

Reglement Cameratoezicht Avans Hogeschool

(definitieve versie 25 februari 2025)

1. Inleiding

Een camerasysteem dat wordt gebruikt voor toezicht maakt en bewaart beelden aan de hand waarvan personen kunnen worden geïdentificeerd. Het gebruik van een camerasysteem is dus een verwerking van persoonsgegevens en moet daarom voldoen aan de Algemene Verordening Gegevensbescherming (AVG). Dit reglement geeft een beschrijving van uitgangspunten, taken, verantwoordelijkheden en procedures om integer gebruik van het cameratoezicht en de privacy van betrokkenen te waarborgen. Het reglement is van toepassing op alle locaties (gebouwen en terreinen) van Avans Hogeschool.

2. Begripsbepalingen

- 2.1 Beeldinformatie: de door het camerasysteem verkregen en geregistreerde filmbeelden;
- 2.2 Beheerder: degene die is belast met het beheren van het camerasysteem;
- 2.3 Betrokkene: degene wiens persoonsgegevens worden verwerkt;
- 2.4 Camerasysteem: het geheel van camera's, monitoren, opnameapparatuur, opslagmedia, servers, verbindingen en bevestigingen;
- 2.5 Cameratoezicht: toezicht met behulp van camera's of andere huidige en toekomstige apparatuur waarmee toezicht kan worden uitgeoefend door het maken van opnames op of in een gebouw, gebied of van (groepen) mensen;
- 2.6 Functionaris Gegevensbescherming: de persoon die bij Avans Hogeschool belast is met het toezichthouden op de toepassing en naleving van de AVG;
- 2.7 Geautoriseerde medewerker: de (beveiligings-)medewerker die bevoegd toegang heeft tot de beeldinformatie of derden die zich vooraf gelegitimeerd hebben en toestemming hebben van de geautoriseerde medewerker (onderhoud) en toegang hebben tot de beeldinformatie;
- 2.8 Incident: een al dan niet via het camerasysteem waargenomen / vermoedelijk strafbaar feit, ongeval of andere gebeurtenis die vraagt om optreden;
- 2.9 Incidentenregister: het document waarin de door middel van het cameratoezicht geconstateerde incidenten worden vastgelegd.
- 2.10 Medewerker locatiedienst: de door de beheerder aangewezen persoon die de beeldinformatie live bekijkt;
- 2.11 Technisch beheerders: de medewerkers die belast zijn met het onderhoud en kwaliteit van het camerasysteem en de daar bijhorende randvoorwaarden;

3. Uitgangspunten cameratoezicht Avans Hogeschool

3.1 Subsidiariteit en proportionaliteit

Cameratoezicht kan een effectief middel zijn om de veiligheid van personen, goederen en gebouwen te vergroten. Tegelijkertijd kan cameratoezicht relatief sterk in de persoonlijke levenssfeer ingrijpen. Daarom is cameratoezicht een onderdeel van een breder pakket veiligheidsmaatregelen binnen Avans Hogeschool. De afspraak is dat cameratoezicht alleen wordt ingezet waar middelen die voor de privacy van betrokkenen minder ingrijpend zijn niet volstaan én voor zover de inzet van camera's in redelijke verhouding staat tot de nagestreefde doelen (zie artikel 3.2).

3.2 Doelen van het cameratoezicht

Cameratoezicht kan worden ingezet voor:

1. De bescherming van de veiligheid en gezondheid van één of meer natuurlijke personen, zoals studenten en medewerkers;
2. Het beveiligen van (de toegang tot) gebouwen en terreinen van Avans Hogeschool;
3. Het tegengaan van diefstal of vernieling van goederen in de gebouwen of op terreinen van Avans Hogeschool;
4. Het vastleggen van mogelijke incidenten.

Avans verzamelt beeldinformatie in het kader van de eerder genoemde beveiligingsdoeleinden door cameratoezicht op basis van haar gerechtvaardigd belang. Het gerechtvaardigd belang vormt de grondslag voor de gegevensverwerking, zie daarover ook het privacy statement van Avans Hogeschool (privacystatement.avans.nl/#beeldmateriaal-bij-avans). Beeldinformatie mag niet voor andere dan de hierboven genoemde doeleinden worden gebruikt.

3.3 Positionering camera's

Het is van belang dat de camera's op een zodanige manier worden gepositioneerd dat de negatieve impact op de privacy van de betrokkenen wordt geminimaliseerd. Gebieden die niet relevant zijn om te filmen, worden niet in beeld gebracht.

