Stichting PrimAH

Procedure & reglement Cameratoezicht

Inhoud

1 Inleiding

Cameratoezicht, ook wel bekend onder het Engelse begrip CCTV, wordt in verschillende situaties gebruikt. Bijvoorbeeld om personen en eigendommen te beschermen. Gemeentes gebruiken cameratoezicht o.a. in het kader van veiligheid op straat. Het is hierbij van belang dat organisaties zorgvuldig met camerabeelden omgaan. Ook onderwijsinstellingen maken in bepaalde gevallen gebruik van cameratoezicht.

Cameratoezicht mag geen doel op zichzelf zijn. Bij Stichting PrimAH is het uitgangspunt dat we geen cameratoezicht hanteren, tenzij noodzakelijk. Bij cameratoezicht is de inbreuk op de privacy van leerlingen, medewerkers en bezoekers groot. Daarom mogen po -instellingen alleen camera's ophangen als zij aan een aantal voorwaarden voldoen. Ook moeten zij ervoor zorgen dat de inbreuk op de privacy zo klein mogelijk is. Een camera in bijvoorbeeld een toilet gaat te ver, omdat mensen dan ontkleed in beeld kunnen komen.

Dit document regelt het gebruik van camera's, en waarborgt de privacy van leerlingen, medewerkers en bezoekers. Het bijgesloten reglement cameratoezicht heeft betrekking op die locaties van Stichting PrimAH, waar toezicht door middel van camerasystemen wordt ingezet. Het geeft een beschrijving van taken, verantwoordelijkheden en procedures over het cameratoezicht, met het oog op integer gebruik van het camerasysteem en de bescherming van privacy van leerlingen, medewerkers en bezoekers.

2 Randvoorwaarden cameratoezicht

2.1. Verantwoordelijkheid

Het zorgvuldig omgaan met gegevens is (wettelijk) de verantwoordelijkheid van po-instellingen (verder te noemen 'onderwijsinstellingen') zelf. De Algemene Verordening Gegevensbescherming (AVG) wijst het bevoegd gezag aan als verwerkingsverantwoordelijke om de privacy van leerlingen, medewerkers en bezoekers te regelen. Een instelling kan deze verantwoordelijkheid niet afwentelen op bijvoorbeeld haar leveranciers (die in het kader van de privacywetgeving in de AVG verwerkers worden genoemd).

De persoon op wie de persoonsgegevens betrekking hebben, noemen we betrokkene: dat kunnen leerlingen zijn, maar ook medewerkers (leerkrachten, administratief personeel) of zelfs bezoekers. Indien de betrokkene de leeftijd van 16 jaar nog niet bereikt heeft, wordt de betrokkene vertegenwoordigd door zijn wettelijk vertegenwoordiger. Meestal zal dit een ouder zijn, maar een voogd kan ook.

Als een onderwijsinstelling cameratoezicht wil inzetten, dan ligt de eindverantwoordelijkheid daarvoor bij het bevoegd gezag. Die stelt, met instemming van de GMR, een reglement vast met randvoorwaarden en waarborgen waar het toezicht aan moet voldoen. Het bevoegd gezag kan een deel van haar beslissingsbevoegdheid overdragen aan één of meerdere personen in de organisatie om praktisch uitvoering te geven aan het cameratoezicht. Deze persoon legt verantwoording af aan het bevoegd gezag.

2.2. Randvoorwaarden

De wetgever geeft een onderwijsinstelling een aantal randvoorwaarden mee waar cameratoezicht aan moet voldoen. De toezichthouder in Nederland op het gebruik van persoonsgegevens, de Autoriteit Persoonsgegevens, heeft dit uitgewerkt in de Beleidsregels cameratoezicht van 28 januari 2016.

2.2.1. Gerechtvaardigd belang

De onderwijsinstelling moet een zogeheten gerechtvaardigd belang hebben voor het cameratoezicht. Bijvoorbeeld diefstal tegengaan of leerlingen, medewerkers en bezoekers beschermen.

2.2.2. Doel en doelbinding

Het inzetten van cameratoezicht, en het gebruik van de (opgenomen) beelden, is alleen toegestaan voor een beperkt aantal vooraf vastgestelde doelen. Voor het onderwijs zijn dit:

a. de bescherming van de veiligheid en gezondheid van leerlingen, medewerkers en bezoekers;
b. de beveiliging van de toegang tot gebouwen en terreinen;
c. de bewaking van zaken die zich in gebouwen of op terreinen bevinden;
d. het vastleggen van incidenten.

