

# Den Haag

## Privacyreglement Cameratoezicht

Stadhuis, stadskantoor, stadsdeelkantoren en overige locaties van de gemeente Den Haag.

Vastgesteld door:

|               | DT-IDC                                                   | GMT | COR | College |
|---------------|----------------------------------------------------------|-----|-----|---------|
| <b>Datum</b>  | 22-1-2019                                                |     |     |         |
| <b>Paraaf</b> | Vastgesteld en akkoord met<br>doorgeleiding div. gremia. |     |     |         |

Datum  
maart 2019

Versie

1.1

Auteur

10.2.E

Opdrachtnaam

Cameratoezicht

Opdrachtgever

10.2.E

Status

Definitief 1.1

## INDEX

---

|            |                                                                |               |
|------------|----------------------------------------------------------------|---------------|
|            | <b>INLEIDING</b>                                               | <b>blz. 3</b> |
| Artikel 1  | Begripsbepalingen                                              | blz. 4        |
| Artikel 2  | Doel van de persoonsregistratie                                | blz. 5        |
| Artikel 3  | De verantwoordelijke van de persoonsregistratie                | blz. 5        |
| Artikel 4  | De beheerder van de persoonsregistratie.                       | blz. 5        |
| Artikel 5  | Derden                                                         | blz. 5        |
| Artikel 6  | Categorieën van personen opgenomen in de persoonsregistratie   | blz. 5        |
| Artikel 7  | Soorten van vastgelegde gegevens en wijze van verkrijging      | blz. 5        |
| Artikel 8  | Toegang tot de registratie                                     | blz. 6        |
| Artikel 9  | Verwijdering en vernietiging van vastgestelde persoonsgegevens | blz. 6        |
| Artikel 10 | Verstreking van persoonsgegevens                               | blz. 6        |
| Artikel 11 | Verbod op koppeling van persoonsgegevens                       | blz. 7        |
| Artikel 12 | Protocolplicht                                                 | blz. 7        |
| Artikel 13 | Beveiliging persoonsgegevens                                   | blz. 7        |
| Artikel 14 | Meldingsregister Autoriteit Persoonsgegevens                   | blz. 7        |
| Artikel 15 | Toegestane bewaartermijn                                       | blz. 7        |
| Artikel 16 | Meldplicht datalekken                                          | blz. 7        |
| Artikel 17 | Klachtenprocedure                                              | blz. 8        |
| Artikel 18 | Doorschakelen 'live-beelden' naar de politie Den Haag          | blz. 8        |
| Artikel 19 | Slotbepaling                                                   | blz. 8        |
|            | Toelichting privacyreglement                                   | blz. 9        |

## BIJLAGEN:

---

|           |                                                     |
|-----------|-----------------------------------------------------|
| <b>01</b> | Protocol: inzage recht cameratoezicht               |
| <b>02</b> | Protocol: inzage en gegevensverstrekking aan derden |
| <b>03</b> | Formulier: verzoek verstrekking camerabeelden       |
| <b>04</b> | Geheimhoudingsverklaring                            |
| <b>05</b> | Protocol: gebruik Bodycam                           |

## INLEIDING

De Wet bescherming persoonsgegevens, per 25 mei 2018 Algemene Verordening Gegevensbescherming (AVG) beschermt burgers tegen het ongeoorloofd vastleggen van zijn of haar persoonsgegevens in geautomatiseerde systemen. De AVG is voor een groot deel gebaseerd op de Europese 'data protectie richtlijn' (95/46/EG).

De focus van de AVG ligt op het verwerken van persoonsgegevens en niet zo zeer het registreren<sup>1</sup> van gegevens. Onder verwerking wordt verstaan, alle handelingen met persoonsgegevens van het verzamelen tot en met het vernietigen. Deze handelingen vallen onder de reikwijdte van de AVG. Het landelijk toezichthoudend orgaan op AVG is per 1 januari 2016, de Autoriteit Persoonsgegevens (AP).

In het kort komt de AVG erop neer dat een organisatie slechts die mag verwerken die voor de organisatie aantoonbaar noodzakelijk zijn om te verzamelen en waar geen expliciet verbod voor bestaat. Het verwerken van beeldmateriaal waarop personen herkenbaar zijn (cameratoezicht) valt onder de AVG. De AVG vereist dat wordt vastgesteld hoe de organisatie de privacy van personen die zijn vastgelegd via beveiligingscamera's optimaal waarborgt. Met dit privacyreglement voldoet de gemeente Den Haag aan de wettelijke kaders gesteld in de AVG.

Doel van dit privacyreglement is om binnen de wettelijke mogelijkheden, kaders vast te stellen die Cameratoezicht rechtvaardigen en de voorwaarden waaronder dit gerechtvaardigd is te beschrijven.

De gemeente Den Haag heeft op 28 maart 2011 het interne-cameratoezicht aangemeld bij de Autoriteit Persoonsgegevens, de melding is opgenomen in het openbare meldingenregister onder nummer: 1315923. Sedert de inwerkingtreding van de AVG per 25-5-2018, is deze meldplicht vervallen.

Dit privacyreglement is opgesteld voor:

- **de betrokkenen:** een ieder van wie gegevens zijn vastgelegd door beveiligingscamera's.
- **de gemandateerde verantwoordelijke:** de directeur van het Intern Dienstencentrum of diens plaatsvervanger.
- **de beheerder:** de teammanager Beveiliging en Veiligheid of diens plaatsvervanger.
- **derden:** zij die namens de organisatie gemachtigd zijn met deze gegevens te werken, de beveiliging.

Voor het opstellen van dit privacyreglement is gebruik gemaakt van de volgende informatiebronnen:

- Website: Autoriteitpersoonsgegevens.nl/cameratoezicht
- Algemene Verordening Gegevensbescherming (AVG) (25-05-2018)
- Protocol cameratoezicht van A+O fonds Gemeenten (06-12-2013)
- Procedure Meldplicht 'datalek' gemeente Den Haag (05-01-2016)
- Convenant gemeente Den Haag en de Politie Den Haag (02-04-2015)

Voor het opstellen van dit privacyreglement is advies ingewonnen bij de volgende functionarissen:

- |               |                                                  |
|---------------|--------------------------------------------------|
| 10.2.E        | - Coördinator AVG (BEC)                          |
| 10.2.E        | - Jurist - Team Advies (BSD)                     |
| 10.2.E        | - Strategisch adviseur (IDC)                     |
| 10.2.E        | - Functionaris Persoonsgegevens (tot 1-1-2019)   |
| 10.2.E S      | - Functionaris Persoonsgegevens (vanaf 1-1-2019) |
| 10.2.E 10.2.E | - Team Integriteit (IDC)                         |

<sup>1</sup> In dit privacyreglement wordt gesproken over registratie van gegevens, hier kan ook verwerken van gegevens worden gelezen.

## Artikel 1 - Begripsbepalingen

In dit privacyreglement wordt verstaan onder:

|                                     |                                                                                                                                                                                                                                                                        |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>persoonsregistratie:</b>         | een samenhangende verzameling van op verschillende personen betrekking hebbende persoonsgegevens die langs geautomatiseerde weg wordt gevoerd of met het oog op een doeltreffende raadpleging van die gegevens systematisch is aangelegd;                              |
| <b>persoonsgegevens:</b>            | elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;                                                                                                                                                                                  |
| <b>verstrekkingen:</b>              | het bekend maken of ter beschikking stellen van persoonsgegevens, voor zover dat geheel of gedeeltelijk steunt op gegevens welke in die persoonsregistratie zijn opgenomen, of die door verwerking daarvan, al dan niet in verband met andere gegevens zijn verkregen; |
| <b>verantwoordelijke:</b>           | het college van burgemeester en wethouders dan wel de door het college gemandateerde functionarissen, zijnde de directeur van het Intern Dienstencentrum (IDC) of diens plaatsvervanger;                                                                               |
| <b>beheerder:</b>                   | degene aan wie de verantwoordelijke de dagelijkse zorg voor een persoonsregistratie heeft opgedragen, de teammanager Beveiliging en Veiligheid en diens plaatsvervanger;                                                                                               |
| <b>derde:</b>                       | ieder, niet zijnde de betrokkene, de verantwoordelijke, die onder rechtstreeks gezag van de verantwoordelijke gemachtigd is om persoonsgegevens te verwerken;                                                                                                          |
| <b>betrokkene:</b>                  | degene op wie een persoonsgegeven betrekking heeft;                                                                                                                                                                                                                    |
| <b>gebouw en terrein:</b>           | in en rond stadhuis, stadskantoor, stadsdeelkantoren en overige gemeente locaties;                                                                                                                                                                                     |
| <b>bedrijfsruimten:</b>             | alle ruimten in beheer bij en bestemd voor het uitoefenen van de gemeentelijke werkzaamheden;                                                                                                                                                                          |
| <b>de wet:</b>                      | Algemene Verordening Gegevensbescherming (AVG);                                                                                                                                                                                                                        |
| <b>Autoriteit Persoonsgegevens:</b> | toezichthouder AVG;                                                                                                                                                                                                                                                    |
| <b>coördinator AVG:</b>             | aangewezen functionaris van het Intern Dienstencentrum (IDC);                                                                                                                                                                                                          |
| <b>veiligstellen:</b>               | kopieën van informatie (beeldmateriaal) opgeslagen op digitale media (USB stick en/of CD/DVD) met als doel deze te gebruiken voor onderzoek en/of vervolging;                                                                                                          |
| <b>verstrekken:</b>                 | het fysiek overhandigen of laten bekijken van beeldmateriaal;                                                                                                                                                                                                          |
| <b>verwerken:</b>                   | registratie (beeldmateriaal) die digitaal wordt opgeslagen en voorzien wordt van extra informatie, zoals tijd, datum, plaats.                                                                                                                                          |