Als algemene regel geldt dat Avans Hogeschool het cameratoezicht beperkt tot:

- zorgvuldig geselecteerde gebieden met gevoelige informatie, voorwerpen van hoge waarde of andere activa die om een specifieke reden een verhoogde bescherming vereisen,
- in- en uitgangen van de gebouwen (met inbegrip van nooduitgangen en branduitgangen en muren of hekken rond het gebouw of het terrein), en
- in- en uitgangen binnen het gebouw die verschillende gebieden verbinden waarvoor verschillende toegangsrechten gelden en die van elkaar gescheiden zijn door vergrendelde deuren of een ander mechanisme voor toegangscontrole.

Op plaatsen waar een hogere bescherming van de privacy wordt verwacht mag geen cameratoezicht worden uitgeoefend.

3.4 Kenbaarheid cameratoezicht

Waar gebruik wordt gemaakt van cameratoezicht, wordt dit in beginsel altijd voor een ieder kenbaar gemaakt door stickers op toegangsdeuren en op informatieborden bij de toegang tot terreinen of gebouwen van Avans Hogeschool. Naast cameratoezicht worden geen geluidsopnamen gemaakt.

Artikel 6 omschrijft de (beperkte) mogelijkheid van heimelijk (verborgen) cameratoezicht.

4. Taken en verantwoordelijkheden

- 4.1 Het cameratoezicht geschiedt onder verantwoordelijkheid van het College van Bestuur (CvB), in mandaat door de directeur DF&V. Het CvB houdt zich wel de beslissingen met betrekking tot verborgen cameratoezicht voor.
- 4.2 Het effect van het cameratoezicht op de privacyaspecten wordt beoordeeld aan de hand van een gegevensbeschermingseffectbeoordeling (DPIA) waarbij de mate van en de ernst van de inbreuk op de privacy van de studenten, medewerkers en bezoekers wordt afgewogen tegen het belang van Avans Hogeschool om cameratoezicht te gebruiken. Hierbij wordt onder andere meegewogen of de doelstellingen als geformuleerd in artikel 3.2, op een andere wijze kunnen worden bereikt met een minder ingrijpend middel dan cameratoezicht. Deze beoordeling wordt periodiek herhaald en tevens uitgevoerd wanneer de inzet van cameratoezicht wezenlijk wordt gewijzigd, bijvoorbeeld door het gebruik van nieuwe technologieën of verruiming van de reikwijdte van het toezicht.
- 4.3 De beheerder van het camerasysteem is de contractmanager E&W van Dienst Facilitair en Vastgoed. (DF&V)
- 4.4 Het technisch beheer van het cameratoezicht geschiedt door een door de

beheerder aan te wijzen persoon/personen.

Hierin is onderscheid gemaakt in:

- Hardware: technisch beheerder is Team E&W van DF&V.

. Zij houden toezicht op technisch beheer (onderhoud en plaatsing) van de hardware welke is uitbesteed aan een leverancier van Avans;

- Software: technisch beheerder is DI&T. Zij beheren de software welke verband houdt met het cameratoezicht, hieronder wordt onder meer verstaan verstrekking van toegang tot applicaties aan geautoriseerde medewerkers, up to date houden van applicaties en zorgdragen voor goede werking van de software. Software kan al dan niet worden onderhouden in samenwerking met de externe leverancier. Ten aanzien van technisch camerabeheer is de gecontracteerde partij welke verantwoordelijk is voor het up-to-date houden van soft-/firmware;

- Protocollen en positionering van de camera's: technisch beheerder is Dienst Facilitair en Vastgoed (E&W en Veiligheid). Hieronder wordt verstaan het actueel houden van en toezien op juiste naleving van dit reglement met ondersteuning van Team Privacy en Security en Juridische Zaken. Daarnaast bepalen zij, in samenspraak met de leverancier, de positionering van de camera's met inachtneming van hetgeen is bepaald in artikel 3 van dit reglement.

4.5 Bevoegd tot het bedienen van het camerasysteem c.q. het live bekijken van beeldinformatie zijn:

- a. de medewerkers locatiediensten (alleen bekijken van live beelden);

- b. de technische beheerders zoals genoemd onder 4.4.;

- c. de beheerder of diens vervanger (volledig bevoegd, d.w.z. het bekijken van live beelden en eerder gemaakte opnames en het vastleggen van beeldinformatie);

- d. derden, indien dat functioneel noodzakelijk is, uitsluitend met toestemming van de beheerder of diens vervanger.

