

REGLEMENT CAMERATOEZICHT UNIVERSITEIT MAASTRICHT

Artikel 1 Doelen en grondslag van het cameratoezicht, noodzakelijkheid en proportionaliteit

1. Het Cameratoezicht van de Universiteit Maastricht (hierna: UM) heeft ten doel:
 - a. de bescherming van de veiligheid en gezondheid van medewerkers, studenten en bezoekers van de UM;
 - b. de beveiliging van de toegang tot gebouwen en terreinen van de UM;
 - c. de bewaking van zaken die zich in gebouwen of op terreinen van de UM bevinden;
 - d. het vastleggen van incidenten;
 - e. het reguleren van verkeersstromen voor studenten, medewerkers en bezoekers van de UM ten behoeve van de verkeersveiligheid.
2. De grondslag voor het verwerken van Persoonsgegevens middels Cameratoezicht is gelegen in de behartiging van de gerechtvaardigde belangen van de UM in het kader van de onder het eerste lid beschreven doelen.
Bij het Cameratoezicht van de UM worden de vereisten van noodzakelijkheid en proportionaliteit in acht genomen, evenals de overige wettelijke vereisten op grond van de AVG.

Artikel 2 Reikwijdte

Dit reglement betreft alle beveiligingscamera's van de UM. Camera's die worden ingezet voor het opnemen van (hoor)colleges vallen buiten de reikwijdte van dit reglement.

Artikel 3 Begripsbepalingen

1. **AVG**: de Algemene Verordening Gegevensbescherming (EU Verordening nr. 2016/679);
2. **Betrokkene**: degene op wie een persoonsgegeven betrekking heeft (artikel 4 sub 1 AVG);
3. **Camerasysteem**: het geheel van camera's, monitoren, opnameapparatuur, servers, verbindingkasten, verbindingen en bevestigingen of andere wijze van datatransport van beeldmateriaal en of apparatuur;
4. **Cameratoezicht**: het vervaardigen van afbeeldingen van een of meer personen, gebruik makend van duidelijk zichtbare camera('s) waarbij de Verwerkingsverantwoordelijke de student, medewerker of bezoeker op duidelijke wijze in kennis heeft gesteld van de mogelijkheid van cameratoezicht op algemeen toegankelijke ruimtes in de universitaire gebouwen en terreinen, niet zijnde de werkplekken;
5. **Centralist**: geautoriseerde medewerker die de beelden live bekijkt en die belast is met het bedienen van het camerasysteem;
6. **Derde(n)**: een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan niet zijnde de Betrokkene, de Verwerkingsverantwoordelijke, de Verwerker, of enig persoon die onder rechtstreeks gezag van de Verwerkingsverantwoordelijke of de Verwerker gemachtigd is om persoonsgegevens te verwerken (artikel 4 sub 10 AVG);
7. **Functionaris Gegevensbescherming ('FG')**: de door het College van Bestuur aangestelde medewerker die toezicht houdt op de naleving en toepassing van de AVG;
8. **Functioneel beheerder**: de medewerker van de UM die ten behoeve van de Verwerkingsverantwoordelijke is belast met het beheer van het camerasysteem;
9. **Geautoriseerde medewerker**: de medewerker die toegang heeft tot de live-beelden van het camerasysteem en het bedienen ervan;
10. **Gebouwenbeheerder**: een door het Hoofd van de beheerseenheid als gebouwenbeheerder aangewezen medewerker;
11. **Gegevens**: de door het camerasysteem verkregen en geregistreerde camerabeelden die mogelijk persoonsgegevens kunnen bevatten;
12. **Hoofd beheerseenheid**: de decaan van een faculteit dan wel de directeur van een servicecentrum of van MUO;
13. **Incident**: een waargenomen gedraging, ongeval of andere gebeurtenis die vraagt om onmiddellijk optreden;

14. **Persoonsgegevens:** elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4 sub 1 AVG);
15. **Receptie/portiersloge:** de ruimte van waaruit een portier of receptionist de live camerabeelden kan bekijken;
16. **Systeemeigenaar:** degene die door het College van Bestuur is aangewezen als verantwoordelijke voor het camerasysteem en belast is met het beheer van het camerasysteem (i.e. de directeur Facility Services);
17. **Technisch beheerder:** de medewerker die belast is met het technisch beheer van het camerasysteem;
18. **Verwerker:** een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, ten behoeve van de Verwerkingsverantwoordelijke persoonsgegevens verwerkt (artikel 4 sub 8 AVG);
19. **Verwerkingsverantwoordelijke:** een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Ter zake de inzet van het cameratoezicht betreft dit de UM;
20. **Verwerking van persoonsgegevens:** een bewerking of geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding, of enige andere vorm van terbeschikkingstelling, samenbrengen, aligneren of combineren, afschermen, uitwissen, of vernietigen van Gegevens (artikel 4 sub 2 AVG);
21. **Video-observatieruimte:** de besloten ruimte van waaruit de beelden via de opnameapparatuur kunnen worden teruggekeken. Dit kan een voor de gelegenheid gekozen ruimte/werkplek zijn waar middels technische voorzieningen de filmbeelden kunnen worden teruggekeken.

