Reglement cameratoezicht mboRijnland

Voorgenomen besluit Raad van Bestuur	15 mei 2018
Instemming ondernemingsraad	10 januari 2019
Instemming studentenraad	28 mei 2019
Definitief besluit College van Bestuur	18 juni 2019

Auteur(s):
Informatiemanagement

Dit stuk is gebaseerd op het model reglement videocameratoezicht van de Facilitair Samenwerkingsverband Roc's, aoc's en vakscholen

Versie:
2.0, december 2018

Reglement cameratoezicht mboRijnland

Dit reglement cameratoezicht heeft betrekking op alle locaties van mboRijnland 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 studenten, 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 Wet bescherming persoonsgegevens en 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 studenten, medewerkers en bezoekers.
   c. Camerasysteem: het geheel van camera's, monitoren, opnameapparatuur, verbindingskasten en verbindingen waarmee het cameratoezicht wordt uitgevoerd.
   d. Serverruimte: afgesloten ruimte waar de opnameapparatuur staat waarop de opgenomen camerabeelden geregistreerd staan.
   e. Camera-observatieruimte: afgesloten ruimte waarin de mogelijkheid bestaat om opgenomen camerabeelden terug te kijken en/of op een informatiedrager te plaatsen.
   f. Camerabeeld: de door het cameratoezicht verkregen camerabeeld.
   g. Incident: een waargenomen ongewenst en/of strafbaar feit, ongeval of andere gebeurtenis die vraagt om handhaving, onderzoek en/of strafrechtelijke vervolging.
   h. Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Artikel 2 –Werkingssfeer en doelstellingen cameratoezicht

1. Dit reglement is van toepassing op studenten, medewerkers en bezoekers die zich bevinden in de gebouwen of op de terreinen van mboRijnland.
2. Het inzetten van cameratoezicht, en het gebruik van de camerabeelden, is alleen toegestaan voor:
   a. de bescherming van de veiligheid en gezondheid van studenten, medewerkers en bezoekers;
   b. de beveiliging van de toegang tot gebouwen en terreinen, waaronder mede is begrepen het weren van onbevoegde of onbevoegd verklaarde personen;
   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 College van bestuur.
2. Alvorens te besluiten tot het instellen of intensiveren van cameratoezicht, voert het College van Bestuur een privacytoets uit, waarbij de mate van inbreuk op de privacy van de studenten, medewerkers en bezoekers wordt afgewogen tegen het belang van de instelling om cameratoezicht te gebruiken. Hierbij wordt meegewogen of de doelstellingen als geformuleerd in artikel 2 tweede lid, op een andere wijze kunnen worden bereikt, met een minder ingrijpend middel dan cameratoezicht.
3. Het College van Bestuur wijst de directeur Shared Service Center Facilitaire Dienstverlening & ICT als verantwoordelijke aan voor de inrichting, het beheer en toezicht op het cameratoezicht.
4. De directeur Shared Service Center Facilitaire Dienstverlening & ICT is bevoegd tot het live uitkijken van camerabeelden. De volgende personen zijn hiertoe eveneens bevoegd:
   a. de locatiebeheerder (teamleider Facilitaire Dienstverlening);
   b. de locatieverantwoordelijke directeur, voor zover het camerabeelden betreffen van het gebouw c.q. het terrein waarvan hij directeur is;
   c. de veiligheidscoördinator;
   d. beveiligingsmedewerkers;
   e. andere medewerkers van mboRijnland voor zover zij daartoe (incidenteel) zijn geautoriseerd. Autorisatie kan slechts worden verleend door het College van Bestuur of de directeur Shared Service Center Facilitaire Dienstverlening & ICT .
7. De bevoegde medewerkers (zoals genoemd in het vorige lid) zijn ook bevoegd tot het terugkijken van opgenomen camerabeelden.
8. Het terugkijken van opgenomen camerabeelden geschiedt door ten minste twee bevoegde medewerkers.
9. De met cameratoezicht belaste medewerkers gaan vertrouwelijk en integer om met de kennis die zij tot zich nemen vanwege het cameratoezicht, in het bijzonder met betrekking tot de privacy van studenten, medewerkers en bezoekers.
10. In geval het College van Bestuur een verwerker in de zin van de Algemene verordening gegevensbescherming inschakelt, geeft deze de verwerker de opdracht om te handelen conform dit reglement.

