Limburgs Voortgezet Onderwijs

Horizon 2025 - onderwijs vanuit waarderend perspectief

Reglement cameratoezicht Stichting LVO

Versie 31 januari 2024

Inleiding

Wij staan voor een professionele en veilige omgeving waar alle medewerkers hun kennis en kunde inzetten om het best denkbare onderwijs te realiseren. Bij het aanbieden van het onderwijs verwerken wij ook persoonsgegevens. Dit willen wij op een transparante en veilige manier doen. We zien het dan ook als onze verantwoordelijkheid om uiterst zorgvuldig om te gaan met de persoonsgegevens van leerlingen, ouders, medewerkers en andere personen die betrokken zijn bij het onderwijs dat wij aanbieden.

In dit reglement cameratoezicht – dat betrekking heeft op alle locaties van Stichting LVO waar toezicht door middel van camerasystemen wordt ingezet – wordt een beschrijving gegeven van taken, verantwoordelijkheden en procedures over het cameratoezicht en het gebruik en delen van camerabeelden. Hiermee wordt voldaan aan de wet- en regelgeving zoals de Algemene Verordening Gegevensbescherming (AVG) maar het reglement draagt ook bij aan het creëren van een veilige omgeving voor zowel leerlingen, medewerkers als bezoekers.

Het reglement cameratoezicht van Stichting LVO kent de volgende uitgangspunten:

1. AVG-grondslagen
   Op grond van de AVG zijn er een aantal redenen/grondslagen op basis waarvan cameratoezicht op een school gerealiseerd kan worden.
2. De privacyverklaring van LVO
   In de LVO-privacyverklaring (zie link hieronder) worden de AVG-grondslagen ook expliciet genoemd, zoals bijvoorbeeld de plicht om een veilige schoolomgeving te creëren waarbij de veiligheid van zowel leerlingen als medewerkers zoveel mogelijk wordt bewaakt.
   https://www.stichtinglvo.nl/privacyverklaring-lvo/
3. Het privacyreglement van LVO
   In het privacyreglement van LVO (zie link hieronder) komt het cameratoezicht ook aan bod.
   https://www.stichtinglvo.nl/de-organisatie/privacy/
4. Het voorbeeldreglement over cameratoezicht van kennisnet
   https://aanpakibp.kennisnet.nl/beveiligingscameras/

Privacytoets of Data Protection Impact Assessment (DPIA)

Het uitvoeren van een DPIA is volgens de Autoriteit Persoonsgegevens (AP) verplicht als een organisatie cameratoezicht wil inzetten. In bijlage 1 is een voorbeeld DPIA opgenomen (vragenlijst) die door de school kan worden gebruikt als cameratoezicht wordt toegepast op onderstaande locaties:

a. Ingangen schoolterrein;
b. Schoolplein inclusief fietsenstalling;
c. Ingangen schoolgebouw;
d. Gemeenschappelijke ruimtes zoals de aula, gangen, pauzeplaatsen of kantines;
e. Trappenhuizen en liften;
f. Garderobe en/of de ruimtes waar kluisjes zijn.

De school dient deze privacytoets/vragenlijst te controleren op correctheid.
Voor andere locaties dan hiervoor vermeld dient de school de privacytoets/vragenlijst nog zelf in te vullen.
Het reglement cameratoezicht is van toepassing op alle scholen van onze organisatie.

Het reglement cameratoezicht werd, na instemming van de gmr, vastgesteld door het college van bestuur van de Stichting LVO in de vergadering d.d. 31 januari 2024.