## **Artikel 2 - Doel van de persoonsregistratie (beeldregistratie)**

Doel van deze persoonsregistratie is het vastleggen van persoonsgegevens ter ondersteuning van:

- 2.1** het beveiligen van het personeel, werkzaam voor de gemeentelijke organisatie, alsmede overige personen die zich in de betreffende gebouwen, op de terreinen en/of in de betreffende bedrijfsruimten bevinden;
- 2.2** het beveiligen van de bezittingen tegen inbreuken en/of daden waaruit schade aan of vermindering van de veiligheid welke in of rond de betreffende locatie, kan ontstaan;
- 2.3** de opsporing van personen die zich mogelijk schuldig hebben gemaakt aan het plegen van enig strafbaar feit (publiekrecht) of een onrechtmatige daad (privaatrecht) in of rond het gebouw of het terrein; hierbij geeft de registratie tevens inzicht in de aard en de wijze van het plegen van dit feit.

## **Artikel 3 - De verantwoordelijke voor de persoonsregistratie**

De verantwoordelijke voor deze persoonsregistratie is het college van burgemeester en wethouders. Het college heeft met notitie BSD/2002.228 de integrale verantwoordelijkheid bij de diensten neergelegd. De directeur van het Intern Dienstencentrum is gemandateerd verantwoordelijk en heeft de zeggenschap over de persoonsregistratie. De verantwoordelijke wijst een beheerder aan voor de persoonsregistratie.

## **Artikel 4 - De beheerder van de persoonsregistratie**

De beheerder draagt zorgt voor de naleving van de in dit privacyreglement gestelde regels en beheert alle gegevens en beelden. Het verstrekken van gegevens, zoals bedoeld in artikel 10 van dit privacyreglement, dient met toestemming van de verantwoordelijke te gebeuren, tenzij de wet anders bepaalt. Het verstrekken van persoonsgegevens geschiedt alleen op vertoon van een ondertekend verzoek van de directeur van het Intern Dienstencentrum.

## **Artikel 5 - Derden**

Ieder, niet zijnde de betrokkene, de verantwoordelijke, de beheerder en diens plaatsvervanger, die onder rechtstreeks gezag van de verantwoordelijke gemachtigd is om persoonsgegevens te verwerken:

- 5.1 Beveiliging:** het monitoren van camerabeelden geschiedt uitsluitend door gecertificeerd beveiligingspersoneel in een beveiligde ruimte, de Centrale Meldkamer (CMK). Beveiligingspersoneel is gescreend en is uit hoofde van zijn functie gebonden aan de geheimhoudingsplicht.
- 5.2 Receptie:** medewerkers van de receptie hebben uitsluitend toegang in de zin van het monitoren van de beelden tijdens de werkzaamheden bij de receptie.
- 5.3 Senior medewerker beveiliging:** heeft toegang tot de opgeslagen persoonsgegevens en kan deze gegevens veiligstellen en na toestemming van de beheerder of de verantwoordelijke verstrekken.
- 5.4**

## **Artikel 6 - Categorieën van personen opgenomen in de persoonsregistratie**

De persoonsregistratie bevat uitsluitend persoonsgegevens over:

- 6.1** Alle personen die gebruik maken van -of zich ophouden in- de gemeentelijke objecten en terreinen.
- 6.2** De personen die zich in het gebouw, op het terrein of in de bedrijfsruimte bevinden en zich mogelijk schuldig hebben gemaakt aan het plegen van een strafbaar feit en/of het plegen van een onrechtmatige daad.
- 6.3** Personen die zich ten tijde van het afspelen van het bij punt 2 van dit artikel vermeld voorval in of op de genoemde locatie bevinden en daar al dan niet getuige van zijn geweest.

## **Artikel 7 - Soorten van vastgelegde gegevens en wijze van verkrijging bij persoonsregistratie**

- 7.1** De persoonsregistratie bevat wat betreft de in artikel 6 vermelde personen de volgende gegevens:
  - beeldopname van de persoon;
  - datum en tijd indicatie van de opname;
  - plaats van de opname.
- 7.2** De bovengenoemde persoonsgegevens worden verkregen uit het camerabewakingssysteem dat zich bevindt in en rond het stadhuis, het stadskantoor, de stadsdeelkantoren of andere objecten in gebruik bij de gemeente Den Haag.
- 7.3** Naast 7.2 worden de gegevens verkregen door een mobiel camera- en audio systeem (Bodycam), gehanteerd door beveiligingspersoneel.
- 7.4** Camera's zijn zichtbaar geplaatst of worden zichtbaar gedragen door de beveiliging (Bodycam). Tevens is bij de ingangen van de voor het publiek toegankelijke ruimten zichtbaar melding gemaakt van de aanwezigheid van cameratoezicht.
- 7.5** Medewerkers van de gemeente zijn op de hoogte gesteld van de aanwezigheid van camera's op of rond de werkplek.

- 7.6 De camerabeelden, opgenomen gedurende en buiten werktijden, zullen niet worden aangewend voor de registratie van andere bewegingen of gedragingen van personen dan de registratie van een onrechtmatige daad tegen personen, goederen of het object.

## **Artikel 8 - Toegang tot de registratie**

### **8.1 Directe en indirecte toegang tot de registratie hebben:**

- de verantwoordelijke en de door verantwoordelijke aangewezen personen;
- de beheerder en diens plaatsvervanger;
- opsporingsambtenaren van Politie of Justitie in verband met ingestelde onderzoeken naar strafbare feiten, na verzoek aan de beheerder, op basis van hun wettelijke bevoegdheden;
- voor het uitvoeren van systeembeheeractiviteiten: de door de beheerder aangewezen ICT medewerkers die behoren tot de gemeente en de door de beheerder aangewezen onderhoudsfirma's, mits de beheerder deze toegang protocollert (zie artikel 11).

### **8.2 Voorts hebben toegang tot de registratie na een gerede verdenking van diefstal of andere onregelmatigheden die vallen onder de in artikel 2 genoemde beveiligingsdoeleinden:**

- functionarissen werkzaam voor of namens de verantwoordelijke, belast met het instellen van civielrechtelijke vorderingen tegen de in de persoonsregistratie opgenomen personen;
- de gemeentesecretaris, als eindverantwoordelijk ambtenaar;
- de betrokkene, uitsluitend op verzoek van de verantwoordelijke en uitsluitend tot de gegevens die betrekking hebben op zijn persoon en uitsluitend zonder dat de bescherming van andere personen kan worden geschaad.

## **Artikel 9 - Verwijdering en vernietiging van vastgestelde persoonsgegevens**

- 9.1 Persoonsgegevens die niet meer nodig zijn voor het doel van de registratie, worden automatisch van het videosysteem verwijderd. De gebruikte techniek hierbij is volgens het 'first-in, first-out' principe. De bewaarduur van persoonsgegevens is afhankelijk van een aantal omstandigheden, maar zal nooit langer zijn dan de wettelijke termijn dan wel de door de toezichthouder geadviseerde termijn.
- 9.2 De configuratie is zodanig ontworpen dat beeldmateriaal tenminste 6 dagen zal worden bewaard. Na maximaal 6 dagen is sprake van onherstelbare vernietiging van de registratie.
- 9.3 Mediadragers gebruikt voor het vastleggen van gegevens (zoals harde schijven) worden bij vervanging ter vernietiging aangeboden aan een gespecialiseerd bedrijf, zodat alle aanwezige informatie volledig wordt vernietigd. Hiervoor is een verwerkersovereenkomst afgesloten.

## **Artikel 10 - Verstrekking van persoonsgegevens**

### **Rechten van betrokkenen**

De betrokkene heeft het recht zich vrijelijk en met redelijke tussenpozen tot de verantwoordelijke te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden verwerkt. De verantwoordelijke deelt de betrokkene schriftelijk binnen vier weken mee of hem betreffende persoonsgegevens worden verwerkt.

De verantwoordelijke beslist of de beheerder gegevens kan verstrekken aan personen of instanties die betrokken zijn bij en/of belast zijn met strafrechtelijke dan wel civielrechtelijke acties, voor zover dit voortvloeit uit het doel van de registratie:

- a) De verantwoordelijke beslist of de beheerder gegevens kan verstrekken, indien dit wordt vereist als gevolg van een wettelijk voorschrift dan wel geschiedt met toestemming van de betrokkene.
- b) De verstrekking van deze gegevens blijft achterwege voor zover uit hoofde van ambt, beroep of wettelijk voorschrift geheimhouding is geboden.

