Reglement cameratoezicht

Documentsoort: Reglement cameratoezicht
Eigenaar: Liz Chermin (CvB)
Auteur: Joyce Kolen (FG)
Datum: 20 december 2021
Document ID: CvB/2122.015
Versie: 2024

yonder

Inhoud

Hoofdstuk 1: Inleiding

Cameratoezicht wordt in verschillende situaties gebruikt, bijvoorbeeld om personen en eigendommen te beschermen. Het is hierbij van belang dat organisaties zorgvuldig met het cameratoezicht en de camerabeelden omgaan. Het inzetten van cameratoezicht past in een totaalpakket aan fysieke maatregelen dat wordt toegepast om de veiligheid van leerlingen, studenten, medewerkers en bezoekers binnen en buiten in de directe omgeving van de locaties van de scholen te waarborgen. Cameratoezicht mag geen doel op zichzelf zijn. Cameratoezicht maakt deel uit van een totaalpakket aan maatregelen rondom beveiliging en sociale veiligheid binnen een school.

Op scholen hangen steeds vaker camera's, bijvoorbeeld om vernielingen of diefstal tegen te gaan. Maar er is ook sprake van een inbreuk op de privacy van leerlingen, studenten, medewerkers en bezoekers als cameratoezicht wordt toegepast. Daarom mogen scholen alleen camera's ophangen als aan een aantal voorwaarden wordt voldaan. Ook moet met cameratoezicht de inbreuk op de privacy zo klein mogelijk zijn. Het uitgangspunt blijft dat mensen onbevangen zichzelf moeten kunnen zijn.

Dit document is bedoeld om het gebruik van cameratoezicht goed te regelen, en daarbij de privacy van leerlingen, studenten, medewerkers en bezoekers te waarborgen. Het reglement cameratoezicht heeft betrekking op die locaties waar toezicht door middel van camerasystemen wordt ingezet. Het geeft een beschrijving van taken, verantwoordelijkheden en procedures met betrekking tot het cameratoezicht, met het oog op integer gebruik van het camerasysteem en de bescherming van privacy van leerlingen, studenten, medewerkers en bezoekers.

Hoofdstuk 2: Toelichting

Verantwoordelijkheid
Het zorgvuldig omgaan met gegevens is (wettelijk) de verantwoordelijkheid van Yonder zelf. De Algemene Verordening Gegevensbescherming (AVG) wijst het bevoegd gezag, concreet het College van Bestuur, aan als verantwoordelijke om de privacy van leerlingen, studenten, medewerkers en bezoekers (ook wel betrokkenen genoemd) te regelen. Yonder kan deze verantwoordelijkheid niet afwentelen op bijvoorbeeld haar leveranciers (die in het kader van de AVG ook wel verwerkers worden genoemd). De persoon op wie de persoonsgegevens betrekking hebben, wordt betrokkene genoemd. Dat kan een leerling of student zijn, maar ook een medewerker of zelfs bezoekers.

Wanneer Yonder een extern (beveiligings)bedrijf inhuurt voor het cameratoezicht, dan is dat bedrijf een verwerker. Dat betekent onder meer dat Yonder aparte afspraken (verwerkersovereenkomst) maakt over de toegang tot en het gebruik van het camerasysteem en de camerabeelden. Het (beveiligings)bedrijf moet zich houden aan de instructies van Yonder, en dus ook aan dit reglement cameratoezicht.

Als Yonder cameratoezicht wil inzetten, dan ligt de eindverantwoordelijkheid daarvoor bij het College van Bestuur. Die stelt, met instemming van de medezeggenschap, 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 AVG geeft een school een aantal randvoorwaarden mee waar cameratoezicht aan moet voldoen. De toezichthouder in Nederland op het gebruik van persoonsgegevens, de Autoriteit Persoonsgegevens (AP), heeft dit uitgewerkt in de Beleidsregels cameratoezicht van 28 januari 2016.