Artikel 1 – Begripsbepalingen

1. In dit reglement wordt verstaan onder:

a. *Privacytoets:* Op basis van een vragenlijst wordt afgewogen of de mate van inbreuk op de privacy van de leerlingen, medewerkers en bezoekers proportioneel is t.o.v. het belang van de onderwijsinstelling om cameratoezicht te gebruiken. Hierbij wordt meegewogen of de doelstellingen op basis waarvan cameratoezicht wordt overwogen op een andere wijze kunnen worden bereikt, met een minder ingrijpend middel dan cameratoezicht.
b. *Cameratoezicht*: toezicht met behulp van camera's, waardoor er sprake is van verwerking van persoonsgegevens als bedoeld in artikel 5 lid 2 van de Algemene Verordening Gegevensbescherming (AVG).
c. *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.
d. *Serverruimte*: de van een toegangscontrolesysteem voorziene ruimte, waar de server of opnameapparatuur staat waarop de opgenomen camerabeelden geregistreerd staan.
e. *Camerasysteem*: het geheel van camera's, monitoren, opnameapparatuur, verbindingskasten en verbindingen waarmee het cameratoezicht wordt uitgevoerd.
f. *Camera-observatieruimte*: een centraal gesitueerde, van een toegangscontrolesysteem voorziene ruimte, waarin de camerabeelden - van een of meerdere 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.
g. *Camerabeeld*: het door het cameratoezicht verkregen camerabeeld.
h. *Beheerder*: de schoolleiding die namens het college van bestuur van Stichting LVO verantwoordelijk is voor de inrichting, het beheer en de controle op het cameratoezicht.
i. *Locatiebeheerder*: een door de beheerder als zodanig aangewezen persoon die belast is met het cameratoezicht op één of meerdere locaties van Stichting LVO.
j. *Technisch beheerder*: de (bedrijfs)functionaris die, onder verantwoordelijkheid van de beheerder, belast is met het technisch beheer van het camerasysteem.
k. *Bevoegde medewerker*: een door de beheerder [in geval van cameratoezicht op meerdere locaties: de locatiebeheerder] als zodanig aangewezen persoon die betrokken is bij de uitvoering van het cameratoezicht.
l. *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 LVO.
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 zodat diefstal en vernieling van die zaken voorkomen wordt;
   d. het vastleggen van incidenten, zoals opstootjes, vechtpartijen en ongewenst grensoverschrijdend gedrag.
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 de schoolleiding een privacytoets uit. 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. De schoolleiding selecteert volgens de geldende regels een leverancier die een conceptcontract en een conceptverwerkersovereenkomst opstelt.
4. De schoolleiding legt het voorstel tot het inzetten van cameratoezicht op een bepaalde locatie - samen met de privacytoets, het conceptcontract en de conceptverwerkersovereenkomst - voor aan de medezeggenschapsraad (mr).
5. De schoolleiding wijst een beheerder aan die verantwoordelijk is voor de inrichting, het beheer en toezicht op het cameratoezicht binnen de onderwijsinstelling, alsmede een technische (bedrijfs)beheerder die, onder verantwoordelijkheid van de beheerder, belast is met het technisch beheer van het camerasysteem.
6. De beheerder wijst bevoegde medewerkers aan, en zo nodig een of meer locatiebeheerder(s). Deze medewerkers hebben kennis (door training en/of instructie) over het bekijken en terugkijken van camerabeelden. Hierbij dient interne en externe geheimhouding te worden betracht.
7. De beheerder wijst voor zichzelf en voor de locatiebeheerder een plaatsvervanger aan, die in geval van afwezigheid van de beheerder respectievelijk locatiebeheerder in diens taken en verantwoordelijkheden treedt.
8. De beheerder, locatiebeheerder(s) en bevoegde medewerkers zijn bevoegd tot het live uitkijken van camerabeelden.
9. De beheerder en locatiebeheerder zijn bevoegd tot het terugkijken en uitgeven van opgenomen camerabeelden.
10. De beheerder en locatiebeheerder kunnen een bevoegde medewerker autoriseren om onder verantwoordelijkheid van de beheerder of locatiebeheerder - onder nader te stellen voorwaarden en voor een vooraf bepaald doel c.q. een vooraf bepaalde periode camerabeelden terug te kijken.

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 de directie van de school uitgevoerde privacytoets 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, de serverruimte en camera-observatieruimte.
3. Het terugkijken van opgenomen camerabeelden geschiedt slechts in aanwezigheid van tenminste twee daartoe bevoegd verklaarde medewerkers, en alleen indien hiertoe aanleiding is, gekoppeld aan de doelstellingen zoals genoemd in artikel 2 lid 2. Dit geldt ook ingeval van gebruikmaking van het inzagerecht (zie artikel 5 en 6).
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

daartoe een geheimhoudingsverklaring met de locatiebeheerder(s), technisch beheerder en/of bevoegde medewerker(s).