Artikel 4 Taken en verantwoordelijkheden

1. Het College van Bestuur (hierna: 'CvB') is binnen de UM verantwoordelijk voor de Verwerking van de persoonsgegevens.
2. De directeur Facility Services is aangewezen als Systeemeigenaar en is jegens het CvB verantwoordelijk voor het Cameratoezicht.
3. De Systeemeigenaar is verantwoordelijk voor het treffen van adequate technische en organisatorische maatregelen ter bescherming van het Camerasysteem.
4. De directeur Facility Services heeft het beheer van het Camerasysteem gemandateerd aan de Functioneel beheerder. De Functioneel beheerder besluit over het plaatsen van camera's daartoe gemandateerd door de directeur Facility Services.
5. Het technisch beheer van het Cameratoezicht is toegewezen aan de Technisch beheerder en geschiedt onder verantwoordelijkheid van de Systeemeigenaar.
6. Door of namens het CvB worden Geautoriseerde medewerkers aangewezen welke uit hoofde van hun functie toegang hebben tot de camerabeelden.
7. De Centralisten en Geautoriseerde medewerkers zijn bevoegd tot het live bekijken van de camerabeelden en het bedienen van het Camerasysteem. Zij zijn gehouden om vertrouwelijk met deze Gegevens om te gaan conform het in de CAO Nederlandse Universiteiten en de Gedragscode Integriteit UM bepaalde.
8. Ingeval van een Incident meldt de Centralist, de portier c.q. receptionist dit bij de geëigende instantie.

Artikel 5 Het plaatsen van camera's

1. Het feit dat Cameratoezicht plaatsvindt wordt onder meer kenbaar gemaakt door middel van borden of afbeeldingen bij de terreinen en de ingangen van de gebouwen van de UM. Betrokkenen worden daarbij geïnformeerd over de identiteit en contactgegevens van de Verwerkingsverantwoordelijke teneinde hun rechten zoals bedoeld in artikel 11 hierna c.q. hoofdstuk III AVG te kunnen uitoefenen.
2. Op aanvraag van de Gebouwenbeheerder kunnen camera's worden geplaatst. Een aanvraag wordt gedaan bij de Functioneel beheerder. Op basis van een toetsing conform de door de Systeemeigenaar vastgestelde richtlijnen zal deze vervolgens over een definitieve plaatsing beslissen.

Artikel 6 Heimelijk cameratoezicht

1. In bijzondere omstandigheden kunnen op de terreinen en in de gebouwen van de UM tijdelijk verborgen camera's worden ingezet bij de bescherming en beveiliging van personen en zaken indien er vermoedens zijn van strafbare feiten of ander laakbaar gedrag. Toepassing van heimelijk Cameratoezicht kan alleen worden toegestaan met inachtneming van het wettelijk kader.
2. Een verborgen camera kan slechts met toestemming van het CvB worden geplaatst.
3. De Functioneel beheerder kan een voorstel doen voor het plaatsen van een verborgen camera, na overleg met de Systeemeigenaar en het betrokken Hoofd van de beheerseenheid en na advies van de FG. De desbetreffende Gebouwenbeheerder wordt over het plaatsen van een verborgen camera geïnformeerd.

Artikel 7 Beveiliging

De Systeemeigenaar draagt zorg voor passende technische en organisatorische maatregelen om de Persoonsgegevens te beveiligen tegen verlies of om enige vorm van onrechtmatige Verwerking van persoonsgegevens te voorkomen.

Met betrekking tot het Camerasysteem is een risico beoordeling uitgevoerd conform de UM classificatierichtlijn. Het risico profiel is vastgesteld op Midden, Midden, Midden op de elementen Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV=MMM). Alle door de UM vastgestelde beveiligingsmaatregelen behorende bij dit risicoprofiel zijn geïmplementeerd en worden periodiek getoetst.

Artikel 8 Toegang tot het camerasysteem

1. Voor zover de toegang tot de Gegevens noodzakelijk is voor de uitvoering van hun taak, hebben de door of namens het CvB aangewezen personen rechtstreeks toegang tot de Persoonsgegevens.
2. Onbevoegden c.q. Derden hebben geen toegang tot het Camerasysteem.