4.6 Om het aantal personen dat bevoegd is tot het niet live bekijken van beeldinformatie zoveel mogelijk te beperken teneinde de privacy en de veiligheid van betrokkenen te waarborgen, zijn naast de beheerder geautoriseerde medewerkers bevoegd zijnde:

- a. Leidinggevenden van Avans Hogeschool voor zover noodzakelijk voor hun werkzaamheden die verband houden met hun verantwoordelijkheden;

- b. Coördinatoren van locatiediensten;

- c. Medewerkers van team Veiligheid;

4.7 Alleen geautoriseerde medewerkers mogen toegang hebben tot beeldinformatie. Periodiek controleert de beheerder de rollen en rechten van de geautoriseerde medewerkers om onbevoegde toegang te voorkomen.

4.8 Medewerkers locatiediensten rapporteren middels een melding in Servicepunt relevante bijzonderheden meteen aan de geautoriseerde medewerker.

4.9 De technisch beheerders zijn ieder verantwoordelijk voor hetgeen is genoemd in artikel 4.4. en voeren daartoe op gezette tijden controles uit.

5. Inrichting en beveiliging van het camerasysteem

5.1 De beheerder is verantwoordelijk voor de inrichting van het camerasysteem en de plaatsing van de camera's, binnen de kaders van de uitgevoerde DPIA als bedoeld in artikel 4 lid 2.

5.2 De beheerder is verantwoordelijk voor passende technische en organisatorische maatregelen om de beeldinformatie 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 de te beschermen beeldinformatie. De maatregelen betreffen in ieder geval het camerasysteem en de serverruimte.

- 5.3 De met het camerasysteem en -toezicht belaste medewerkers gaan vertrouwelijk en integer om met de kennis die zij tot zich krijgen door de beeldinformatie in het bijzonder met betrekking tot de privacy van betrokkenen. Voor zover voornoemde medewerkers niet onder de CAO van het HBO vallen, waarborgt de beheerder dat de betreffende geautoriseerde medewerker een geheimhoudingsverklaring tekent.
- 5.4 De beeldinformatie en het feitenverslag worden maximaal 28 dagen bewaard waarna de informatie wordt gewist. In geval van een incident wordt de bewaartermijn verlengd tot het incident is afgehandeld. In geval van een inzageverzoek conform artikel 7 van dit reglement wordt de beeldinformatie bewaard totdat een beslissing is genomen op dit verzoek.

6. Verborgene cameratoezicht

- 6.1 Gebruik van verborgene cameratoezicht is alleen toegestaan wanneer het doel van de inzet vereist dat het gebruik van camera's niet bekend wordt. Een verborgene camera zal enkel worden ingezet als 'laatste redmiddel'. Voorafgaand aan de inzet van verborgene cameratoezicht, wordt advies ingewonnen van de Functionaris Gegevensbescherming.
- 6.2 Het besluit tot plaatsing van een verborgene camera is voorbehouden aan het College van Bestuur. In haar schriftelijke besluit vermeldt het College van Bestuur de voorwaarden die voor de inzet gelden.
- 6.3 De inzet van een verborgene camera is altijd tijdelijk. Het besluit van het College van Bestuur dat aan de inzet van verborgene cameratoezicht ten grondslag ligt, vermeldt de maximale duur van de inzet.
- 6.4 Wanneer verborgene cameratoezicht wordt ingezet dan moet hiervoor altijd een DPIA worden uitgevoerd. Ook als het verborgene cameratoezicht incidenteel is.

7. Rechten van betrokkene

Een betrokkene heeft verschillende rechten ten aanzien van zijn/haar persoonsgegevens. Met betrekking tot persoonsgegevens die worden verwerkt als gevolg van het cameratoezicht, hebben betrokkenen het recht om camerabeelden in te zien waarop zij zelf zichtbaar zijn, vergeten te worden, en bezwaar te maken tegen het gebruik van de betreffende persoonsgegevens. Het [privacy statement](#) bevat meer informatie over de wijze waarop deze rechten kunnen worden uitgeoefend. Ter aanvulling op hetgeen beschreven staat in het privacy statement geldt dat de beeldinformatie nog beschikbaar moet zijn en dat rechten kunnen worden geweigerd, indien dat noodzakelijk is in het belang van voorkoming, opsporing en vervolging van strafbare feiten of ter bescherming van rechten en vrijheden van anderen.