Artikel 4 – Inrichten camerasysteem en beveiliging

1. De directeur Shared Service Center Facilitaire Dienstverlening & ICT is verantwoordelijk voor de inrichting van het camerasysteem en de plaatsing van de camera's, binnen de kaders van de door het College van Bestuur uitgevoerde privacytoets als bedoeld in artikel 3 lid 2.

2. De directeur Shared Service Center Facilitaire Dienstverlening & ICT 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 (zoals te doen gebruikelijk in de informatiebeveiligings- en beveiligingsbranche) en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's van het cameratoezicht en de aard van te beschermen camerabeelden met zich meebrengen. De maatregelen betreffen het camerasysteem en de serverruimte en camera-observatieruimte.
3. De directeur Shared Service Center Facilitaire Dienstverlening & ICT draagt er zorg voor dat het cameratoezicht kenbaar wordt gemaakt aan studenten, medewerkers en bezoekers op zichtbare en herkenbare wijze, zoals borden en stickers bij de ingang van de gebouwen of terreinen.
4. Voor zover er in het camerasysteem camerabeelden worden opgeslagen, worden deze beelden 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.
5. Het camerasysteem is zodanig uitgerust dat het terugkijken van opgenomen camerabeelden of het uitgeven daarvan slechts mogelijk is in de camera-observatieruimte.
6. 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 directeur Shared Service Center Facilitaire Dienstverlening & ICT of de locatiebeheerder, en tekent voor ontvangst van de uitgegeven camerabeelden.
4. Inzage of uitgifte geschiedt slechts na akkoord van de directeur Shared Service Center Facilitaire Dienstverlening & ICT of het College van Bestuur.
5. De beeldinformatie wordt op DVD/USB of ander digitaal medium verstrekt.
6. Van de inzage en uitgifte wordt door de bedrijfsbeveiliging melding gemaakt in een daarvoor aangewezen registratiesysteem en bij de veiligheidscoördinator. De veiligheidscoördinator draagt zorg voor de melding in het incidentregistratiesysteem.
7. Aan andere derden wordt geen inzage in de camerabeelden gegeven, of camerabeelden uitgegeven, anders dan met de uitdrukkelijke toestemming van de betrokken studenten, medewerkers of bezoekers.

Artikel 6 – Rechten van betrokkenen

1. Betrokken studenten, 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 directeur Shared Service Center Facilitaire Dienstverlening & ICT, 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, de identiteit van de verzoeker niet vastgesteld kan worden, of als met dit verzoek kennelijk misbruik van recht wordt gemaakt.
4. In geval van een incident, kan een inzageverzoek worden geweigerd als dat noodzakelijk is in het belang van de (verdere) voorkoming, opsporing en vervolging van strafbare feiten.
5. Voor klachten over de toepassing van het camerasysteem, dit reglement en over het gedrag van de directeur Shared Service Center Facilitaire Dienstverlening & ICT , locatiebeheerder of de bevoegde medewerkers, wordt de reguliere klachtenprocedure gevolgd zoals die door het College van Bestuur is vastgesteld.