Artikel 9 Verslaglegging en rapportage

1. Van het gebruik van het Camerasysteem wordt een vertrouwelijk logboek bijgehouden.
2. In het logboek worden vermeld: naam van de dienstdoende Centralist, datum, tijd en bijzonderheden, zoals: storingen, Incidenten, meldingen, vordering van Gegevens etc.
3. Buiten gebruik wordt het logboek opgeborgen in een afgesloten kast.
4. Elke geconstateerde bijzonderheid of onregelmatigheid wordt onverwijld gemeld bij de Functioneel beheerder.
5. Jaarlijks wordt door de Functioneel beheerder aan de Systeemeigenaar een rapportage uitgebracht over Incidenten, het gebruik van het logboek, de bevindingen met de registratie en het raadplegen van het materiaal.
6. Desgevraagd levert de Functioneel beheerder een overzicht van namen van de Centralisten en Geautoriseerde medewerkers.

Artikel 10 Omgang met gegevens; bewaartermijn

1. De Gegevens worden uitsluitend gebruikt voor de doelstellingen zoals vermeld in artikel 1 van dit reglement.
2. De Gegevens worden niet langer bewaard dan noodzakelijk, waarbij als richtlijn geldt een bewaartermijn van maximaal 7 kalenderdagen, met als uitzondering een bewaartermijn van 14 kalenderdagen gedurende de sluitingsweek van de UM tussen kerstmis en de jaarwisseling. Indien er sprake is van gegronde redenen, bijvoorbeeld met betrekking tot de afhandeling van een op camera vastgelegd Incident, blijven de betreffende Gegevens bewaard zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen noodzakelijk is en het geconstateerde Incident is afgehandeld. Het College van Bestuur of een daartoe gemandateerde bepaalt of er sprake is van gegronde redenen.

Artikel 11 Rechten van betrokkenen

1. Een Betrokkene heeft ingevolge hoofdstuk III van de AVG onder andere recht op informatie over de Verwerking (artikel 13 AVG), recht op inzage (artikel 15 AVG), recht op gegevenswissing (artikel 17 AVG), recht op beperking van de Verwerking (artikel 18 AVG), recht op overdraagbaarheid van Gegevens (artikel 20 AVG) en recht van bezwaar (artikel 21 AVG), een en ander met inachtneming van de toepasselijke wettelijke voorwaarden en beperkingen. Een verzoek van een Betrokkene strekkende tot uitoefening van één of meerdere van deze rechten dient te worden gericht aan het CvB via privacy@maastrichtuniversity.nl.
2. Inzage in de Gegevens geschiedt altijd onder begeleiding van de Functioneel beheerder of een andere daartoe door of namens het CvB aangewezen Geautoriseerde medewerker. Betrokkene legitimeert zich vooraf ten overstaan van de in de voorgaande volzin genoemde personen. Betrokkenen die inzage verkrijgen, tekenen een inzage-verklaring.
3. Klachten over de toepassing van het Camerasysteem en/of over het gedrag van de bij het Cameratoezicht betrokken medewerkers worden schriftelijk ingediend bij het CvB en worden afgehandeld conform de daarvoor geldende procedure.
4. Het CvB zal binnen 6 weken na datum ontvangst van een verzoek of klacht beslissen.

Artikel 12 Uitgifte van gegevens en inzage aan Derden

1. Gegevens worden slechts aan Derden, waaronder opsporingsambtenaren en de rechtercommissaris, verstrekt op verzoek, vordering en/of op basis van een getoetste wettelijke grondslag. Een dergelijk verzoek of vordering dient te worden gericht aan het CvB via privacy@maastrichtuniversity.nl.
2. De Gegevens worden in onderling overleg op een beveiligde wijze uitgewisseld.
3. Inzage van Gegevens aan Derden wordt uitsluitend gegeven met inachtneming van de geldende wet- en regelgeving.
4. Inzage vindt plaats overeenkomstig artikel 11, tweede lid.
5. De betreffende Derde tekent voor ontvangst c.q. inzage van de Gegevens.
6. Het CvB zal binnen 6 weken na datum ontvangst van een verzoek of vordering beslissen.

Artikel 13 Wijze van openbaarmaking

Het Reglement Cameratoezicht UM wordt online gepubliceerd op de website van de UM.

Artikel 14 Slotbepalingen

1. In alle gevallen waarin dit reglement niet voorziet beslist het CvB.
2. Dit reglement treedt in werking de dag na vaststelling door het CvB en vervangt de eerder in 2006 vastgestelde versie.

Aldus vastgesteld, na instemming van de Universiteitsraad en het Lokaal Overleg, in de vergadering van het College van Bestuur d.d. 18 december 2018.