Het op schrift gestelde verzoek (zie bijlage 03) tot het inzien van camerabeelden wordt ingediend (mail) bij de verantwoordelijke of beheerder.

De volgende uitgangspunten zijn van toepassing op het inzien van beelden:

### **10.1 - Inzien door betrokkenen**

- a) Een betrokkene mag alleen gegevens zien die hem of haar zelf betreffen.
- b) Daarnaast mag een betrokkene beelden inzien wanneer hij of zij slachtoffer is geworden van een misdrijf en de beelden als bewijsmateriaal kunnen dienen in een strafzaak.

## 10.2 - Inzien door derden

- a) Bij de beoordeling of een verzoek van een derde wordt ingewilligd, wordt overwogen of de verstrekking van persoonsgegevens plaatsvindt ter nakoming van een wettelijke plicht, en/of de verstrekking noodzakelijk is voor de behartiging van het algemeen belang. Verstrekking vindt niet plaats indien het privacybelang van de betrokkene (degene die op de beelden staat) voorgaat.
- b) Er zal aangifte worden gedaan bij de politie als op de beelden een incident wordt waargenomen waarbij er:
  - gevaar bestaat voor de algemene veiligheid van personen of goederen;
  - een vermoeden is van een misdrijf;
  - een misdrijf op heterdaad ontdekt wordt;
  - een aanwijzing is voor een terroristisch misdrijf.
- c) Wanneer Politie of Justitie (Rechter Commissaris en/of Officier van Justitie) op grond van hun bevoegdheden nadere gegevens vorderen, zullen die worden verstrekt. Daarbij zal eventueel het voorbehoud worden gemaakt dat de verstrekte gegevens niet aan de betrokkene bekendgemaakt mogen worden. De directeur van het Intern Dienstencentrum wordt onverwijld hiervan op de hoogte gebracht.

## Artikel 11 – Protocolplicht

- 11.1 De beheerder legt, met instemming van de verantwoordelijke, een verstrekking als bedoeld in artikel 10 van dit privacyreglement vast (bijlage 01 en 02).
- 11.2 De beheerder legt vast welke personen in het kader van onderhoud of voor ICT-doeleinden direct toegang hebben gehad tot het beeldmateriaal, wanneer dat was en welk beeldmateriaal dat betrof.
- 11.3 Op verzoek van de betrokkene gericht aan de verantwoordelijke, verstrekt de beheerder, in afstemming met de coördinator AVG (IDC), binnen 2 weken na ontvangst van het verzoek, informatie aan de betrokkene betreffende een verstrekking van gegevens die zijn persoon betreffen.
- 11.4 De persoonsgegevens worden tenminste 24 maanden bewaard door de beheerder.

## Artikel 12 - Verbod op koppeling van persoonsgegevens

De persoonsgegevens verkregen via Cameratoezicht zijn niet gekoppeld aan andere systemen, zoals het toegangscontrolesysteem.

## Artikel 13 – Beveiliging persoonsgegevens

- a) De beheerder draagt zorg voor dat de code tot het inzien van het beeldmateriaal uitsluitend bekend is bij:
  - de verantwoordelijke;
  - senior medewerker beveiliging;
  - Coördinator Sociale Veiligheid van het Expertisepunt Veilig Publieke Taak van het Bedrijfsvoeringsexpertisecentrum (BEC).
- b) De beheerder treft voorzieningen ter bescherming van de gegevens tegen opzettelijk verkeerd of onachtzaam gebruik door personen die met de werkzaamheden, verbonden aan de werking van de persoonsregistratie zijn belast, evenals beschadiging door toedoen van derden.
- c) Iedereen die betrokken is bij de verwerking van de persoonsregistratie, is verplicht tot geheimhouding van de gegevens in de registratie, behoudens voor zover doelstelling van de persoonsregistratie dan wel enig wettelijk voorschrift hem daartoe noodzaakt

## Artikel 14 - Meldingsregister Autoriteit persoonsgegevens

Vervallen

## Artikel 15 - Toegestane bewaartermijn

De persoonsgegevens moeten uiterlijk 28 dagen nadat de opnames zijn gemaakt worden verwijderd, tenzij een langere bewaartermijn vanwege een incident noodzakelijk is. Na afhandeling van een incident worden de opnames onmiddellijk verwijderd.

## Artikel 16 - Meldplicht datalekken

De gemeente is verplicht om (potentiële) datalekken te melden via de functionaris gegevensbescherming aan de Autoriteit Persoonsgegevens en aan de betrokkene van wie de gegevens zijn gelekt. Iedere medewerker die te maken heeft met vermissing/diefstal van zaken die van de gemeente zijn en die persoonsgegevens bevatten, of met een informatiebeveiligingsincident, dient dit volgens de *“procedure meldplicht datalekken”* direct te melden bij de Servicedesk Automatisering.

#### **Artikel 17 - Klachtenprocedure**

Indien een medewerker of iemand van het publiek een klacht heeft over het cameratoezicht, is de klachtenregeling van de gemeente Den Haag van toepassing.

#### **Artikel 18 – Doorschakelen ‘live-beelden’ naar de Politie Regio Den Haag**

In geval van incidenten en situaties in, dan wel in de directe omgeving van het stadhuis, kan bij de Politie Den Haag de behoefte bestaan die camerabeelden rechtstreeks (‘live’) te kunnen bekijken. De Politie kan haar inzet en inzet van eventuele hulpdiensten daarop afstemmen, wat de uitvoering aan de wettelijke politietaak ten goede komt. De Politie Den Haag heeft met de gemeente Den Haag op 2 april 2015 het convenant *‘Doorschakelen live-beelden bewakingscamera’s Stadhuis’* afgesloten.

Het opslaan van de beelden van de bewakingscamera’s is voorbehouden aan het team Beveiliging en Veiligheid van de gemeente Den Haag. De Politie slaat doorgeschakelde live beelden niet op. Het afstaan van opgeslagen camerabeelden door de beveiliging van de gemeente Den Haag aan derden, kan alleen plaatsvinden als aan artikel 10 van dit privacyreglement wordt voldaan.

#### **Artikel 19 – Slotbepaling**

Dit privacyreglement treedt één dag na vaststelling door het college van burgemeester en wethouders in werking.

### 1. Cameratoezicht

Cameratoezicht wordt selectief uitgevoerd. De opstelling van de camera's en de periode waarin de camera's beelden registreren en/of vastleggen zijn zodanig dat observatie van plaatsen die niet relevant zijn voor voormelde doeleinden zo veel mogelijk wordt beperkt. Per camera is schriftelijk vastgelegd waar en wanneer opnames noodzakelijk zijn.

Cameratoezicht wordt kenbaar uitgevoerd opdat bezoekers en personeel weten wanneer zij zich binnen het bereik van een camera begeven. De gemeente installeert de camera's daarom op een duidelijk zichtbare plaats en brengt bij de ingangen van gemeentelijke gebouwen borden / stickers aan die wijzen op de uitvoering van cameratoezicht.

Beveiligingspersoneel kan gebruik maken van een Bodycam, welke zij activeren in geval van een dreiging, Agressie en Geweld, Calamiteit of ander voorval welke de veiligheid van personen, goederen en/of de organisatie kunnen schaden.

### 2. Wettelijk kader

Op de toepassing van cameratoezicht met digitale technieken is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Deze wet normeert het verwerken van persoonsgegevens.

### 3. Reikwijdte AVG

De AVG is van toepassing op het geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens van natuurlijke persoon. Aangezien beeldmateriaal ook bepaalde informatie over een persoon kan bevatten, valt de verwerking hiervan onder de reikwijdte van de AVG.

### 4. Gerechtvaardigde doeleinden

Persoonsgegevens mogen slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. De verzamelde persoonsgegevens mogen niet verder worden verwerkt op een wijze die onverenigbaar is met het doel waarvoor ze zijn verkregen. De doeleinden moeten herleidbaar zijn tot één van de rechtvaardigingsgronden uit artikel 8 van de AVG. Als eerste grond geldt de ondubbelzinnige toestemming van betrokkene. Indien deze ontbreekt, mogen persoonsgegevens worden verwerkt indien dit noodzakelijk is voor de uitvoering van een overeenkomst, wet, publieke taak of gerechtvaardigd belang.

De beveiliging en bewaking van lijf en goederen wordt algemeen aangemerkt als een gerechtvaardigd belang.

Beelden mogen in het geval van incidenten worden verstrekt aan de politie. Of deze vorm van cameratoezicht rechtmatig is, hangt echter ook af van de hiernavolgende criteria.

#### A) Proportioneel

De uitvoering van cameratoezicht moet proportioneel zijn. Dit houdt in dat er een noodzaak moet zijn om tot deze privacy aantastende maatregel over te gaan. Het bedrijfsbelang moet zwaarder wegen dan de privacy van bezoekers / personeel, en het moet vaststaan dat hetzelfde doel niet op een andere, minder privacygevoelige wijze kan worden gerealiseerd. Voorts geldt dat cameratoezicht op een selectieve wijze moet worden uitgevoerd. Er mogen dus niet meer gegevens worden vastgelegd dan strikt noodzakelijk. Ten slotte moet cameratoezicht altijd onderdeel zijn van een breder pakket van beveiligingsmaatregelen.