Het gebruik van de camerabeelden voor bijvoorbeeld interne trainingen of educatieve doeleinden, is dus niet toegestaan. Onder deze doelen valt niet het gebruik van camerabeelden voor absentie- of aanwezigheidscontrole of als personeelsvolgsysteem.

2.2.3. Noodzaak cameratoezicht

Het cameratoezicht moet noodzakelijk zijn. Dat wil zeggen dat de onderwijsinstelling het doel niet op een andere manier kan bereiken. De onderwijsinstelling moet eerst nagaan of er geen andere mogelijkheid is, die minder ingrijpend is voor de privacy van betrokkenen. Ook mag het cameratoezicht niet op zichzelf staan. Het moet onderdeel zijn van een totaalpakket aan maatregelen in het kader van beveiliging en sociale veiligheid.

2.2.4. Privacytoets

De onderwijsinstelling moet eerst een privacytoets uitvoeren alvorens er besloten wordt tot het inrichten en gebruiken van cameratoezicht. Betrek bij deze toets de manager Informatiebeveiliging en Privacy (MIBP) en Functionaris gegevensbescherming (FG). Bij deze toets weegt de onderwijsinstelling de belangen van de leerlingen, medewerkers en bezoekers af tegen de wens om cameratoezicht te gebruiken. Daarbij kan meewegen of camerabeelden alleen ‘live’ worden meegekeken, of dat er ook beelden worden opgenomen (wat doorgaans als een grotere inbreuk op de privacy wordt gezien). Ook de gebruikte cameratechniek kan relevant zijn: de ene camera- of softwaretechniek kan ingrijpender zijn dan de andere. Ook het maken van opnames met of zonder geluid is belangrijk. De onderwijsinstelling moet kunnen uitleggen waarom het toepassen van cameratoezicht belangrijker is dan de mogelijke inbreuk op de privacy van de betrokkenen. In het kader van de transparantie en verantwoordingsplicht van het bevoegd gezag, is het raadzaam om de uitkomsten van de privacy toets schriftelijk vast te leggen.

2.2.5. Informatieplicht cameratoezicht

De onderwijsinstelling moet ervoor zorgen dat de leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers, en bezoekers weten dat er een camera hangt. Bijvoorbeeld door bordjes (bij de ingang) op te hangen, het reglement cameratoezicht publiek beschikbaar te stellen en op bijvoorbeeld de website beknopt uit te leggen dat er gebruik wordt gemaakt van cameratoezicht en waarom.

2.2.6. Bewaartermijn camerabeelden

De onderwijsinstelling mag de camerabeelden niet langer bewaren dan noodzakelijk is. De richtlijn van de Autoriteit Persoonsgegevens is hiervoor maximaal 4 weken. Voor een geconstateerd incident, zoals diefstal, fraude of mishandeling, mag de school alleen de betreffende beelden van het incident langer bewaren, namelijk totdat dit incident is afgehandeld.

2.2.7. Heimelijk cameratoezicht

Het gebruik van verborgen camera’s, zonder daarover de betrokken personen te informeren, is normaal gesproken niet toegestaan. Alleen in geval een onderwijsinstelling duidelijke en concrete vermoedens van bijvoorbeeld diefstal of fraude door leerlingen, medewerkers of anderen heeft, mag er onder strikte voorwaarden gebruik worden gemaakt van heimelijk cameratoezicht. Belangrijk is dat in het reglement cameratoezicht de leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers, en bezoekers vooraf erop gewezen zijn dat verborgen camera’s in bepaalde

situaties (bijvoorbeeld diefstal of fraude) mogelijk zijn. Het heimelijk cameratoezicht moet zelf ook beperkt zijn: bij overlast in de avonduren is het overdag toepassen daarvan niet proportioneel, evenmin is het filmen van een gehele gang niet noodzakelijk indien er zich alleen bij één specifieke deur incidenten voordoen.

2.2.8. Meldingsplicht cameratoezicht

Het toepassen van cameratoezicht hoeft – in beginsel - niet te worden gemeld bij de Autoriteit Persoonsgegevens (of functionaris voor gegevensbescherming indien deze binnen de onderwijsinstelling is aangesteld). Er moet dan wel voldaan zijn aan de hiervoor genoemde randvoorwaarden, en het gaat om duidelijk zichtbare camera's. De vrijstelling geldt dus niet voor heimelijk cameratoezicht: dat moet wél worden gemeld.

