • Raadpleging van beeldopnames: idem • Logging: monitoring en controle naleving regelgeving en monitoring gebruik • Rechten- en profielbeheer: bepalen van gebruiksrechten conform bevoegdheden van de regelgeving • Toegang door leverancier: operationeel houden van systeem	• camerabeelden worden gebruikt om de doelstelling van de ondersteuning van de opdrachten van bestuurlijke en gerechtelijke politie omschreven in de artikelen 14 tem 25 WPA sneller en efficiënter te bereiken. De verwerking moet leiden tot een betere besluitvorming op het terrein (situational awareness/common operational picture), het handhaven van de openbare orde en veiligheid, het verbeteren van heterdaadkracht en opsporing en het bijdragen aan bewijsvoering.	• de camera 's zullen gebruikt worden voor duidelijk omschreven en gerechtvaardigde doeleinden conform de voorwaarden in WPA. De wet heeft deze evenwichten immers ingebouwd; • strikt beleid en uniforme procedures met betrekking tot de inzet. Het ontwikkelen van een beleid en procedures met betrekking tot het gebruik van de camera's en beleidsvereisten die nodig zijn voor een goede implementatie van de technologie is cruciaal. • training van politieagenten in de manier waarop de camera te gebruiken zal worden voorzien; • een officier wordt door de korpschef organisatorisch belast met de naleving van deze regelgeving; • de camera's zullen noch beelden opleveren die de intimiteit van een persoon

			schenden, noch beelden die gericht zijn op het inwinnen van informatie over vreemdelingen en de filosofische, religieuze, politieke, syndicale gezindheid, etnische of sociale origine, het seksuele leven of de gezondheidstoestand van de gefilmde personen; • bewoners en de bezoekers van de gemeenten van de politiezone HEKLA zullen worden ingelicht over het camerasysteem in voorkomend geval via een mondelinge waarschuwing of via andere informatiekanalen van de HEKLAgemeenten (website, pers, nieuwsbrief); • de technologie beantwoordt aan de state of the art beveiligingsstandaarden; • geregistreerde gegevens zijn niet door elke politie ambtenaar en niet zonder grondige reden raadpleegbaar. De toegang tot de applicatie wordt geregeld conform de WPA. Het is de korpschef die

			beslist of de medewerker toegang krijgt tot de applicatie, en dit op basis van de uitgeoefende functie en het noodzakelijke profiel. Enkel gebruikers met het juiste profiel kunnen het systeem bevragen op basis van een concrete politionele behoefte in het raam van de bestuurlijke of de gerechtelijke politie. Deze reden van raadpleging moet geregistreerd worden. • bewaartermijn van de gegevens is maximaal 1 jaar. De ventilatie gebeurt op maximaal geautomatiseerde wijze en is onherroepelijk. • Derden kunnen hun recht op inzage uitoefenen via de vigerende regelgeving.

RISICOMATRIX (cf. matrix DRI)

Besproken items	*AANWEZIG*	Identificatie		Risico waarde	Aanvaardbaarheid	Maatregelen ter vermindering		Residuele risico
		Kwetsbaarheden	Bedreigingen			Technisch	Operationeel	
ICT-beleid/ beleidsverantwoordelijke specifiek voor ICT/ICT-beleidsplan/ICT-organisatie	ja		Onwettelijke toegang tot de gegevens Ongewenste wijziging van de gegevens Verdwijnen van de gegevens	LAAG	JA	Cf. ICT beleid		/
Beheer van hardware/software/ serverpark/toepassingen/ veiligheidsvoorzieningen (antivirus, firewall,…)/bekabeling	ja		Onwettelijke toegang tot de gegevens Ongewenste wijziging van de gegevens Verdwijnen van de gegevens	LAAG	JA	Cf ICT beleid		/
Fysieke beveiliging en beveiliging van de omgeving	ja			VERWAARLOOSBAAr	JA			/
Beveiliging via beheersmaatregelen	ja		Onrechtmatige queries, misbruik van de beoogde verwerkingen in het systeem Onwettelijke toegang tot de gegevens Ongewenste wijziging van de gegevens Verdwijnen van de gegevens	MATIG TOT LAAG	ja	Privacy by design Toegangsbeheer Rechten- en profielbeheer Data wordt enkel bekeken in beveiligde politie-omgeving Data worden opgeslagen in het beveiligde, politionele datacenter Encryptie Audit trail Controle		Reden van raadpleging nog te implementeren
Leveranciersrelaties	Ja	Geen toegang op afstand door leverancier van het systeem. Toegang ter plaatse door leverancier van het systeem steeds met begeleiding		LAAG	ja	Profielen, firewalls, badges, logging, opmaak NDA		/
Privacy policy	In opmaak							
disciplinaire, statutaire of ordemaatregelen	ja							
SLA				Kwaliteit beelden		Kwaliteitscontrole: - Dagelijkse checks		

						- Identificatie van veel voorkomende problemen en feedback		

Bijkomende opmerkingen

De functionaris voor de Gevensbescherming voor PZ HEKLA werd betrokken.

Aanpak residuele risico's

Volgende residuele risico's dienen aangepakt te worden voor ingebruikname

Toegangsbeheer

- reden raadpleging implementeren teneinde misbruik uit te sluiten

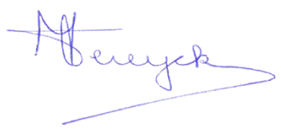
8. AANVRAAG

Overwegende dat

- de bodycams worden gebruikt in uitvoering van de opdrachten van de politie, zoals bepaald in de Wet Politieambt. Het betreffen zowel opdrachten van bestuurlijke als gerechtelijke politie;
- de prioriteiten die werden vastgelegd in de Korpsnota en de interne richtlijnen hierbij leidend zijn;
- PZ HEKLA door bovengenoemde toepassingen in te zetten wil komen tot
    - een betere besluitvorming op het terrein ('operational awareness' tijdens evenementen, incidenten,…);
    - het bevorderen van het veiligheidsgevoel van bewoners en bezoekers van de gemeenten, maar ook van de politiemedewerkers zelf;
    - handhaven van de openbare orde en veiligheid;
    - verbeteren van heterdaadkracht en opsporing;
    - bijdragen aan bewijsvoering (waarheidsvinding, bewijs, reconstructie na incidenten);
    - gebruik beeldmateriaal voor training en coaching;
- de camera's gebruikt worden met respect voor de privacy van de bewoners en bezoekers en dat het publiek ook zal ingelicht worden, zoals voorzien in de wet.

vraag ik de principiële toestemming om de PZ HEKLA gebruik te laten maken van mobiele camera's type bodycam op het ganse grondgebied van de politiezone

Met als doel te streven naar een optimaal gebruik van camera's door de politie en de coherentie binnen het grondgebied van de politiezone zoveel als mogelijk te bewaren, adviseer ik het ontwikkelen van strikte en uniforme procedures met betrekking tot het gebruik en de inzet van de verschillende types camera's enerzijds en anderzijds de training van politieagenten in de manier waarop de camera te gebruiken.



Ivo VEREYCKEN

1 HCP

KC PZ HEKLA