#### B) Noodzaak

De gemeente Den Haag loopt als bestuur en als uitvoerende organisatie risico's op het gebied van veiligheid van haar medewerkers en bezoekers. Een deel van het cameratoezicht wordt specifiek toegepast met het oog op de bescherming van het bestuur, personeel en overige medewerkers. De balies, de kas en bepaalde overleg ruimten kunnen met camera's worden geobserveerd om agressie en overvallen te voorkomen dan wel om hier adequaat tegen op te treden. Een ander doel van cameratoezicht is het beveiligen van de bezittingen tegen inbreuken en/of daden waaruit schade aan of vermindering van de veiligheid kan ontstaan.

Voor het gebruik van de mobiele camera (Bodycam) is een protocol opgesteld, dit protocol voldoet aan het gestelde in de privacyreglementen 'Cameratoezicht' en 'Voice Logging' en is als bijlage 05 opgenomen bij dit privacyreglement.

Voor het opsporen van personen die zich mogelijk schuldig hebben gemaakt aan het plegen van een strafbaar feit en/of een onrechtmatige daad, kunnen de camerabeelden worden gebruikt. Hierbij geeft de registratie tevens inzicht in de aard en de wijze van het plegen en/of ontstaan van de strafbare gedraging en/of de onrechtmatige daad.

Daarnaast is er sprake van zogenaamde afgeleide risico's vanwege de aanwezigheid van risico aantrekkende objecten en gebouwen in de directe omgeving. Van de gemeente mag maatschappelijk worden verwacht dat zij adequate maatregelen treft om deze risico's te voorkomen.

### **C) Selectief**

De eis van proportioneel cameratoezicht heeft consequenties voor de plaatsing, het bereik en het daadwerkelijke gebruik van de camera's. Cameratoezicht moet zodanig zijn ingericht dat niet meer plaatsen en personen worden waargenomen en vastgelegd dan voor voormelde doeleinden noodzakelijk is. Dit betekent in principe dat er slechts cameratoezicht mogelijk is ten aanzien van de te beveiligen gebouwen en terreinen en de zich daarop bevindende personen en zaken waarover de zorg van het gemeentebestuur zich uitstrekt. Alleen indien dit voor een goede beveiliging onvermijdelijk is, kunnen ook gedeelten van de openbare weg en/of andere gebouwen in beeld worden gebracht. Het is echter niet toegestaan om privé-vertrekken te observeren. Technisch kan dit worden voorkomen door beperking van de draaibeweging of door hierin 'zwarte vlekken' op te nemen. Een andere mogelijkheid om selectief met cameratoezicht om te gaan is het beperken van de periode waarin de camera's beelden registreren en/of vastleggen. Deze periode moet ook voldoen aan de noodzakelijkheidseis.

De gemeente past bij de uitvoering van cameratoezicht beide beperkingen (noodzakelijk en selectief) toe. Dit wordt per camera vastgelegd in een overzicht waarin ook staat beschreven wanneer opnames noodzakelijk zijn. Zo zullen bepaalde camera's pas opnames maken als een signaal de camera in werking stelt. Dit signaal kan komen van een alarmcontact bij een nooddeur, een agressiemelder of een bewegingsmelder. Andere camera's maken slechts opnames op vastgestelde tijden, zoals de openingstijden van de balies/kas.

### **D) Kenbaarheid**

Een voorwaarde voor rechtmatig cameratoezicht is dat het kenbaar moet zijn. Bezoekers en personeel moeten in kennis worden gesteld van de mogelijkheid dat zij op beelden kunnen voorkomen zodra zij een bepaald gebouw of terrein betreden dat binnen het bereik van de camera's valt. Aan het kenbaarheid vereiste moet niet alleen worden voldaan als er beelden worden vastgelegd, maar ook als sprake is van alleen 'Live' monitoren. Door het zichtbaar ophangen van de camera's en het vermelden van de aanwezigheid van cameratoezicht bij de ingangen van het object, worden medewerkers en bezoekers geattendeerd. Overigens houdt het kenbaarheidsvereiste niet in dat de camera's altijd zichtbaar moeten zijn of dat de burgers op de hoogte moeten worden gesteld van de precieze opnametijden van de camera's.

In artikel 441b van het Wetboek van Strafrecht is de niet-kenbare toepassing van cameratoezicht op voor het publiek toegankelijke plaatsen strafbaar gesteld. De straf kan een hechtenis van ten hoogste twee maanden inhouden of een geldboete van de derde categorie.

## **5. Andere maatregelen**

Cameratoezicht heeft het grootste effect als de maatregel wordt ingebed in een pakket van andere maatregelen die samen bijdragen aan de beveiligingsdoeleinden. Zo is een belangrijke maatregel de efficiënte en effectieve inzet van beveiligingspersoneel. Om tijdig onraad te herkennen en adequaat hiertegen op te treden, zijn goed opgeleid personeel en goede werkafspraken belangrijk. Het cameratoezicht dient ter aanvulling en ondersteuning van het fysiek toezicht, in en rond de gebouwen.

## **6. Geheimhouding en beveiliging**

Op grond van de AVG rust op het personeel dat noodzakelijkerwijs bij het cameratoezicht is betrokken een geheimhoudingsplicht. Voorts moet de gemeente passende technische en organisatorische maatregelen nemen om het verlies van de opnames of onrechtmatige verwerking tegen te gaan. De AVG geeft niet aan wat passende beveiligingsmaatregelen zijn. In het woord "passend" ligt besloten dat de maatregelen proportioneel zijn gelet op de aard van de gegevens, de stand van de techniek en de kosten van de maatregelen. De mogelijke gevoeligheid van de opnames vraagt om een daarop toegesneden beveiliging.

Het monitoren geschiedt door beveiligingspersoneel. Zij zijn uit hoofde van hun functie gebonden aan een geheimhoudingsplicht. Zij hebben geen toegang tot de opnameapparatuur. Deze bevindt zich in een afgesloten ruimte. De beheerder heeft op grond van aan hem toegekende bevoegdheden toegang tot deze ruimte (toegangspas) en de opnameapparatuur. Slechts de betrokkenen en de gemeentesecretaris kunnen (schriftelijk) verzoeken om opnames te bekijken. De directeur van het Intern Dienstencentrum dient vervolgens schriftelijk hiervoor toestemming te verlenen. Degenen die toegang krijgen tot de gegevens zijn gehouden tot geheimhouding. Het bekijken van de opnames moet noodzakelijk zijn voor de doeleinden waarvoor het cameratoezicht is ingesteld, wat inhoudt dat het bekijken van de opnames proportioneel moet zijn.

Dit zal bijvoorbeeld doorgaans het geval zijn indien de opnames nodig zijn om informatie te verkrijgen over strafbare feiten. De directeur van het Intern Dienstencentrum kan op basis van de opnames aangifte doen.

Indien de gemeente een vordering krijgt van opsporingsinstanties of de Algemene Inlichtingen- en Veiligheidsdienst, dan heeft zij de wettelijke plicht om hieraan te voldoen. Bij besluit van 20 juni 2006 (BSD/2006.1603) heeft het college de diensthoofden gemachtigd om deze vorderingen af te doen. Dit betekent dat de directeur IDC deze bevoegdheid heeft ten aanzien van vorderingen van opnames.

#### **7. Bewaartermijnen**

Persoonsgegevens mogen op grond van de AVG niet langer worden bewaard dan noodzakelijk is voor de verwerking van de doeleinden waarvoor zij zijn verzameld. Het landelijk toezichthoudend orgaan op de privacywetgeving, de Autoriteit persoonsgegevens geeft als richtlijn een bewaartermijn van maximaal 28 dagen. De gemeente bewaart de opnames maximaal 6 dagen, waarmee zij ruimschoots blijft binnen de termijn uit de richtlijn. Met uitzondering voor beelden waarop incidenten zijn vastgelegd. Deze kunnen dienen als bewijsmateriaal bij strafvervolgning of schade aansprakelijkheid bepaling.

#### **8. Meldingsplicht**

Vervallen

#### **9. Rechten betrokkenen**

De AVG bevat voor een ieder het recht op inzage in, aanvulling, verbetering, verwijdering en afscherming van zijn/haar persoonsgegevens. Ook kan een ieder verzet aantekenen tegen het gebruik van zijn/haar gegevens.

#### **10. Meldplicht datalek**

Sinds 1 januari 2016 geldt de meldplicht datalekken.

Er is sprake van een datalek als er sprake is van een inbreuk op de beveiligingsmaatregelen waarbij persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Voorbeelden van een datalek zijn het verlies van een mobiel apparaat waarop gevoelige persoonsgegevens staan. Maar ook 'computerhacking', besmetting met 'ransomware', of het technische falen van apparatuur, ook stroomuitval, wateroverlast kan leiden tot een datalek.

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (leken) van gegevens, maar ook onrechtmatige verwerking van gegevens.