Gerechtvaardigd belang
De school moet een zogeheten gerechtvaardigd belang hebben voor het cameratoezicht. Bijvoorbeeld diefstal tegengaan of de sociale en fysieke veiligheid van leerlingen, studenten, medewerkers en bezoekers beschermen.

Noodzaak cameratoezicht
Het cameratoezicht moet noodzakelijk zijn. Dat wil zeggen dat de school het doel niet op een andere manier kan bereiken. De school 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.

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:
de bescherming van de veiligheid en gezondheid van leerlingen, studenten, medewerkers en bezoekers;
de beveiliging van de toegang tot gebouwen en terreinen;
de bewaking van zaken die zich in gebouwen of op terreinen bevinden;
het vastleggen van incidenten.
Het gebruik van deze camerabeelden voor bijvoorbeeld interne trainingen of educatieve doeleinden, is dus niet toegestaan. Het is tevens niet toegestaan om camerabeelden te gebruiken voor absentie- of aanwezigheidscontrole of als personeelsvolgsysteem.

Privacytoets
Yonder voert vanaf de datum van inwerkingtreding van dit reglement een privacytoets (DPIA) uit over veranderingen in het cameratoezicht. Bij deze toets wordt de afweging gemaakt tussen de privacybelangen van de leerlingen, studenten, medewerkers en bezoekers en 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. Het College van Bestuur 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 College van Bestuur, wordt dit in een DPIA vastgelegd.

Informatieplicht cameratoezicht
De leerlingen, 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 schoolgids 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 de school 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 betrokkenen te informeren, is normaal gesproken niet toegestaan. Alleen in geval van duidelijke en concrete vermoedens van bijvoorbeeld diefstal of fraude door leerlingen, studenten, medewerkers of bezoekers mag er onder strikte voorwaarden gebruik worden gemaakt van heimelijk cameratoezicht. Belangrijk is dat in het reglement cameratoezicht de leerlingen, 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 bij de Autoriteit Persoonsgegevens (of Functionaris Gegevensbescherming, indien deze is aangesteld). Er moet dan wel voldaan zijn aan de hiervoor genoemde randvoorwaarden, en het gaat om duidelijk zichtbare camera's. Bij heimelijk cameratoezicht is een DPIA verplicht.

Beveiliging
De toegang tot en het 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 van betrokkenen
De AVG geeft leerlingen, studenten, medewerkers en bezoekers een aantal rechten. Belangrijk is om te beseffen dat de leerlingen, 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. 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 medezeggenschap
Cameratoezicht betreft de privacy van leerlingen, studenten, medewerkers en bezoekers. Bij het vaststellen, wijzigen of intrekken van het reglement cameratoezicht, wordt de ondernemingsraad, de gemeenschappelijke medezeggenschapsraad en de studentenraad om instemming gevraagd.

Hoofdstuk 3: Reglement cameratoezicht

Dit reglement cameratoezicht heeft betrekking op alle locaties van Yonder 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, studenten, medewerkers en bezoekers.

Artikel 1 Begripsbepalingen

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, 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) Betrokkenen: de betrokken leerlingen, studenten, medewerkers en bezoekers van wie camerabeelden worden verwerkt.