2.2.9. Beveiliging

De toegang en gebruik van camera's en opgenomen camerabeelden moet adequaat beveiligd zijn. Denk hierbij ook aan het instellen van de juiste autorisaties: niet iedereen hoeft toegang te hebben tot alle beelden. Ook de apparatuur waarop de beelden worden opgenomen of opgeslagen, moet zijn beveiligd door bijvoorbeeld de recorders in een afgesloten kast te plaatsen. Houd ook rekening met technisch of functioneel beheer, en het verkrijgen van fysieke toegang tot de opgenomen beelden (toegang serverruimte bijvoorbeeld).

2.2.10. Rechten betrokkenen

De leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers hebben een aantal rechten. Deze worden geregeld in het reglement cameratoezicht. Belangrijk is om te beseffen dat de leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers het recht hebben op inzage in 'hun' camerabeelden. Dit verzoek mag niet worden geweigerd om administratieve lasten van de onderwijsinstelling te beperken. Wél mag een dergelijk inzageverzoek worden afgewezen wanneer het verzoek tot inzage in camerabeelden ongespecificeerd is of als het inzagerecht kennelijk misbruikt wordt. Hiernaast mag een inzageverzoek worden geweigerd als het noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten.

2.2.11. Inzage door en verstrekking aan derden

De (opgenomen) camerabeelden worden alleen intern gebruikt indien dat past binnen de vastgestelde doeleinden voor cameratoezicht. Derden krijgen alleen inzage in de camerabeelden met uitdrukkelijke toestemming van de betrokkene en/of diens wettelijk vertegenwoordiger. Een andere grond is als inzage of verstrekking van de beelden noodzakelijk is op grond een wettelijke verplichting of voor de goede vervulling van de (publiekrechtelijke) taak van politie en justitie in het geval van incidenten.

2.3. Rol van de MR

Bij cameratoezicht gaat het over de privacy van leerlingen, medewerkers en bezoekers. Bij het vaststellen, wijzigen of intrekken van het privacy beleid, waar deze procedure en regelement onderdeel van zijn, wordt de GMR om instemming gevraagd. Het gaat immers om een regeling omtrent het verwerken van alsmede de bescherming van de persoonsgegevens .

3. Reglement cameratoezicht

Reglement cameratoezicht Stichting PrimAH

Dit reglement cameratoezicht heeft betrekking op alle scholen van Stichting PrimAH waar toezicht door middel van camerasystemen wordt ingezet. Het geeft een beschrijving van taken, verantwoordelijkheden en procedures over het cameratoezicht, met het oog op integer gebruik van het camerasysteem en de bescherming van privacy van leerlingen, medewerkers en bezoekers.

Artikel 1 – Begripsbepalingen

1. In dit reglement wordt verstaan onder:

a. Cameratoezicht: toezicht met behulp van camera's, waardoor er sprake is van verwerking van persoonsgegevens als bedoeld in de Algemene Verordening Gegevensbescherming.
b. Heimelijk cameratoezicht: toezicht met behulp van verborgen en/of niet-zichtbare camera's, of cameratoezicht dat niet kenbaar is gemaakt aan leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers.
c. Serverruimte: de van een toegangscontrolesysteem voorziene ruimte, waar de server of opnameapparatuur staat waarop de opgenomen camerabeelden geregistreerd staan.
d. Camerasysteem: het geheel van camera's, monitoren, opnameapparatuur, verbindingskasten, verbindingen en bevestigingen waarmee het cameratoezicht wordt uitgevoerd.
e. Camera observatieruimte: een centraal gesitueerde, van een toegangscontrolesysteem voorziene ruimte, waarin de camerabeelden - van alle locaties - centraal live worden bekeken en/of waar ook de mogelijkheid bestaat om opgenomen camerabeelden terug te kijken en/of op een informatiedrager te plaatsen.
f. Camerabeeld: het door het cameratoezicht verkregen camerabeeld.
g. Beheerder cameratoezicht: de door het bevoegd gezag aangewezen medewerker van de school/stichting, die verantwoordelijk is voor de inrichting, het beheer en toezicht op het cameratoezicht.
h. Bevoegde medewerker: een door de beheerder cameratoezicht als zodanig aangewezen persoon die betrokken is bij de uitvoering van het cameratoezicht.
i. Incident: een waargenomen ongewenst en/of strafbaar feit, ongeval of andere gebeurtenis die vraagt om handhaving, onderzoek en/of strafrechtelijke vervolging.

Artikel 2 –Werkingssfeer en doelstellingen cameratoezicht

1. Dit reglement is van toepassing op leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers die zich bevinden in de gebouwen of op de terreinen van Stichting PrimAH.

