



# Protocol camerabewaking Intermaris

Dit protocol ziet toe op de camerabewaking bij complexen van Intermaris. Camerabewaking is een persoonsgegevensverwerking in de zin van de Algemene verordening gegevensverwerking (AVG).

Het protocol geeft een beschrijving van taken, verantwoordelijkheden en procedures over camerabewaking, met het oog op een integer gebruik van het camerasysteem en de bescherming van de privacy.

## 1. Begripsbepaling

- 1.1. Camerasysteem: Het geheel van camera's, monitoren, opnameapparatuur, verbindingssystemen, bekabeling, kabelgoten en bevestigingen.
- 1.2. Beeldinformatie: De door het camerasysteem verkregen en geregistreerde filmbeelden. Beeldinformatie is onderdeel van het begrip persoonsregistratie in de zin van de wet.
- 1.3. Beheer: Zorg voor de continuïteit van de camerabewaking.
- 1.4. Beheerder: De medewerker(s) die is/zijn belast met het beheer van het camerasysteem, het bedienen van het camerasysteem en het bekijken van de beelden.
- 1.5. Technisch beheer: De zorg voor het technisch functioneren van het camerasysteem en de opslagmedia. Dit bestaat uit het noodzakelijk periodiek onderhoud en het herstel van het systeem bij storing of schade.
- 1.6. Incident: een waargenomen strafbaar feit, ongeval of andere gebeurtenis die vraagt om op te treden.
- 1.7. Complex: een gebouw met woonruimten en/of bedrijfsruimten inclusief aangelegenheden zoals een terrein met parkeerplaatsen.

## 2. Doel van camerabewaking

Het doel van camerabewaking is om personen of zaken, in gebouwen of op terreinen waarvan Intermaris eigenaar is en/of verantwoordelijk voor het beheer, te beschermen en te beveiligen. Daarnaast is het doel om overlast te bestrijden. De nevensdoelen worden per complex vastgelegd in het register. Voorbeelden hiervan zijn:

- Voorkomen van (ernstige) vervuiling;
- Voorkomen van gevoelens van onveiligheid;
- Verminderen van schade aan gebouwen en installaties van Intermaris;
- Vervolgen van strafbare feiten.

De camerabeelden mogen niet voor een ander doel gebruikt worden. De grondslag voor de inzet van camerabewaking is voor de behartiging van het gerechtvaardigd belang van Intermaris.

### 3. Noodzakelijkheid van camerabewaking

- 3.1. Voor het plaatsen van het camerasysteem wordt door Intermaris vastgesteld of camerabewaking noodzakelijk en proportioneel is aan de hand van de volgende vragen:
  - Wat is het doel van de camerabewaking en is dit gebaseerd op concrete risico's?
  - Is het doel ook op een andere, minder verstrekkende wijze, te bereiken?
  - Hoe groot zijn de risico's voor bescherming van privacy van de personen die op de beelden te zien zullen zijn?
  - Staat de inbreuk op de privacy in verhouding tot het te beschermen belang?
- 3.2. Indien er een verhoogd risico is voor de bescherming van privacy van personen die op de beelden te zien zijn, maakt Intermaris gebruik van een Data Protection Impact Assessment (DPIA). Bij het toepassen van camerabewaking voert Intermaris een DPIA uit.
- 3.3. De wijze van camerabewaking (real-time meekijken op een monitor, app en/of mobile device en/of terugkijken) wordt getoetst aan het beoogde doel.

### 4. Voorwaarden voor camerabewaking

- 4.1. Camerabewaking wordt in ieder geval niet ingezet in woningen of gericht op de voordeur van woningen.
- 4.2. De openbare weg wordt alleen in beeld gebracht voor zover dit onvermijdelijk is.
- 4.3. Camerabewaking wordt niet ingezet met het doel bijzondere persoonsgegevens te registreren.
- 4.4. Intermaris maakt geen gebruik van heimelijke cameraregistratie (verborgen camera's), tenzij sprake is van een concrete en redelijke verdenking van diefstal of fraude in of rondom het complex.
- 4.5. Indien een leverancier bij de uitvoering van een opdracht van Intermaris gebruik maakt van camerabewaking, dan worden hierover afspraken gemaakt in de verwerkers-overeenkomst; dit cameraprotocol is dan onverkort van toepassing.