8. Inzagerecht beeldinformatie door derden

- 8.1 Inzage in de beeldinformatie en uitgifte van de beeldinformatie aan derden vindt alleen plaats:
- a. op vordering van de politie of het Openbaar Ministerie, waarbij de vordering gebaseerd is op een wettelijke grondslag;
 - b. aan de politie bij aangifte van een (vermoeden van een) strafbaar feit; en
 - c. in andere gevallen wanneer dit verenigbaar is met doeleinden zoals vermeld in dit reglement en de wet hiervoor een grondslag biedt.
- 8.2 De directeur DF&V en Services toetst altijd of de vordering van de politie of het Openbaar Ministerie voldoende grondslag biedt voor de gevraagde inzage en/of uitgifte.
- 8.3 Een verzoek tot inzage en/of uitgifte door derden, dient te worden ingediend bij de beheerder. De beheerder informeert hierover de directeur DF&V.
- 8.4 De directeur DF&V beslist zo spoedig mogelijk op het verzoek, waarbij uitdrukkelijk rekening wordt gehouden met het recht op bescherming van de persoonlijke levenssfeer van de betrokkenen.
- 8.5 Eenieder die de beelden mag inzien of daarvan een kopie ontvangt dient zich vooraf

te legitimeren ten overstaan van de beheerder. De inzage in de beelden vindt plaats in het bijzijn van de beheerder of een geautoriseerde medewerker. Voor ontvangst van een kopie van de beeldinformatie dient getekend te worden door zowel de directeur DF&V en Services als door de ontvanger.

9. Verslaglegging & Rapportage

- 9.1 De beheerder draagt zorg voor het bijhouden van een logboek van het volledig bevoegd gebruik van het camerasysteem.
- 9.2 De technisch beheerder houdt een logboek bij betreffende de controle op juiste werking van het camerasysteem.
- 9.3 Deze logboeken zijn vertrouwelijk en uitsluitend ter inzage voor de beheerder, de geautoriseerde medewerkers zijnde coördinatoren locatiediensten, medewerkers van het team Veiligheid en het College van Bestuur.
- 9.4 In de logboeken wordt vermeld: naam van de dienstdoende (technisch) beheerder, datum, tijd en bijzonderheden, zoals: storingen, incidenten, meldingen, vordering van beeldinformatie.
- 9.5 Buiten gebruik wordt het logboek op veilige wijze digitaal opgeslagen.
- 9.6 De technisch beheerder meldt de technische bijzonderheden aan het camerasysteem aan de beheerder.
- 9.7 De beheerder voert periodiek controle uit van de logbestanden, de wijze waarop opvolging wordt gegeven en de uitkomsten daarvan.
- 9.8 In het eerste kwartaal van elk jaar wordt de AMR van Avans Hogeschool door het College van Bestuur geïnformeerd over eventueel reeds toegepast cameratoezicht met behulp van verborgen camera's. De AMR wordt geïnformeerd over de aard, frequentie en duur van het verborgen cameratoezicht in het voorafgaande jaar. Het College van Bestuur en/of de AMR kunnen op verzoek inzage in het incidentenregister en logboek krijgen.

10. Toezicht

- 10.1 De Functionaris Gegevensbescherming (FG) van Avans Hogeschool voert de controle uit op de naleving van de in dit reglement opgenomen bepalingen.
- 10.2 Deze controle omvat het nagaan of de opzet van de organisatie, met inbegrip van de procedures, in overeenstemming is met het gestelde in dit reglement en het nagaan, op willekeurige tijdstippen, of door de desbetreffende functionarissen dit reglement en de procedures worden nageleefd. De controle betreft ook de beveiliging van het camerasysteem tegen inbraak en diefstal.
- 10.3 De FG rapporteert ten minste eenmaal per jaar zijn bevindingen aan het College van bestuur, dat het verslag doorstuurt naar de AMR.

11. Slotbepalingen

- 11.1 In gevallen waarin dit reglement niet voorziet beslist het College van Bestuur.
- 11.2 Dit reglement is door het College van Bestuur en na instemming van de medezeggenschapsraad op 25 februari 2025 vastgesteld en treedt per die datum in werking.
- 11.3 Avans Hogeschool heeft het recht om wijzigingen aan te brengen in dit reglement. Wijzigingen in deze tekst maken we via de website van Avans Hogeschool bekend en treden in werking vanaf het moment dat ze op de website zijn gepubliceerd.