Artikel 2 Werkingssfeer en doelstellingen cameratoezicht

1 Dit reglement is van toepassing op leerlingen, studenten, medewerkers en bezoekers die zich bevinden in de gebouwen of op de terreinen van Yonder.
2 Het inzetten van cameratoezicht, en het gebruik van de camerabeelden, is alleen toegestaan voor:
> de bescherming van de veiligheid en gezondheid van leerlingen, studenten, medewerkers en bezoekers;
> de beveiliging van de toegang tot gebouwen en terreinen, waaronder mede is begrepen het weren van onbevoegde of onbevoegd verklaarde personen;
> de bewaking van zaken die zich in gebouwen of op terreinen bevinden;
> 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 (DPIA) uit, waarbij de mate van inbreuk op de privacy van de leerlingen, studenten, medewerkers en bezoekers wordt afgewogen tegen het belang van de school om cameratoezicht te gebruiken. Hierbij wordt meegewogen of de doelstellingen, als geformuleerd in artikel 2, lid 2 op een andere wijze kunnen worden bereikt, met een minder ingrijpend middel dan cameratoezicht.
3 Het College van Bestuur wijst het Hoofd Huisvesting en Facilitair als beheerder aan. De beheerder is verantwoordelijk voor de inrichting, het beheer en toezicht op het cameratoezicht.
4 Het College van Bestuur wijst het Hoofd Huisvesting en Facilitair als technisch beheerder aan. De technisch beheerder is verantwoordelijk voor het technisch beheer van het cameratoezicht en -systeem.
5 Het operationeel beheer is gedelegeerd aan de locatiebeheerder van de betreffende locatie of school. De locatiebeheerder is verantwoordelijk voor de werking van het camerasysteem als ook de opslag en het veiligstellen van de beelden op de betreffende locatie of school.
6 De beheerder, de betreffende locatiebeheerder(s) en de bevoegde medewerkers zijn bevoegd tot het live uitkijken van camerabeelden. De volgende personen zijn hiertoe eveneens bevoegd:
a) Hoofd en teamcoördinatoren Huisvesting en Facilitair;
b) Schooldirecteur, voor zover het camerabeelden betreffen van het gebouw c.q. het terrein van de school waarvan hij directeur is;
c) Stafmedewerkers integrale veiligheid;
d) Beveiligingsmedewerkers en toezichthouders;
e) Andere medewerkers van Yonder, voor zover zij daartoe (incidenteel) zijn geautoriseerd. Autorisatie kan slechts worden verleend door het College van Bestuur.
7 De beheerder, de betreffende locatiebeheerder(s) en de bevoegde medewerkers, zoals genoemd in lid 6, zijn bevoegd tot het terugkijken van opgenomen camerabeelden.
8 Het terugkijken van opgenomen camerabeelden geschiedt door ten minste twee bevoegde medewerkers samen.
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 leerlingen, studenten, medewerkers en bezoekers.

10 In geval het College van Bestuur een verwerker inschakelt, geeft deze de verwerker de opdracht om te handelen conform dit reglement.

Artikel 4 Inrichten camerasysteem en beveiliging

1 De beheerder 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 (DPIA), als bedoeld in artikel 3, lid 2.
2 De beheerder 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 beheerder draagt er zorg voor dat het cameratoezicht kenbaar wordt gemaakt aan leerlingen, studenten, medewerkers en bezoekers op zichtbare en herkenbare wijze, zoals, maar niet beperkt tot, 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 schriftelijke 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 (technisch) beheerder of locatiebeheerder, en tekent voor ontvangst van de uitgegeven camerabeelden.
4 Inzage of uitgifte geschiedt slechts na akkoord van de beheerder of het College van Bestuur, na advies van de stafmedewerker(s) integrale veiligheid.
5 De beeldinformatie wordt op een versleutelde externe gegevensdrager verstrekt.
6 Van de inzage en uitgifte wordt door de locatiebeheerder melding gemaakt in het incidentenregistratiesysteem en bij de stafmedewerker(s) integrale veiligheid. De stafmedewerker integrale veiligheid draagt zorg voor de verdere melding in het incidentregistratiesysteem conform de werkinstructie.
7 Aan andere derden wordt geen inzage in de camerabeelden gegeven, en worden geen camerabeelden uitgegeven, anders dan met de uitdrukkelijke toestemming van de betrokken leerlingen, studenten, medewerkers of bezoekers en na akkoord van het College van Bestuur. Van de inzage en uitgifte wordt melding gemaakt, zoals bedoeld in lid 6.