### 5. Taken en verantwoordelijkheden

- 5.1. Camerabewaking geschiedt onder verantwoordelijkheid van de directie van Intermaris, de houder van het camerasysteem.
- 5.2. De beheerders van het camerasysteem zijn door de directie van Intermaris aangewezen medewerkers of derden.
- 5.3. Het technische beheer van de camerabewaking geschiedt door de leverancier van de camera's. Dit gaat om de registratie en het veiligstellen van de beelden.
- 5.4. De beelden worden alleen bekeken door de beheerder als hiertoe aanleiding voor is, bijvoorbeeld in het geval van een incident.
- 5.5. De beheerder draagt er zorg voor dat er zorgvuldig met het beeldmateriaal wordt omgegaan wanneer dit in verband met een incident moet worden veiliggesteld.

- 5.6. In geval van een incident meldt de beheerder dit bij zijn leidinggevende en de geëigende instantie (politie, brandweer, spoedeisende medische hulpverlening (ambulance)).
- 5.7. Onderhoud van het camerasysteem en het verhelpen van storingen geschiedt door de technisch beheerder.
- 5.8. De technisch beheerder heeft toegang tot de camerabeelden om deze veilig te stellen.
- 5.9. Een overzicht van namen van de beheerders staan per complex opgenomen in het register.

## 6. Beveiliging van het camerasysteem

- 6.1. Het camerasysteem is tegen onbevoegd gebruik beveiligd door logische en fysieke toegangsbeveiligingsmaatregelen.
- 6.2. Het camerasysteem is beveiligd tegen toegang tot beelden door derden en onbedoeld verlies van beelden. Voor de back-up geldt dezelfde bewaartermijn als in het overzicht genoemd.
- 6.3. De opnameapparatuur van het camerasysteem staat opgesteld in een voor onbevoegden afgesloten ruimte. De ruimte is uitsluitend toegankelijk voor mensen die in het bezit zijn van een tag of sleutel van de ruimte en de sleutel van de kast.
- 6.4. Via een beveiligde verbinding zijn de camerabeelden die opgeslagen zijn op de opnameapparatuur op kantoor van Intermaris uit te lezen. De beelden zijn alleen in te zien door personen die een inlogcode hebben van de client PC.

## 7. Bediening van het camerasysteem

- 7.1. Onbevoegden hebben geen toegang tot het camerasysteem.
- 7.2. De technisch beheerder is bevoegd tot het bedienen van het camerasysteem c.q. het bekijken van de beelden om deze veilig te stellen.
- 7.3. Bevoegd tot slechts het raadplegen van de beelden zijn:
  - de beheerder;
  - politiefunctionarissen, voor de uitoefening van hun wettelijke taken;
  - officieren van justitie, voor opsporingsdoeleinden.
- 7.4. Onder het bedienen van de apparatuur wordt ook begrepen het terugkijken van de digitale opnamen en het vastleggen van beeldinformatie op een beveiligde informatiedrager of een andere beveiligde wijze van datatransport.

## 8. Integriteit, privacy en rechten van de geregistreeerde

- 8.1. De persoonsregistratie wordt uitsluitend gebruikt voor de doelstellingen van het camerabewaking.
- 8.2. De camerabewaking wordt kenbaar gemaakt door middel van bordjes en/of stickers bij de toegangsdeuren van het complex. De camera's worden zichtbaar opgehangen, er wordt geen gebruik gemaakt van verborgen camera's.

- 8.3. De beeldinformatie wordt maximaal 28 dagen bewaard waarna de informatie wordt gewist, tenzij zich een incident voordoet. De beelden worden dan opgeslagen en bewaard ten behoeve van de bewijslast, tot dat het incident is afgehandeld.
- 8.4. Onbevoegden hebben geen toegang tot het camerasysteem.
- 8.5. Het camerasysteem is elektronisch beveiligd tegen onbevoegd gebruik.
- 8.6. De onder 7.2 genoemde functionarissen gaan vertrouwelijk en integer om met de kennis die zij tot zich verkrijgen met de camerabewaking, in het bijzonder met betrekking tot de privacy van derden.
- 8.7. De (technisch) beheerder(s) hebben een akte van geheimhouding getekend.

## 9. Rechten van betrokkenen

- 9.1. Betrokkenen hebben het recht op inzage in de beelden waarop zij te zien zijn, voor zover mogelijk en daarmee de privacy van anderen niet geschaad wordt. De beheerder beslist binnen één week dat het verzoek ingewilligd kan worden of licht betrokkene in waarom dit niet mogelijk is. Betrokkenen hebben ook recht op de logboekgegevens over de beelden waarop zij te zien zijn.
- 9.2. Bij het inwilligen van het verzoek tot recht op inzage, moet rekening worden gehouden met derden die op de beelden te zien zijn.
- 9.3. Betrokkenen kunnen een verzoek tot verwijdering van de beelden indienen, of vanwege persoonlijke omstandigheden bezwaar maken tegen het maken of verder verwerken van camerabeelden. De beheerder beslist binnen één week dat het verzoek ingewilligd kan worden of licht betrokkene in waarom dit niet mogelijk is.