5. De beheerder 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, zoals maar niet beperkt tot signaleringsborden en stickers bij de ingang van de gebouwen of terreinen van de onderwijsinstelling, waar cameratoezicht plaatsvindt.
6. 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. Dit wordt voorgelegd aan de directie van de school die hierover een besluit neemt dat wordt vastgelegd inclusief de argumentatie tot het bewaren van de gegevens. Na afhandeling van het incident worden de betreffende camerabeelden (en eventueel gemaakte kopieën of afdrukken) gewist.
7. Het camerasysteem is zodanig uitgerust dat het terugkijken van opgenomen camerabeelden of het uitgeven daarvan slechts mogelijk is in de camera-observatieruimte.
8. 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.
9. 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.
10. 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 van het incident (of daaraan gerelateerd) in het kader van de uitoefening van diens publiekrechtelijke taak, alleen indien er een gerechtelijk bevel kan worden overlegd.
2. Uitgifte van camerabeelden van het incident (of daaraan gerelateerd) 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, toont het rechtelijk bevel ten overstaan van de beheerder of locatiebeheerder, en tekent voor ontvangst van de uitgegeven camerabeelden van het incident (of daaraan gerelateerd).
4. De inzage en uitgifte wordt door de beheerder of locatiebeheerder geregistreerd.
5. Aan andere derden wordt geen inzage in de camerabeelden van het incident (of daaraan gerelateerd) gegeven of 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 AVG. Hieronder vallen het recht op informatie, 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.
3. Het verzoek tot inzage wordt afgewezen wanneer het verzoek tot inzage in camerabeelden ongespecificeerd is, 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 voorkoming, opsporing en vervolging van strafbare feiten.
5. Klachten over de toepassing van het camerasysteem, dit reglement en over het gedrag van de beheerder, locatiebeheerder of de bevoegde medewerkers, worden schriftelijk ingediend bij het college van bestuur. Het college van bestuur zal binnen 6 weken na datum ontvangst van de klacht reageren.

Artikel 7 – Heimelijk cameratoezicht

1. Heimelijk cameratoezicht is slechts toegestaan indien regulier cameratoezicht en andere door Stichting LVO 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 college van bestuur onder vermelding van de voorwaarden waaronder het heimelijk cameratoezicht plaatsvindt.
4. Voordat heimelijk cameratoezicht wordt toegepast, meldt het college van bestuur haar voornemen bij de AP. Er wordt niet eerder aangevangen met heimelijk toezicht dan na instemming daarmee van de AP.
5. De schoolleiding informeert namens het college van bestuur – voor zover redelijkerwijs mogelijk - achteraf de betrokken leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers over het toegepaste heimelijk cameratoezicht.

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 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 college van bestuur stelt dit reglement vast. Voorafgaand aan het vaststellen, wijzigen of intrekken van dit reglement cameratoezicht, vraagt het college van bestuur de gmr om instemming.
2. Het college van bestuur informeert, indien aanwezig, de leerlingenraad over het vaststellen, wijzigen of intrekken van dit reglement.
3. Het reglement cameratoezicht Stichting LVO treedt in werking met ingang van 31 januari 2024.
   Een wijziging in dit reglement treedt in werking binnen 30 dagen na bekendmaking van de wijziging.
4. In situaties waarin dit reglement niet voorziet, beslist het college van bestuur.

Bijlage 1: Addendum: Privacytoets

Bron: IBP – Kennisnet.
Bewerkt namens Stichting LVO door kernteam IB&P.

Stichting LVO heeft de privacytoets uitgevoerd aan de hand van onderstaande checklist Data Protection Impact Assessment (DPIA). In goed Nederlands heet dit Gegevensbeschermingseffectbeoordeling. Dit betekent dat de school de belangen van de leerlingen, medewerkers en bezoekers heeft afgewogen tegen de andere belangen die er zijn. Deze toets geeft inzicht in het zogeheten gerechtvaardigd belang, doel en doelbinding, en noodzaak van cameratoezicht.