Artikel 6 Rechten van betrokkenen

1 Betrokken leerlingen, 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 beheerder, die binnen 10 werkdagen na ontvangst van het verzoek inhoudelijk zal reageren. De beheerder volgt de vastgestelde procedure rechten van betrokkenen van Yonder.
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, als met het verzoek een inbreuk wordt

gemaakt op de rechten van andere betrokkenen 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 beheerder, de betreffende locatiebeheerder(s) of de bevoegde medewerker(s), 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 Yonder 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 leerlingen, 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 Yonder informeert - voor zover redelijkerwijs mogelijk - achteraf de betrokken leerlingen, studenten, medewerkers en bezoekers over het toegepaste heimelijk cameratoezicht.
5 Voordat heimelijk cameratoezicht wordt toegepast, voert het College van Bestuur een DPIA uit.

Artikel 8 Verslaglegging en rapportage

1 De beheerder 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 medezeggenschap over het cameratoezicht betreffende het voorafgaande jaar. Daarbij wordt specifiek gemeld indien heimelijk cameratoezicht is toegepast.

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, gemeenschappelijke medezeggenschapsraad en de studentenraad om instemming.
2 Het reglement treedt onmiddellijk na vaststelling in werking. Een wijziging in dit reglement treedt in werking binnen 30 dagen na bekendmaking van de wijziging.

Hoofdstuk 4: Werkinstructie bij Reglement cameratoezicht

Deze werkinstructie behoort bij het reglement cameratoezicht van Yonder en geeft een praktische uitwerking van de taken die voortvloeien uit het reglement.

Artikel 3 Camerabeelden terugkijken

1 Het terugkijken van de beelden gebeurt altijd door daartoe geautoriseerde medewerkers (zie artikel 3, leden 6, 7 en 8 van het reglement cameratoezicht Yonder) in opdracht van het College van Bestuur, de beheerder of de schooldirecteur van de betreffende school.
2 Wanneer zich een incident heeft voorgedaan kunnen camerabeelden die hiermee in relatie staan worden bewaard tot dat het onderzoek van het incident is afgesloten. Camerabeelden kunnen slechts door de locatiebeheerder in opdracht van de beheerder of het College van Bestuur bewaard worden in verband met

dit onderzoek. De beelden worden bewaard op een versleutelde USB-stick en ter beschikking gesteld aan het Hoofd ICT Services die deze in de kluis van Yonder bewaart.

Artikel 4 Het plaatsen van camera's

Voordat camera's worden geplaatst, dient er een privacytoets (DPIA) uitgevoerd te worden door de beheerder. Voor de uitvoering hiervan dient advies te worden ingewonnen bij de Coördinator Informatiebeveiliging, de stafmedewerker(s) integrale veiligheid en de Functionaris Gegevens-bescherming. Bij deze privacytoets maakt de beheerder de afweging tussen de privacybelangen van de leerlingen, studenten, medewerkers en bezoekers en de wens van Yonder 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 resultaten van deze privacytoets (DPIA) worden schriftelijk vastgelegd.

Artikel 5 Inzage en uitgifte opgenomen camerabeelden aan derden

3 Het terugkijken van de beelden gebeurt altijd alleen door daartoe geautoriseerde medewerkers en indien noodzakelijk een vertegenwoordiging van de politie waarvoor toestemming is verleend door de beheerder of het College van Bestuur. Deze werkwijze geldt ook als de politie wordt opgeroepen c.q. verzocht om assistentie te verlenen.

4 Camerabeelden mogen slechts aan de politie, de rechter-commissaris of de Officier van Justitie worden verstrekt indien daaraan een schriftelijke vordering ten grondslag ligt. Inzage in de camerabeelden dan wel uitgifte daarvan vindt enkel plaats na toestemming van de beheerder en/of het College van Bestuur. De beheerder en/of het College van Bestuur legt het betreffende verzoek voorafgaand aan zijn akkoord ter beoordeling voor aan Juridische Zaken of de Functionaris Gegevensbescherming en de stafmedewerker(s) integrale veiligheid.