We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 33 en 34 van de AVG). Een datalek dient uiterlijk binnen 72 uur na ontdekking van het datalek te worden gemeld aan de toezichthouder.

#### **11. Samenwerken Politie Den Haag**

De Politie meldkamer heeft de gemeente Den Haag benaderd, om in specifieke gevallen gebruik te kunnen maken van live beeldmateriaal dat de Centrale Meldkamer (CMK) van de gemeente beschikbaar heeft. De Politie kan hierdoor beter bewegingen van mensen monitoren en bij dreiging of escalatie de inzet van de politie bepalen. Er is een convenant afgesloten tussen de gemeente Den Haag en de Politie Den Haag. Voorwaarde is dat de CMK kan bepalen of de beelden worden doorgezeten (vrijwillige basis) en het beeldmateriaal niet door de Politie wordt opgeslagen en bewaard. Met deze voorwaarden in het convenant voldoet de gemeente Den Haag nog steeds aan AVG.

- 1 Op het gebruik van cameratoezicht in en om het stadhuis, het stadskantoor, de stadsdeelkantoren en andere objecten van de gemeente Den Haag, is de Algemene Verordening Gegevensbescherming (AVG) van toepassing.

- 2 Het recht op inzage wordt geregeld in artikel 15 van de AVG en deze luidt als volgt:

Een betrokkene/verzoeker heeft het recht zich vrijelijk en met redelijke tussenpozen tot de verantwoordelijke van de gemeente Den Haag (namens het college van burgemeester en wethouders) te wenden met het verzoek hem/haar mede te delen of hem/haar betreffende persoonsgegevens worden verwerkt.

N.B. Dit mogen alleen gegevens zijn die de betrokkene/verzoeker zelf betreffen.

- 3 Onder betrokkene/verzoeker wordt verstaan: een ieder die zich in, of rond het met camera bewaakte object van de gemeente Den Haag begeeft en wiens gegevens worden verwerkt.
- 4 Naar aanleiding van het verzoek wordt in eerste instantie schriftelijk informatie verschaft, welke inzicht geeft in het doel van cameratoezicht bij de gemeente Den Haag.
- 5 Een verzoek om verstrekking/inzage dient binnen 5 dagen na het tijdstip van registratie te worden gedaan, aangezien de beelden daarna mogelijk worden gewist, al dan niet door automatische overschrijving. De beelden worden geïsoleerd totdat de verantwoordelijke gereageerd heeft op het inzageverzoek.
- 6 Betrokkene/verzoeker hoeft geen opgave van redenen te doen waarom hij/zij verstrekking/inzage wil van de camerabeelden.

Het verzoek om verstrekking/inzage moet schriftelijk (per brief of mail) worden gedaan en dient specifiek aan te geven om welke dag en welk tijdstip het gaat. Voor het doen van het verzoek is een standaardformulier beschikbaar bij de receptie.

- 7 De verantwoordelijke voor de verwerking dient binnen twee weken een schriftelijke reactie te geven (per brief of email) op het verzoek van de betrokkene/verzoeker.
  - 7.1 In deze reactie moet op een duidelijke en begrijpelijke manier aan de betrokkene/verzoeker worden uitgelegd welke gegevens gebruikt worden, met welk doel en aan wie de gegevens eventueel verstrekt zijn.
  - 7.2 Ook wordt aangegeven of de persoonsgegevens gebruikt worden voor het opsporen van daders van strafbare feiten die hebben plaatsgevonden op dezelfde plek en hetzelfde tijdstip als waar het verzoek om inzage betrekking op heeft.
  - 7.3 Indien er zich geen incidenten hebben voorgedaan en/of de gegevens inmiddels gewist zijn, wordt dit gemeld aan de betrokkene/verzoeker (bijvoorbeeld doordat tussen het tijdstip van registratie en het verzoek om verstrekking/inzage meer dan 5 dagen zijn verstreken).
- 8 Een weigering van of het niet tijdig reageren op een inzageverzoek is een besluit in de zin van de Algemene wet bestuursrecht (Awb). Het indienen van een bezwaarschrift en het vragen van een voorlopige voorziening staan hierbij open.
- 9 Indien de betrokkene/verzoeker een klacht heeft over de wijze waarop verzoeken naar aanleiding van dit onderwerp zijn behandeld, is de klachtenregeling van de gemeente Den Haag van toepassing.

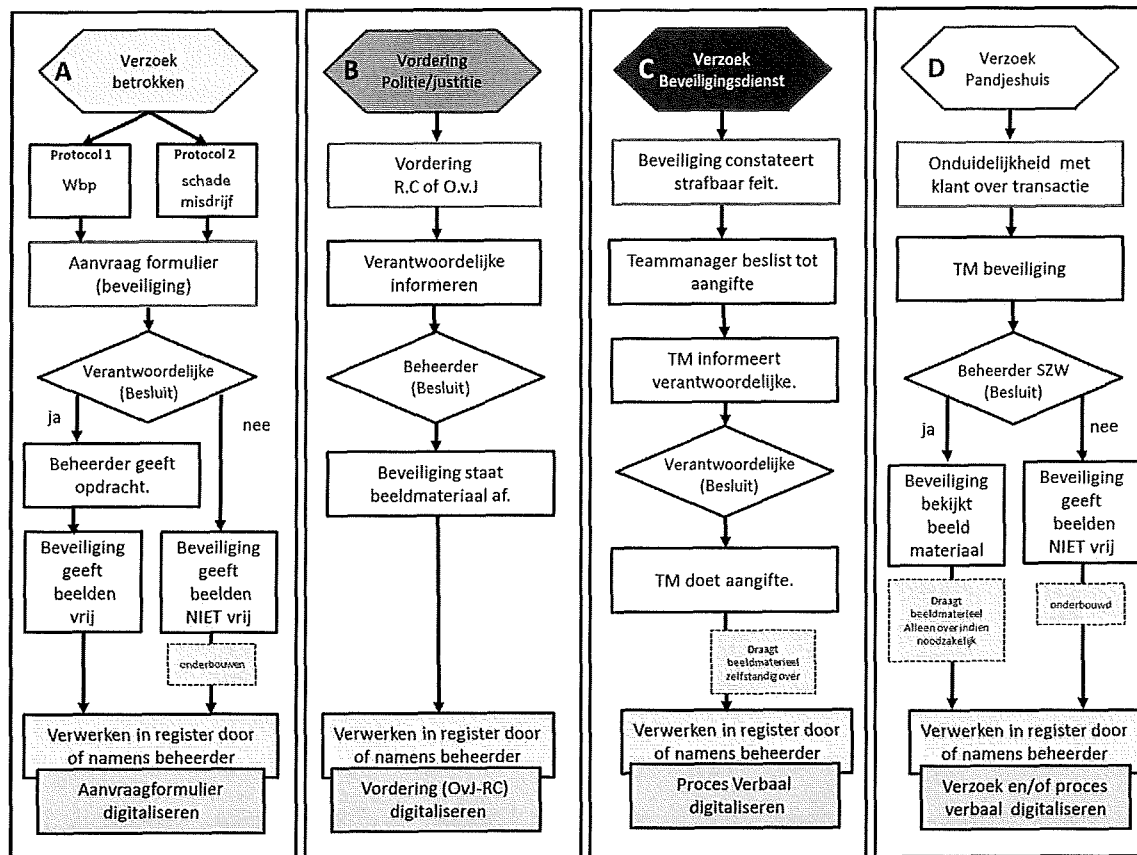
## **BIJLAGE 02:** Protocol gegevensverstrekking aan derden in relatie tot Cameratoezicht

---

In dit protocol staat de procedure beschreven die wordt gevolgd indien derden verzoeken om informatie te verstrekken die voortvloeit uit het cameratoezicht.