## 10. Uitgifte van beeldinformatie

- 10.1. Politiefunctionarissen en officieren van justitie die beroepshalve beelden uitkijken en/of het camerasysteem bedienen, legitimeren zich vooraf ten overstaan van de beheerder en bij diens afwezigheid bij de beheerder. Na ontvangst en beoordeling van een verzoek tot bekijken van beelden kunnen deze functionarissen daadwerkelijk beelden bekijken in het bijzijn van de beheerder.
- 10.2. Beeldinformatie wordt verstrekt op (schriftelijke) vordering van de politie of de officier van justitie.
- 10.3. De beeldinformatie wordt als bestand(en) op een beveiligde informatiedrager of andere beveiligde digitale wijze verstrekt.
- 10.4. De informatiedrager waarop beeldinformatie wordt opgeslagen wordt gemerkt en geregistreerd in het logboek door de beheerder.
- 10.5. De politiefunctionaris dan wel de officier van justitie tekent een inzageverklaring voor ontvangst en voor het zorgvuldig en integer gebruik van de beeldinformatie.
- 10.6. Bij afwezigheid van de beheerder maakt de politiefunctionaris of de officier van justitie een proces-verbaal van vordering van beeldinformatie en stuurt een afschrift daarvan naar de beheerder.

## 11. Inzagerecht beeldinformatie van derden

- 11.1. Het recht op inzage kan worden verleend als een zwaarwegend belang is aangetoond. Bij een aanvraag tot inzage van beelden dient de betrokkene het tijdstip en de tijdsduur van de beelden waarvan hij inzage verlangt aan te geven.
- 11.2. Een verzoek tot inzage van een advocaat, in het kader een strafproces ter verdediging van een verdachte cliënt, wordt gedaan door tussenkomst van de officier van justitie.
- 11.3. Niet-justitiële verzoeken tot inzage worden gericht aan de beheerder.
- 11.4. De verzoeker dient zich, ter vaststelling van zijn identiteit, in persoon te vervoegen bij de beheerder waarbij een geldig legitimatiebewijs ter inzage moet worden gegeven.
- 11.5. Beeldinformatie kan pas ter inzage worden gegeven na een afweging van belangen, waarbij het belang van de betrokkene bij inzage van de beeldinformatie is afgewogen tegen overige belangen, waaronder bijvoorbeeld het belang van derden die op de beeldinformatie voorkomen ter bescherming van hun privacy.
- 11.6. De beheerder beslist na weging van de belangen binnen één week op de aanvraag.
- 11.7. Personen die inzage in beeldinformatie krijgen tekenen een inzage verklaring.

## 12. Verslaglegging en rapportage

- 12.1. Van het gebruik van het camerasysteem wordt een logboek bijgehouden. Het logboek is vertrouwelijk.
- 12.2. In het logboek wordt vermeld: naam van de dienstdoende beheerder, datum, tijd en bijzonderheden, zoals: storingen, incidenten, meldingen, vordering van beeldinformatie, etc.
- 12.3. Het logboek wordt digitaal opgeslagen in een beveiligde omgeving.
- 12.4. Elk half jaar wordt door de beheerder (aan de hand van het logboek) gerapporteerd aan de specialist Leefbaarheid van Intermaris over de bijzonderheden.
- 12.5. De technisch beheerder meldt de technische bijzonderheden aan de beheerder.
- 12.6. De beheerder legt verantwoording af aan de specialist Leefbaarheid.
- 12.7. Bij ernstige incidenten wordt gerapporteerd aan de teamleider Bewoners en Leefbaarheid en de directeur Wonen & Vastgoed van Intermaris.

## 13. Klachten

Klachten over de toepassing van het camerasysteem, over het gedrag van de bij de camerabewaking betrokken functionarissen, met uitzondering van politie- en justitiefunctionarissen, of klachten over het weigeren van inzage van beeldinformatie, dienen schriftelijk binnen zes weken te worden ingediend bij de directie van Intermaris.

De behandeling van deze klacht geschiedt volgens de klachtenregeling van Intermaris.