2. Het inzetten van cameratoezicht, en het gebruik van de camerabeelden, is alleen toegestaan voor:

a. de bescherming van de veiligheid en gezondheid van leerlingen, medewerkers en bezoekers;
b. de beveiliging van de toegang tot gebouwen en terreinen, waaronder mede is begrepen het weren van ongewenste bezoekers;
c. de bewaking van zaken die zich in gebouwen of op terreinen bevinden;
d. het vastleggen van incidenten.

3. Camerabeelden worden uitsluitend gebruikt ten behoeve van de doelstelling zoals genoemd in lid 2.

Artikel 3 – Taken en verantwoordelijkheden

1. Het cameratoezicht geschiedt onder verantwoordelijkheid van het bevoegd gezag.

2. Alvorens te besluiten tot het instellen of intensiveren van cameratoezicht, voert de manager Informatiebeveiliging (MIBP) namens het bevoegd gezag een privacy toets uit, waarbij de mate van inbreuk op de privacy van de leerlingen, medewerkers en bezoekers wordt afgewogen tegen het belang van de onderwijsinstelling om cameratoezicht te gebruiken. Hierbij wordt meegewogen of de doelstellingen als geformuleerd in artikel 2, op een andere wijze kunnen worden bereikt, met een minder ingrijpend middel dan cameratoezicht.

3. Het bevoegd gezag wijst een beheerder cameratoezicht aan die verantwoordelijk is voor de inrichting, het beheer en toezicht op het cameratoezicht binnen de onderwijsinstelling.

4. De beheerder cameratoezicht wijst bevoegde medewerkers aan.

5. De beheerder cameratoezicht wijst voor zichzelf een plaatsvervanger aan, die in geval van afwezigheid van de beheerder cameratoezicht in diens taken en verantwoordelijkheden treedt.

6. De beheerder cameratoezicht en bevoegde medewerkers zijn bevoegd tot het live uitkijken van camerabeelden.

7. De beheerder cameratoezicht is bevoegd tot het terugkijken en uitgeven van opgenomen camerabeelden.

8. De beheerder cameratoezicht kan een bevoegde medewerker autoriseren om - onder verantwoordelijkheid van de beheerder cameratoezicht - onder nader te stellen voorwaarden en voor een vooraf bepaald doel cq. een vooraf bepaalde periode camerabeelden terug te kijken.

Artikel 4 – Inrichten camerasysteem en beveiliging

1. De beheerder cameratoezicht is verantwoordelijk voor de inrichting van het camerasysteem en de plaatsing van de camera's, binnen de kaders van de door het bevoegd gezag uitgevoerde privacy toets als bedoeld in artikel 3 lid 2.

2. De beheerder cameratoezicht zorgt voor passende technische en organisatorische maatregelen om de camerabeelden te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau (gelet op de risico's van het cameratoezicht en de aard van te beschermen camerabeelden). De maatregelen betreffen het camerasysteem, de serverruimte en camera observatieruimte.

3. Het terugkijken van opgenomen camerabeelden geschiedt slechts in aanwezigheid van daartoe bevoegd verklaarde personen.

4. De met cameratoezicht belaste medewerkers gaan vertrouwelijk en integer om met de kennis die zij tot zich krijgen vanwege het cameratoezicht, in het bijzonder met betrekking tot de privacy van leerlingen, medewerkers en bezoekers. Voor zover daar arbeidsrechtelijk niet in is voorzien, sluit de beheerder cameratoezicht daartoe een geheimhoudingsverklaring met de bevoegde medewerker(s).

5. De beheerder cameratoezicht draagt er zorg voor dat het cameratoezicht kenbaar wordt gemaakt aan leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers op zichtbare en

herkenbare wijze, maar niet beperkt tot borden en stickers bij de ingang van de gebouwen of terreinen van de onderwijsinstelling.

6. Voor zover er in het camerasysteem camerabeelden worden opgeslagen, worden deze beelden na uiterlijk vier weken na de opname automatisch gewist, tenzij er een incident is geconstateerd op basis waarvan het noodzakelijk is de met het incident samenhangende camerabeelden te bewaren. Na afhandeling van het incident worden de betreffende camerabeelden (en eventueel gemaakte kopieën of afdrukken) gewist.

7. Voor zover er live camerabeelden worden uitgekeken in een andere ruimte dan de serverruimte of camera observatieruimte, zijn er technische en organisatorische maatregelen genomen die het onbevoegd meekijken zoveel als redelijkerwijs mogelijk voorkomen.