- 1 Het gebied in en om en om het stadhuis, het stadskantoor, de stadsdeelkantoren en andere objecten van de gemeente Den Haag is onderworpen aan cameratoezicht. Dit cameratoezicht is primair gericht op de beveiliging van het gebouw. Op het gebruik van het genoemde cameratoezicht is de Algemene Verordening Gegevensbescherming (AVG) van toepassing.
- 2 Onder persoonsgegevens wordt verstaan: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4, lid 1 van de AVG).
- 3 Onder verantwoordelijke wordt verstaan: het college van burgemeester en wethouders dan wel de door het college gemandateerde functionarissen, zijnde de directeur van het Intern Dienstencentrum (IDC) of diens plaatsvervanger (notitie BSD/2002.228).
- 4 Een verzoek om inzage/verstrekking dient bij voorkeur binnen 6 dagen na het tijdstip van registratie te worden gedaan aangezien de beelden daarna mogelijk worden gewist, al dan niet door automatische overschrijving. Indien een verzoek binnen deze termijn wordt gedaan, dan worden de beelden meteen geïsoleerd tot er op het informatieverzoek is gereageerd door de verantwoordelijke of tot zolang voor verzoeker de feitelijke mogelijkheid bestaat de beelden in te zien.
- 5 Verzoeken van derden om gegevensverstrekking dienen gemotiveerd en schriftelijk (per brief of mail) bij de verantwoordelijke te worden ingediend. Het verzoek dient specifiek aan te geven om welke opnames het gaat (welke dag en welk tijdstip).
- 6 Bij de beoordeling van het verzoek wordt in ieder geval nagegaan of er een wettelijke verplichting is om de persoonsgegevens te verstrekken en of het noodzakelijk is vanwege het belang van de gemeente of de derde aan wie de gegevens worden verstrekt. Er wordt geen persoonlijke informatie verstrekt indien het privacybelang van de betrokkene voorgaat.
- 7 Er zal aangifte gedaan worden bij de Politie als het gaat om een incident waarbij er
  - 1) gevaar bestaat voor de algemene veiligheid van personen of goederen,
  - 2) sprake is van een misdrijf of een vermoeden van een misdrijf,
  - 3) aanwijzingen zijn voor een terroristische aanslag.
- 8 Wanneer Politie of Justitie op grond van hun bevoegdheden nadere gegevens vorderen, zullen die worden verstrekt. Daarbij zal eventueel het voorbehoud worden gemaakt dat de verstrekte gegevens niet aan de betrokkene bekendgemaakt mogen worden.
- 9 De gegevens worden verwijderd wanneer deze niet meer noodzakelijk zijn voor het registreren van het incident, en zodra mogelijk vernietigd.
- 10 De gegevens worden verwijderd na verloop van 6 dagen, tenzij Politie of Justitie vorderen dat ze gedurende een door hen te bepalen periode bewaard en beschikbaar gehouden dienen te worden.
- 11 Aan het verstrekken van de gegevens kunnen door de verantwoordelijke nadere voorwaarden worden verbonden, bijvoorbeeld dat de gegevens slechts éénmalig mogen worden gebruikt of dat deze niet mogen worden gebruikt voor publicatie.
- 12 Indien de betrokkene/verzoeker een klacht heeft over de wijze waarop informatieverzoeken zijn behandeld, is de klachtenregeling van de gemeente Den Haag van toepassing.

## Stroomschema verstrekken van camerabeelden aan derden



Ondergetekende

Volgnummer:

**Naam:**

**Adres:**

**Woonplaats:**

**Telefoonnummer:**

**E-mailadres:**

**Soort legitimatiebewijs:** paspoort / rijbewijs / identiteitskaart (doorhalen wat niet van toepassing is)

**Nr. legitimatiebewijs:**

verzoekt tot inzage of verstrekking van relevante camerabeelden voor het volgende doel\*:

.....  
.....  
.....

**A)** Het incident heeft plaatsgevonden op de volgende locatie:

Adres locatie ..... exacte plaats in/rond deze locatie .....

**B)** Het incident heeft plaatsgevonden in de periode tussen:

datum.....tijdstip..... en  
datum.....tijdstip.....

#### **Verklaring van geheimhouding**

Ondergetekende verklaart door ondertekening van dit document dat de beelden die aan hem of haar verstrekt worden, alleen gebruikt worden voor het hierboven omschreven doel. Doorverstrekking kan alleen geschieden als dit noodzakelijk is voor het doel en verder geldt een wettelijke geheimhoudingsplicht.

Voor akkoord betrokkene:

Datum:

Handtekening:

Dit verzoek graag volledig ingevuld en ondertekend mailen naar: [beveiliging@denhaag.nl](mailto:beveiliging@denhaag.nl)

---

\* Camerabeelden kunnen uitsluitend worden verstrekt met het doel:

1. de bescherming van de veiligheid van een of meer natuurlijke personen;
2. de beveiliging van de toegangen tot de objecten van de gemeente Den Haag;
3. de bewaking van de objecten en van de gemeente Den Haag;
4. het vastleggen van incidenten in en rond de objecten van de gemeente Den Haag

Deze geheimhoudingsverklaring is opgemaakt op ..... - 20..

Ondergetekende (naam) :

Voornamen (voluit) :

Geboortedatum : Geboorteplaats:

Werkzaam bij : International Security Agency B.V (ISA)

Ondergetekende verklaart hierbij,

Dat hij/zij zich bewust is van zijn/haar verplichtingen tegenover onbevoegden strikte geheimhouding te betrachten ten aanzien van alles van hem/haar ten gevolge van zijn/haar dienstbetrekking of andere overeenkomst bekend wordt, zowel voor wat betreft de informatie van de werkgever als voor informatie van object gebonden zaken van de opdrachtgever;

Dat hij/zij – voor zover nodig – hierbij nadrukkelijk op zijn/haar verplichtingen en verantwoordelijkheden tot beveiliging van deze materie is gewezen;

Dat hij/zij zich bewust is dat bij overplaatsing in een andere functie dan wel bij beëindiging van zijn/haar huidige dienstverband of overeenkomst door hem/haar aanvaarde verplichtingen van kracht blijven en hij/zij onderworpen blijft aan de sancties bij de wet gesteld, voor het geval dat hij/zij bedoelde gerubriceerde gegevens opzettelijk of uit onachtzaamheid ter kennis van onbevoegde doet komen. Hieronder mede begrepen alle informatie die de privacy van personen kunnen schade en hij/zij kan waarnemen en/of gegenereerd uit beveiligingssystemen.

Dat hij/zij bekend is gemaakt met de wettelijke en administratieve gevolgen van schending van de geheimhoudingsplicht en niet- naleven van de beveiligingsbepalingen, zoals deze zijn vervat in de artikelen 98, 98a, 272, en 273 van het Wetboek van Strafrecht (betreft schending van staats-, ambts- en beroepsgeheimen).

Datum: ..... - 20..

Plaats: .....

.....

(handtekening)

## **Bijlage 05: Protocol gebruik Bodycam**

---

### **Doel:**

Het terugdringen van het aantal voorvallen van agressie en geweld tegen medewerkers van de gemeente Den Haag en/of ingehuurde beveiligingsmedewerkers.

De beelden van een Bodycam worden gebruikt:

- 1) Extern, als bewijsmateriaal voor Politie en Justitie, in geval van opsporing en vervolging van strafbare feiten na een aangifte.
- 2) Intern, als bewijsmateriaal voor 'het overtreden van de huisregels door bezoekers, medewerkers dan wel bestuurders en het kunnen opleggen van een mogelijke sanctie, zoals een gebouwontzegging.

### **Preventie:**

Naar verwachting leidt het gebruik van een Bodycam door beveiligingsmedewerkers tot vermindering van het aantal agressie en geweld incidenten. Dit komt door de sterke preventieve werking van de Bodycam. De agressor weet dat alles wat hij doet en zegt wordt geregistreerd en zal zich daarom minder snel agressief opstellen. Het waarborgen van de veiligheid van interne en externe medewerkers van de gemeente Den Haag is het uitgangspunt voor het inzetten van de Bodycam op (geselecteerde) risico locaties.

### **Verantwoordelijke:**

De teammanager Beveiliging en Veiligheid bepaalt n.a.v. een uitgevoerde risicoanalyse welke locaties, dan wel ruimten hiervoor in aanmerking komen, hij is de 'verantwoordelijke'.

### **Reglement:**

De door het bestuur vastgestelde privacyreglementen Cameratoezicht en 'Voice Logging' zijn van toepassing op de registratie van beeld en geluid door de Bodycam. In deze privacyreglementen is beschreven wat het doel is van Cameratoezicht en 'Voice Logging' en hoe de gemeente Den Haag omgaat met de registratie- en beveiliging van beeld- en geluidsopnames.

### **Gebruiker(s):**

De beveiligingsmedewerkers in risicovolle objecten en ruimten kunnen gebruik maken van een Bodycam welke de gemeente Den Haag ter beschikking heeft gesteld. Eigen Bodycams mogen niet worden gebruikt tijdens de uitvoering van beveiligingswerkzaamheden.

De beveiligingsmedewerkers zijn op de hoogte gesteld van de privacyreglementen Cameratoezicht en 'Voice Logging' en het protocol voor gebruik van de Bodycam.

De beveiligingsmedewerker bepaalt zelf wanneer hij de Bodycam activeert, de Bodycam wordt ingezet voor zijn/haar persoonlijke veiligheid.

### **Beveiliging van het systeem:**

Het beeld en geluid materiaal wordt versleuteld opgeslagen op de Bodycam, welke is beveiligd met een wachtwoord. Dit wachtwoord is alleen bij de teammanager Beveiliging en Veiligheid en diens plaatsvervanger bekend. Overzetten van de opnames gebeurt uitsluitend binnen een daarvoor ingerichte database, deze is beveiligd met een wachtwoord.

### **Uitlezen opnames:**

Voor het uitlezen van de opnames zijn de privacyreglementen Cameratoezicht en 'Voice Logging' van toepassing, waarin onder meer wordt vermeld dat de beelden slechts na toestemming van de teammanager Beveiliging en Veiligheid mogen worden uitgelezen.

Het is niet toegestaan om beeld- en geluidsmateriaal te verspreiden, anders dan in de privacyreglementen is vermeld.