5 Wanneer de rechtsgeldigheid van de vordering is vastgesteld en de beheerder en/of het College van Bestuur toestemming heeft gegeven, mag de beeldinformatie op een digitaal medium aan de politie, rechter-commissaris of de Officier van Justitie worden verstrekt conform de procedure als vermeld in artikel 5 van het reglement.

6 Bij twijfel aan de rechtsgeldigheid van de vordering of bij het ontbreken van de schriftelijke vordering, kunnen de beelden door de locatiebeheerder veiliggesteld worden en mogen de beelden niet verstrekt worden aan de politie, rechter-commissaris of Officier van Justitie.

7 Als de politie, rechter-commissaris of Officier van Justitie niet binnen 4 weken na het oorspronkelijke verzoek tot uitgifte van de beelden een rechtmatige schriftelijke vordering overlegt, dan worden de beelden vernietigd.

8 Inzage door derden geschiedt uitsluitend met toestemming van het College van Bestuur en met uitdrukkelijke toestemming van de betrokken personen die op beeld zijn vastgelegd. Met derden worden andere personen dan de politie, rechter-commissaris of de Officier van Justitie en de in artikel 3, lid 6 genoemde personen bedoeld. Hierbij valt te denken aan bijvoorbeeld leerlingen, studenten en ouders.

9 Het College van Bestuur legt het betreffende verzoek voorafgaand aan zijn akkoord ter beoordeling voor aan Juridische Zaken of de Functionaris Gegevensbescherming en de stafmedewerker(s) integrale veiligheid.

10 Het College van Bestuur wordt schriftelijk door de beheerder geïnformeerd over de vorenbedoelde inzage.

11 Als camerabeelden worden ingezien, veiliggesteld c.q. uitgegeven worden, dan wordt de stafmedewerker integrale veiligheid direct telefonisch geïnformeerd. De melder zal tevens per mail alle uitgevoerde activiteiten melden aan de stafmedewerker integrale veiligheid. De stafmedewerker integrale veiligheid maakt vervolgens melding in het incidentenregistratiesysteem.

Artikel 6 Informatie over cameratoezicht

De beheerder moet ervoor zorgen dat de leerlingen, studenten, medewerkers en bezoekers weten dat er een camera hangt. Bijvoorbeeld door bordjes bij iedere ingang op te hangen, het reglement cameratoezicht Yonder publiek beschikbaar te stellen en op bijvoorbeeld de website of in de studiegids beknopt uit te leggen dat er gebruik wordt gemaakt van cameratoezicht.

Artikel 7 Het plaatsen en gebruik van heimelijk cameratoezicht

12 Het plaatsen van heimelijke camera's is in beginsel verboden. Slechts in bijzondere gevallen is dit toegestaan en alleen na de specifieke en voorafgaande schriftelijke toestemming van het College van Bestuur.

13 Het College van Bestuur legt de aanvraag voor heimelijk cameratoezicht voorafgaand aan zijn akkoord ter beoordeling voor aan Juridische Zaken én de Functionaris Gegevensbescherming. Juridische Zaken en de Functionaris Gegevensbescherming zullen een dergelijk verzoek beoordelen aan de criteria van artikel 7 van het reglement cameratoezicht Yonder. Tevens is de Functionaris Gegevensbescherming bevoegd om eerst toestemming te vragen aan de Autoriteit Persoonsgegevens om heimelijk cameratoezicht toe te mogen passen.

Artikel 8 Rapportage

De stafmedewerker integrale veiligheid rapporteert minimaal 1 keer per jaar aan de beheerder in ieder geval over de volgende zaken:

- Het toegepaste cameratoezicht;
- Aanvraag camera's;
- Uitbreiden cameratoezicht;
- Terugkijken van beelden;
- Verstrekken van beelden.