8. Voor zover er bij het inrichten van het camerasysteem voor gekozen wordt om de leerlingen, medewerkers en bezoekers via een monitor live terugkoppeling te geven van de camerabeelden, kunnen deze live camerabeelden alleen betrekking hebben op deze betreffende leerlingen, medewerkers en bezoekers.

9. Bewerking van camerabeelden vindt slechts plaats in het kader van het verscherpen van deze camerabeelden.

Artikel 5 – Inzage en uitgifte opgenomen camerabeelden aan derden

1. Op verzoek van politie, rechter-commissaris of (hulp)officier van justitie kan inzage worden gegeven in (opgenomen) camerabeelden in het kader van de uitoefening van diens publiekrechtelijke taak.

2. Uitgifte van camerabeelden vindt slechts plaats op vordering van de politie, rechter-commissaris of (hulp)officier van justitie waarbij de vordering gebaseerd is op een wettelijke grondslag.

3. Alvorens tot inzage of uitgifte over te gaan, legitimeert de betreffende functionaris zich vooraf ten overstaan van de beheerder cameratoezicht en tekent voor ontvangst van de uitgegeven camerabeelden.

4. De inzage en uitgifte wordt door de beheerder cameratoezicht geregistreerd.

5. Aan andere derden wordt geen inzage in de camerabeelden gegeven, of camerabeelden uitgegeven, anders dan met de uitdrukkelijke toestemming van de betrokken leerling en/of hun wettelijk vertegenwoordiger, medewerker of bezoeker.

Artikel 6 – Rechten van betrokkenen

1. Betrokken leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers komen de rechten toe zoals bedoeld in de Algemene Verordening Gegevensbescherming. Hieronder vallen het recht op inzage, correctie en verwijdering van camerabeelden waarop zij zijn afgebeeld.

2. Een verzoek tot inzage in camerabeelden geschiedt schriftelijk of per e-mail aan de beheerder cameratoezicht, die binnen 10 werkdagen na ontvangst van het verzoek inhoudelijk zal reageren.

3. Het verzoek tot inzage wordt afgewezen wanneer het verzoek tot inzage in camerabeelden ongespecificeerd is, of als met dit verzoek kennelijk misbruikt van recht wordt gemaakt.

4. In geval van een incident, kan een inzageverzoek worden geweigerd als dat noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten.

Artikel 7– Heimelijk cameratoezicht

1. Heimelijk cameratoezicht is slechts toegestaan indien regulier cameratoezicht en andere door de onderwijsinstelling genomen maatregelen en inspanningen, niet leiden tot beëindiging van de structurele incidenten. Het inzetten van heimelijk cameratoezicht is niet mogelijk voor preventieve doeleinden.

2. Voornoemd heimelijk cameratoezicht mag alleen tijdelijk en op zodanige wijze worden ingezet, dat inbreuk op de persoonlijke levenssfeer van de leerlingen, medewerkers en bezoekers zo klein mogelijk is.

3. Heimelijk cameratoezicht is uitsluitend toegestaan na specifieke voorafgaande schriftelijke toestemming van het bevoegd gezag onder vermelding van de voorwaarden waaronder het heimelijk cameratoezicht plaatsvindt.

4. De onderwijsinstelling informeert - voor zover redelijkerwijs mogelijk - achteraf de betrokken leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers over het toegepaste heimelijk cameratoezicht.

5. Voordat heimelijk cameratoezicht wordt toegepast, meldt het bevoegd gezag haar voornemen bij de Autoriteit Persoonsgegevens. Er wordt niet eerder aangevangen met heimelijk toezicht dan na instemming daarmee van de Autoriteit Persoonsgegevens.

Artikel 8 – Verslaglegging en rapportage

1. De beheerder cameratoezicht rapporteert tenminste jaarlijks aan het bevoegd gezag over het toegepaste cameratoezicht, waaronder begrepen is een verslag over de verstrekkingen van camerabeelden zoals bedoeld in artikel 5.

2. Jaarlijks wordt door het bevoegd gezag gerapporteerd aan de GMR over het cameratoezicht betreffende het voorafgaande jaar (over aard, frequentie en lengte van het toezicht). Daarbij wordt specifiek gemeld indien heimelijk cameratoezicht is toegepast.

Artikel 9 – Slotbepaling

1. Het bevoegd gezag stelt dit reglement vast.

2. Het reglement treedt onmiddellijk in werking. Een wijziging in dit reglement treedt in werking binnen 30 dagen na bekendmaking van de wijziging.