Onderstaande tabel geeft een eerste inzage in de privacy impact van cameratoezicht. Indien u tot andere antwoorden komt dan in de tabel is aangegeven dan is het raadzaam afstemming te zoeken met het kernteam IB&P (Informatiebeveiliging & privacy) van LVO.

Onderstaande voor ingevulde privacytoets / Data privacy Impact Assessment (DPIA) is alleen van toepassing voor camera's die geplaatst zijn in:

- Ingangen schoolterrein (geef ook de ingangen weer waar geen camera hangt*);
- Schoolplein inclusief fietsenstalling;
- Ingangen schoolgebouw (geef ook de ingangen weer waar geen camera hangt*);
- Gemeenschappelijk ruimtes zoals aula, hallen of kantine;
- Trappenhuizen en liften (geef ook de trappenhuizen en liften aan waar geen camera hangt*);
- Garderobe/ruimtes met kluisjes.

Indien op andere locaties camera's worden opgehangen dan dient onderstaande privacytoets volledig opnieuw te worden ingevuld.

	Vraag	Ja	Nee
0	Met welk doel worden camera's op deze plaatsen opgehangen?		
1.	Is er sprake van een nieuwe verwerking (worden er camera's toegevoegd en/of worden camera's geplaatst op andere locatie dan voorheen) of een nieuwe manier van de verwerking van persoonsgegevens (bijvoorbeeld een nieuwe applicatie om camera beelden terug te kijken en/of te zoeken of nieuwe techniek van camera's)?	Ja	
2.	Is de verwerking van camerabeelden en het opnemen van gebeurtenissen met behulp van camera's voor de betreffende type locatie in en/of rondom de school nog niet opgenomen in een verwerkings- of dataregister?	Ja	
3.	Zijn de te verwerken persoonsgegevens, het systeem of de applicatie waarmee de verwerking plaatsvindt geclassificeerd (hebben ze een BIV waarde)? Zie hieronder **B**eschikbaarheid Hoog Te allen tijde wil je in staat zijn om direct te handelen indien de veiligheid van personen in gevaar komt. Te allen tijde wil je beelden kunnen terugkijken - en geen tijdsloten missen - om vandalisme te kunnen achterhalen. **I**ntegriteit Hoog Beelden mogen niet gemanipuleerd / gewijzigd worden. Beelden moeten 100% betrouwbaar zijn in de zin dat onweerlegbaar een gebeurtenis kan worden aangetoond. **V**ertrouwelijkheid Beelden mogen slechts in zeer bijzonder gevallen gedeeld worden met andere partijen. Beelden zijn alleen maar beschikbaar voor de personen die aangesteld zijn om het systeem te gebruiken en voor de schoolleiding indien er gerede aanwijzing is dat zich een incident heeft voorgedaan.	Ja	
4.	Past de nieuwe verwerking bij de verwerkingsdoeleinden van de school? Zie privacyreglement en privacyverklaring van LVO	Ja	
5.	Is er een grondslag voor de nieuwe verwerking? Creëren van een veilige fysieke omgeving voor iedereen.	Ja	
6.	Kun je aantonen dat je alleen de meest noodzakelijke gegevens vastlegt? Geef aan hoe?	Ja	
7.	Kun je aantonen dat je de gegevens op geen enkele andere manier kunt verkrijgen, die minder inbreuk doet op de privacy van individuen en die niet minder zorgvuldig, veilig en gecontroleerd plaatsvindt? Dat laatste zorgt ervoor dat opnames op de mobiele telefoon van de conciërge geen alternatief zijn.	Ja	
8.	Worden er andere persoonsgegevens vastgelegd dan tot nu toe? Alleen Ja als er nog helemaal geen Cameratoezicht is op de school. Indien Ja dan zal zeker het voorstel tot cameratoezicht met de mr besproken moeten worden, maar ook als antwoord Nee is betrek altijd de mr.	Ja	
9.	Worden er geen bijzondere persoonsgegevens over betrokkenen verwerkt?	Ja	
10.	Wordt er informatie verwerkt over kwetsbare personen? (Leerlingen onder 16 jaar)	Ja	