Artikel 7– Heimelijk cameratoezicht

1. Heimelijk cameratoezicht is slechts toegestaan indien regulier cameratoezicht en andere door mboRijnland genomen maatregelen en inspanningen, niet hebben geleid tot beëindiging van de structurele incidenten. Het inzetten van heimelijk cameratoezicht is niet toegestaan voor preventieve doeleinden.
2. Voornoemd heimelijk cameratoezicht mag alleen tijdelijk en op zodanige wijze worden ingezet, dat sprake is van een minimale inbreuk op de persoonlijke levenssfeer van de studenten, medewerkers en bezoekers.
3. Heimelijk cameratoezicht is uitsluitend toegestaan na specifieke voorafgaande schriftelijke toestemming van het College van Bestuur en onder vermelding van de voorwaarden waaronder het heimelijk cameratoezicht plaatsvindt.
4. MboRijnland informeert – voor zover redelijkerwijs mogelijk - achteraf de betrokken studenten, medewerkers en bezoekers over het toegepaste heimelijk cameratoezicht.
5. Voordat heimelijk cameratoezicht wordt toegepast, meldt het College van Bestuur 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 directeur Shared Service Center Facilitaire Dienstverlening & ICT rapporteert tenminste jaarlijks aan het College van Bestuur over het toegepaste cameratoezicht, waaronder begrepen is een verslag over de verstrekkingen van camerabeelden zoals bedoeld in artikel 5.
2. Jaarlijks wordt door het College van Bestuur gerapporteerd aan de Ondernemingsraad over het cameratoezicht betreffende het voorafgaande jaar.

Artikel 9 – Slotbepalingen

1. Het College van Bestuur stelt dit reglement vast. Voorafgaand aan het vaststellen, wijzigen of intrekken van dit reglement cameratoezicht, vraagt het College van Bestuur de ondernemingsraad en de studentenraad om instemming.
2. Het reglement treedt onmiddellijk in werking. Een wijziging in dit reglement treedt in werking binnen 30 dagen na bekendmaking van de wijziging.

Toelichting

Verantwoordelijkheid

Het zorgvuldig omgaan met gegevens is (wettelijk) de verantwoordelijkheid van mboRijnland. De Algemene verordening gegevensbescherming wijst het bevoegd gezag, concreet het College van Bestuur, aan als verantwoordelijke om de privacy van medewerkers, studenten en bezoekers te regelen. mboRijnland kan deze verantwoordelijkheid niet afwentelen op bijvoorbeeld haar leveranciers (die in het kader van de privacywetgeving ook wel verwerkers worden genoemd).
De persoon op wie de persoonsgegevens betrekking hebben, noemen we betrokkene: dat kan een student zijn, maar ook medewerker (docenten, administratief personeel) of zelfs bezoekers.

Wanneer mboRijnland een extern beveiligingsbedrijf inhuurt, dan is dat bedrijf vaak een verwerker in de zin van de Algemene verordening gegevensbescherming. Dat betekent onder meer dat mboRijnland aparte afspraken maakt over de toegang tot en gebruik van het camerasysteem en de camerabeelden in een verwerkersovereenkomst. Het beveiligingsbedrijf moet zich houden aan de instructies van mboRijnland en dus ook aan het reglement cameratoezicht van de instelling.

Als mboRijnland cameratoezicht wil inzetten, dan ligt de eindverantwoordelijkheid daarvoor bij het College van Bestuur. Die stelt, met instemming van de ondernemingsraad, een reglement vast met randvoorwaarden en waarborgen waar het toezicht aan moet voldoen. Het College van Bestuur 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 College van Bestuur.

Randvoorwaarden

De wetgever geeft een mbo-instelling 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[1].

Gerechtvaardigd belang

Het mbo-college moet een zogeheten gerechtvaardigd belang hebben voor het cameratoezicht. Bijvoorbeeld diefstal tegengaan of de sociale en fysieke veiligheid van studenten, medewerkers en bezoekers beschermen.

Noodzaak cameratoezicht

Het cameratoezicht moet noodzakelijk zijn. Dat wil zeggen dat het mbo-college het doel niet op een andere manier kan bereiken. Het mbo-college moet eerst nagaan of er geen andere mogelijkheid, 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. De noodzaak bestaat uit het bestrijden van criminaliteit en het bevorderen van de (gevoel)veiligheid.