## Gegevensbeschermings-effectbeoordeling (PIA)

### 1 Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

Onder 1 wordt de eerste stap beschreven van de PIA: een overzicht van de relevante feiten van de voorgenomen gegevensverwerkingen. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling.

#### A Voorstel

Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet en context waarbinnen deze plaatsvindt op hoofdlijnen.

Het Privacyreglement Cameratoezicht IDC gemeente Den Haag heeft als doel om binnen de wettelijke mogelijkheden, kaders vast te stellen die intern (beveiliging) Cameratoezicht rechtvaardigen en de voorwaarden waaronder dit gerechtvaardigd is te beschrijven.

IDC zet 'zichtbare' beveiligingscamera's in op een groot aantal locaties van de gemeente, zowel aan de buitenzijde van de locaties als in openbare ruimte binnen deze locaties.

De beveiliging kan gebruik maken van een bodycam, die duidelijk zichtbaar op het uniform van de beveiliging wordt gedragen. De beveiliging zal in geval van een (be)dreiging, incident of calamiteit de bodycam activeren. De bodycam maakt zowel beeld- als geluidsopnamen.

Met het Privacyreglement Cameratoezicht maakt de gemeente Den Haag inzichtelijk wat de kaders zijn, wie verantwoordelijk is, om welke gegevens het precies gaat, wat de voorwaarden zijn en hoe de bescherming van gegevens in geborgd.

Noot: Heimelijk (verborgen) cameratoezicht valt niet onder dit reglement.

#### B Persoonsgegevens

Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van persoonsgegevens tevens aan op wie die betrekking hebben. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificerend.

1. Medewerkers gemeente Den Haag - betreft gewone gegevens; 2. leveranciers - betreft gewone gegevens; 3. bezoekers - betreft gewone gegevens en 4. overige betrokkenen (omstanders en passanten) - betreft gewone gegevens.

Het beeldmateriaal toont een weergave van een persoon(signalement) en de handelingen en gedragingen van deze persoon

#### C Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

De persoonsregistratie bevat wat betreft de in punt B vermelde personen de volgende gegevens:

- beeld opname van de persoon;
- datum en tijd indicatie van de opname;
- plaats van de opname.

#### D Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

Doel van deze persoonsregistratie is het vastleggen van persoonsgegevens ter ondersteuning van:

A) het beveiligen van het personeel, werkzaam voor de gemeentelijke organisatie, alsmede overige personen die zich in de betreffende gebouwen, op de terreinen en/of in de betreffende bedrijfsruimten bevinden;

B) het beveiligen van de bezittingen tegen inbreuken en/of daden waaruit schade aan of vermindering van de veiligheid kunnen voortvloeien, in of rond de betreffende locatie;

C) de opsporing van personen die zich mogelijk schuldig hebben gemaakt aan het plegen van enig strafbaar feit (publiekrecht) of een onrechtmatige daad (privaatrecht) in of rond het gebouw of het terrein.

#### E Betrokken partijen

Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

A) Verwerkingsverantwoordelijke: Burgemeester en wethouders van Den Haag- gemandateerd aan de directeur van het Intern Dienstencentrum (IDC), doel is het borgen van de veiligheid en de bescherming van eigendommen binnen de gebouwen van de gemeente Den Haag

B) verwerker/beheerder: degene aan wie de verantwoordelijke de dagelijkse zorg voor een persoonsregistratie heeft opgedragen, zijnde de teammanager Beveiliging en Veiligheid en zijn plaatsvervanger. Tevens de leverancier van de technische beveiligingsinstallatie, waarmee een verwerkingsovereenkomst is afgesloten.

C) verstrekker: de teammanager Beveiliging en Veiligheid en zijn plaatsvervanger

D) ontvanger: 1) justitie en politie 2)interne zaken 3)betrokkenen op verzoek

Aanvulling:

1) Beveiliging: het monitoren van 'Live'camera beelden geschiedt uitsluitend door gecertificeerd beveiligingspersoneel in een beveiligde ruimten, de Centrale Meldkamer (CMK). Beveiligingspersoneel is gescreend en is uit hoofde van zijn functie gebonden aan de geheimhoudingsplicht;

2) Receptie: medewerkers van de receptie hebben uitsluitend toegang in de zin van het monitoren van de beelden tijdens de werkzaamheden bij de receptie;

3) Senior medewerker beveiliging (is Plaatsvervangend verstrekker): heeft toegang tot de opgeslagen persoonsgegevens en kan gegevens veiligstellen en na toestemming van de verantwoordelijke gegevens verstrekken.

4) Bij risicovolle evenementen kan de Politie live meekijken (monitoring) naar de beschikbare camerabeelden.

**F Belangen bij de gegevensverwerking**

Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

De belangen die de verwerkingsverantwoordelijke en anderen hebben zijn:

- A) het beveiligen van het personeel, werkzaam voor de gemeentelijke organisatie, alsmede overige personen die zich in de betreffende gebouwen, op de terreinen en/of in de betreffende bedrijfsruimten bevinden;
- B) het beveiligen van de bezittingen tegen inbreuken en/of daden waaruit schade aan of vermindering van de veiligheid, die in of rond de betreffende locatie, kan ontstaan;
- C) de opsporing van personen die zich mogelijk schuldig hebben gemaakt aan het plegen van enig strafbaar feit (publiekrecht) of een onrechtmatige daad (privaatrecht) in of rond het gebouw of het terrein; hierbij geeft de registratie tevens inzicht in de aard en de wijze van het plegen van dit feit.

**G Verwerkingslocaties**

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

Gegevensverwerking vindt alleen in Nederland plaats. De gemeente Den Haag beheert zelf het beeldmateriaal in een beveiligde ruimte binnen de Centrale Meldkamer op het Stadhuis.

## H Techniek en methode van gegevensverwerking

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi)geautomatiseerde besluitvorming, profilering of big dataverwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

Er wordt gebruik gemaakt van beveiligde Digitale Recorders om beeldmateriaal op te slaan, deze recorders staan in een beveiligde ruimte opgesteld.

Beeldmateriaal wordt slecht uitgelezen op een daarvoor bestemde computer, indien zich een ernstig voorval heeft voorgedaan (veiligheid) of een mogelijk strafbaar heeft plaatsgevonden (beveiliging) Indien beeldmateriaal wordt veiliggesteld gebeurt dit op een beveiligde USB stick, en alleen indien er spraken is van een incident/calamiteit.

Data worden niet gebruikt voor andere analyse doeleinden.

## I Juridisch en beleidsmatig kader Juridisch en beleidsmatig kader

Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen.

A) ARBO-wet - bescherming van medewerkers tegen ongewenst gedrag (agressie en geweld).

B) wetboek van strafrecht - vaststellen van strafbare gedragingen

C) Burgerlijk wetboek - vaststellen van een onrechtmatige daad (artikel 6.162 BW e.v.)

D) Privacyreglement Cameratoezicht IDC (2019)

## J Bewaartermijnen

Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

De Autoriteit Persoonsgegevens (AP) geeft als richtlijn voor het bewaren van camerabeelden 28 kalenderdagen.

De gemeente Den Haag houdt maximale bewaartermijnen van 28 kalenderdagen aan, maar zal in veel gevallen -door technische beperkingen- beeldmateriaal ongeveer 6 werkdagen opslaan.

A) het beveiligen van het personeel;  
maximaal 28 kalenderdagen

B) het beveiligen van de bezittingen tegen inbreuken en/of daden;  
maximaal 28 kalenderdagen voor de periferie en openbare ruimte  
maximaal 28 kalenderdagen voor de vitale ruimten

C) de opsporing van personen die zich mogelijk schuldig hebben gemaakt aan het plegen van enig strafbaar feit:  
maximaal 28 kalenderdagen

Na het verstrijken van 28 kalenderdagen wordt het beeldmateriaal automatisch overschreven door nieuw beeldmateriaal. Indien beeldmateriaal is veilig gesteld voor onderzoek, zoals beschreven bij de verwerkingsdoeleinden, kan dit beeldmateriaal langer worden bewaard.

---

## 2 Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel 1 of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen. Voor dit onderdeel van de PIA is in het bijzonder juridische expertise nodig.

### A Rechtsgrond

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

A. De verwerking is noodzakelijk om de vitale belangen van de betrokkene of een ander natuurlijk persoon te beschermen (bescherming van lijf en leden en/of goederen) (art. 6, sub d, AVG)

10.2.E is een gerechtvaardigd belang voor de organisatie en zijn medewerkers om camera observatie uit te voeren in en rond de gebouwen van de Gemeente Den Haag in gebruik bij de interne organisatie. Het waken over de veiligheid van personen en goederen tegen ongewenste inbreuk, rechtvaardigt Cameratoezicht indien dit proportioneel plaatsvindt (art 6, sub f, AVG).

Zie ook wet- en regelgeving, zoals genoemd bij onderdeel 1 onder I.

### B Bijzondere persoonsgegevens

Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dat is toegestaan.

N.v.t.