[1] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_cameratoezicht-.pdf

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 studenten, 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.

Privacytoets

mboRijnland voert vanaf de datum van inwerkingtreding van dit reglement een privacytoets uit over veranderingen in het cameratoezicht. Bij deze toets wordt de afweging gemaakt tussen de privacybelangen van de studenten, medewerkers en bezoekers en de wens om cameratoezicht te gebruiken.

Informatieplicht cameratoezicht

De studenten, medewerkers en bezoekers worden geïnformeerd dat er camera's hangen. Bij de ingang worden bordjes opgehangen, het reglement cameratoezicht is voor publiek beschikbaar gesteld en op bijvoorbeeld de website of in de studiegids wordt beknopt uitgelegd dat er gebruik wordt gemaakt van cameratoezicht.

Bewaartermijn camerabeelden

De camerabeelden mogen niet langer dan noodzakelijk is bewaard worden. De richtlijn van de Autoriteit Persoonsgegevens is gesteld op maximaal 4 weken. Voor een geconstateerd incident (diefstal, fraude of mishandeling, etc.) mag het mbo-college de incident betreffende beelden bewaren tot het incident is afgehandeld, waarna die beelden moeten worden vernietigd.

Heimelijk cameratoezicht

Het gebruik van verborgen camera's, zonder daarover de betrokken personen te informeren, is normaal gesproken niet toegestaan. Alleen in geval van duidelijke en concrete vermoedens van bijvoorbeeld diefstal of fraude door studenten of medewerkers mag er onder strikte voorwaarden gebruik worden gemaakt van heimelijk cameratoezicht. Belangrijk is dat in het reglement cameratoezicht de studenten, medewerkers en bezoekers vooraf er op 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.
In artikel 7 van dit reglement zijn de kaders van heimelijk cameratoezicht beschreven.

Meldingsplicht (heimelijk) cameratoezicht

Het toepassen van cameratoezicht hoeft - in beginsel - niet te worden gemeld[2] bij de Autoriteit Persoonsgegevens (of functionaris voor gegevensbescherming indien deze 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 nadrukkelijk wél worden gemeld.

Beveiliging

De toegang tot en gebruik van camera's en opgenomen camerabeelden moet adequaat beveiligd zijn. Denk hierbij aan het instellen van de juiste autorisaties: alleen geautoriseerde medewerkers hebben toegang tot alle beelden. Ook de apparatuur waarop de beelden worden opgenomen of opgeslagen, moeten 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).

Rechten betrokkenen

De wet geeft studenten, medewerkers en bezoekers een aantal rechten. Belangrijk is om te beseffen dat de studenten, medewerkers en bezoekers het recht hebben op de beelden in te zien waarop zij zelf te zien zijn. Dit gaat dus niet om beelden waarop enkel hun eigendommen te zien zijn. Dit verzoek mag niet worden geweigerd om personele of administratieve lasten te beperken. Wél mag een dergelijk inzageverzoek worden afgewezen wanneer het inzageverzoek ongespecificeerd is, of als het inzagerecht kennelijk misbruikt wordt[3]. Hiernaast mag een inzageverzoek worden geweigerd als het noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten.

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. Een andere grond is als inzage of verstrekking van de beelden noodzakelijk is op grond van een wettelijke verplichting of voor de goede vervulling van de (publiekrechtelijke) taak van politie en justitie in het geval van incidenten en opsporing. Hieronder valt ook het verstrekken van beelden aan bij wet ingestelde inlichtingendiensten zoals de AIVD.

Rol van de ondernemingsraad en studentenraad

Cameratoezicht betreft de privacy van studenten, medewerkers en bezoekers. Bij het vaststellen, wijzigen of intrekken van het reglement cameratoezicht, wordt de ondernemingsraad en studentenraad om instemming gevraagd.

[2] Artikel 38 Vrijstellingsbesluit Wbp
[3] Zie de richtlijn van de Autoriteit Persoonsgegevens voor een toelichting.