### C Doelbinding

Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

Het doel van cameratoezicht is het borgen van de veiligheid en beveiligen van de belangen van personeel en bezoekers van de gemeentelijke gebouwen en van de gemeente als zodanig. Om het handelen van betrokken functionarissen, beveiliging en BHV, bij incidenten te kunnen analyseren en evalueren, kan de teammanager Beveiliging en Veiligheid gebruik maken van beschikbare beelden. Als er klachten zijn van burgers over gebeurtenissen dan kunnen de beelden worden gebruikt om de feiten vast te stellen. In opdracht van de directeur IDC kunnen de beelden worden veilig gesteld.

### D Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.

- Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?
- Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?

Proportionaliteit: Cameratoezicht vind alleen plaats als dit voor de genoemde doelen noodzakelijk is, indien dit niet meer het geval is wordt de camera verwijderd. Het aantal in te zetten camera's wordt zoveel mogelijk tot een minimum beperkt, maar moet voldoende zijn om de doelstelling te kunnen borgen. Met het uitvoeren van risicoanalyses kan worden bepaald of minder camera's toereikend zijn voor de doelbinding.

Subsidiariteit: de verwerkingsdoeleinden zijn in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, te verwezenlijken. Het inzetten van voldoende personeel 24/7 om dezelfde doelstelling te bewerkstelligen is niet realistisch.

**E Rechten van de betrokkene**

Geef aan hoe invulling wordt gegeven aan de rechten van betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzonderingen dat is toegestaan.

De betrokkene heeft het recht zich vrijelijk en met redelijke tussenpozen tot de verantwoordelijke te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden verwerkt. De verantwoordelijke beslist of de beheerder gegevens kan verstrekken aan personen of instanties die betrokken zijn bij en/of belast zijn met strafrechtelijke dan wel civielrechtelijke acties. Indien de belangen van andere betrokkenen, die ook op het beeldmateriaal zijn vastgelegd prevaleren boven die van de aanvrager kan de Verantwoordelijke beslissen materiaal niet te verstrekken of voor inzage beschikbaar te stellen. De verstrekking van gegevens blijft achterwege voor zover uit hoofde van ambt, beroep of wettelijk voorschrift geheimhouding is geboden.

---

### 3 Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerking zoals in onderdeel 1 en 2 zijn beschreven en beoordeeld. Het gaat hierbij overigens niet om de risico's van de verwerkingsverantwoordelijke zelf.

#### A Risico's

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:

- welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;
- de oorsprong van deze gevolgen;
- de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
- de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

Algemeen: gegevens worden alleen verstrekt aan derden op vordering van Politie en Justitie en ook als er sprake is geweest van een mogelijk strafbaar feit of een onrechtmatige handeling. De belangen van de mogelijke benadeelde wegen zwaarder dan die van overige betrokkenen.

De kans op lekken van opgeslagen camerabeelden wordt als zeer klein ingeschat, de kans op negatieve gevolgen voor de rechten en vrijheden van betrokkenen is minimaal. Bovendien gaat het niet om bijzondere persoonsgegevens, zodat de impact van de gevolgen voor de betrokkene te verwaarlozen is.

Het netwerk voor transport en de opslag van camerabeelden is een beveiligde omgeving. De ruimte waar beeldmateriaal wordt opgeslagen en het opslagsysteem zijn voorzien van toegangsbeveiliging en wachtwoorden.

## 4 Beschrijving voorgenomen maatregelen

In onderdeel 4 wordt gezien welke maatregelen kunnen worden getroffen om de in onderdeel 3 erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

### A Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

De opgeslagen gegevens zijn als 'gewoon' gekwalificeerd, de genomen beveiligingsmaatregelen zijn afdoende om toegang tot en inbreuk op de integriteit van deze opgeslagen gegevens zo goed als uit te sluiten.

Gegevens worden beveiligd opgeslagen in een beveiligde ruimte. Betrokken personen bij cameratoezicht en verwerking zijn gescreend (antecedenten onderzoek en VOG) en hebben een geheimhouding- en integriteitsverklaring getekend.

Hier kunt u aanvullende punten toevoegen:

In het Privacyreglement Cameratoezicht IDC wordt beschreven hoe de Gemeente Den Haag omgaat met zowel vaste - als mobiele beveiligingscamera's.

Er is een convenant afgesloten tussen de gemeente Den Haag en de politie Den Haag. De politie meldkamer kan in specifieke gevallen gebruik maken van live beeldmateriaal welke de Centrale Meldkamer (CMK) van de gemeente beschikbaar heeft.

Voorwaarde is dat de gemeente (CMK) kan bepalen of de beelden worden doorgezonden (vrijwillige basis) en het beeldmateriaal niet door de politie wordt opgeslagen en bewaard.

BTW code (Meerdere items)

| Som van Saldo                                         | Kolomlabels |         |        |            |
|-------------------------------------------------------|-------------|---------|--------|------------|
| Rijlabels                                             | 2018        | 2019    | 2020   | Eindtotaal |
| <b>E000000 - SR: Algemene kostendrager FAD</b>        | 10.2.B      |         |        | 10.2.B     |
| 4050012810 Zepcam Docking station 4 Bay 256GB         | 10.2.B      |         |        | 10.2.B     |
| Diverse producten oktober 2018                        | 10.2.B      |         |        | 10.2.B     |
| Tilt stud for T2 mount + center chest harness for T2  | 10.2.B      |         |        | 10.2.B     |
| Zepcam T2 Bodycam                                     | 10.2.B      |         |        | 10.2.B     |
| <b>E662120 - Technische beveiliging - (B) -</b>       | 10.2.B      |         | 10.2.B | 10.2.B     |
| [ T2 replacement back and front cover                 |             |         | 10.2.B | 10.2.B     |
| Bodycams en oplader                                   |             | 10.2.B  |        | 10.2.B     |
| creditnota voor factuur SI-00002240                   |             | -10.2.B |        | -10.2.B    |
| reparatie Zepcam T2 Bodycam with full HD video, 32 GB |             | 10.2.B  |        | 10.2.B     |
| Zie creditnota SI-0002240-credit                      |             | 10.2.B  |        | 10.2.B     |
| <b>Eindtotaal</b>                                     | 10.2.B      | 10.2.B  | 10.2.B | 10.2.B     |

BTW tarief code (Meerdere items)

| Som van Saldo                                       | Kolomlabels |        |            |
|-----------------------------------------------------|-------------|--------|------------|
| Rijlabels                                           | 2021        | 2022   | Eindtotaal |
| <b>ZEPCAM B.V.</b>                                  | 10.2.B      | 10.2.B | 10.2.B     |
| <b>E581211 IDC Meerjaren onderhoudsplan - (B) -</b> | 10.2.B      |        | 10.2.B     |
| 4x bodycam                                          | 10.2.B      |        | 10.2.B     |
| 4x bodycam/docking station                          | 10.2.B      |        | 10.2.B     |
| Docking station 4 bay 256 GB /w power cable         | 10.2.B      |        | 10.2.B     |
| Overhaul dockingstation 4-bay                       | 10.2.B      |        | 10.2.B     |
| T2+ Bodycam with full HD video, 64 GB               | 10.2.B      |        | 10.2.B     |
| <b>E582120 IDC Technische beveiliging - (B) -</b>   |             | 10.2.B | 10.2.B     |

|                                |        |        |        |
|--------------------------------|--------|--------|--------|
| vervangen batterij / backcover |        | 10.2.B | 10.2.B |
| Eindtotaal                     | 10.2.B | 10.2.B | 10.2.B |

BTW tarief code (Alle)

Som van Saldo

Kolomlabels

Rijlabels

2021 2022 (leeg) Eindtotaal

|                                              |        |        |        |
|----------------------------------------------|--------|--------|--------|
| ZEPCAM B.V.                                  | 10.2.B | 10.2.B | 10.2.B |
| 0000000 Niet van toepassing                  | 10.2.B | 10.2.B | 10.2.B |
| 4x bodycam                                   | 10.2.B |        | 10.2.B |
| 4x bodycam/docking station                   | 10.2.B |        | 10.2.B |
| Docking station 4 bay 256 GB /w power cable  | 10.2.B |        | 10.2.B |
| Overhaul dockingstation 4-bay                | 10.2.B |        | 10.2.B |
| T2+ Bodycam with full HD video, 64 GB        | 10.2.B |        | 10.2.B |
| vervangen batterij / backcover               |        | 10.2.B | 10.2.B |
| E581211 IDC Meerjaren onderhoudsplan - (B) - | 10.2.B |        | 10.2.B |
| 4x bodycam                                   | 10.2.B |        | 10.2.B |
| 4x bodycam/docking station                   | 10.2.B |        | 10.2.B |
| Docking station 4 bay 256 GB /w power cable  | 10.2.B |        | 10.2.B |
| Overhaul dockingstation 4-bay                | 10.2.B |        | 10.2.B |
| T2+ Bodycam with full HD video, 64 GB        | 10.2.B |        | 10.2.B |
| E582120 IDC Technische beveiliging - (B) -   |        | 10.2.B | 10.2.B |
| vervangen batterij / backcover               |        | 10.2.B | 10.2.B |
| (leeg)                                       |        |        |        |
| (leeg)                                       |        |        |        |
| (leeg)                                       |        |        |        |
| Eindtotaal                                   | 10.2.B | 10.2.B | 10.2.B |