11.	Worden er met andere partijen dan tot nu toe persoonsgegevens uitgewisseld? Geef aan met welke partijen en in welke omstandigheden onder welke voorwaarden (zie hiervoor dit reglement en bijbehorende handleiding). Minimaliseer het aantal partijen en laat nooit beelden aan leerlingen en ouders zien en hou rekening met privacy van slachtoffer en dader.	Ja	
12.	Krijgen er meer of andere partijen toegang tot verwerkingen van persoonsgegevens? Indien er nog geen cameratoezicht is, is antwoord hierop Ja omdat in bijzondere gevallen politie en justitie toegang kunnen krijgen tot de camerabeelden.	Ja	
13.	Worden er geautomatiseerd beslissingen genomen over betrokkenen op basis van persoonsgegevens?		Nee
14.	Is het mogelijk om op basis van de persoonsgegevens gedrag, prestaties of aanwezigheid van betrokkenen in kaart te brengen of te beoordelen?	Ja	
15.	Geeft de verwerking de mogelijkheid tot inzage door de betrokkenen? Alleen in bijzondere omstandigheden als er een incident is en het onderzoek plaatsvindt door daartoe gemachtigde personen.		Nee
16.	Geeft de verwerking de mogelijkheid tot correctie voor de betrokkenen?		Nee
17.	Geeft de verwerking de mogelijkheid tot het wissen van persoonsgegevens (vergetelheid) voor de betrokkenen? Geef altijd aan hoe lang camerabeelden bewaard worden in het algemeen en hoe lang beelden worden bewaard die een incident weergeven waar een onderzoek voor is uitgevoerd. Beelden wissen op verzoek van een betrokkene zal vanzelf gebeuren als een redelijke termijn van bewaren wordt gehanteerd voor algemene beelden welke niet gekoppeld zijn aan incident van bijv. max 4 weken.		Nee
18.	Geeft de verwerking de mogelijkheid tot overbrenging van de gegevens naar een ander systeem (dataportabiliteit)? Het kan zijn dat fragmenten van een opname op een locatie in of rondom de school gedeeld moeten worden met politie en justitie, dan worden deze op een beveiligde - door de betreffende instantie aangereikte - gegevensdrager geplaatst.	Ja	
19.	Is duidelijk wat de bewaartermijn van de gegevens is? Indien Ja Geef aan hoeveel weken en wat de bewaartermijn is van beelden die een incident weergeven waar onderzoek voor nodig is.	Ja	
20.	Vindt logging en monitoring plaats op de verwerking? Hier wordt bedoeld dat de werking van de camera's en het camerasysteem continu wordt gecheckt op beschikbaarheid en de juiste werking maar ook dat wijzigingen die aan de camera's en/of systeem plaatsvinden automatisch worden vastgelegd in een logbestand zodat altijd nagegaan kan worden wie welke wijzigingen heeft uitgevoerd (denk bijv. aan weggooien van beelden).	Ja	
21	Wordt de toegang tot het systeem en de camera's beperkt middels Role based Access. Dat wil zeggen dat medewerkers afhankelijk van hun rol m.b.t. het gebruik en beheer van het systeem toegang krijgen tot slechts een beperkt aantal functies in het systeem en dat het aantal personen dat toegang tot het systeem krijgt ook beperkt is en dat toegang tot beelden alleen mogelijk is via een mutificator authenticatie en/of via een sleutel om in de afgesloten ruimte te komen waar de beelden worden getoond.	Ja	
22.	Is geregeld hoe om te gaan met een datalek? Altijd melden bij kernteam.	Ja	

	Dat wil zeggen ongeautoriseerde personen die geen toegang tot de beelden zouden mogen hebben, hebben toch toegang verkregen tot de afgesloten ruimte waar de beelden worden getoond of hebben toegang tot de camera's en het camera systeem.		
23.	Wordt de beveiliging van de persoonsgegevens duidelijk vastgelegd? Met andere woorden is er een ontwerp waarin staat welke beveiligingsmaatregelen geïmplementeerd moeten zijn om misbruik van camera's en camerabeelden zoveel mogelijk te voorkomen. Voldoen deze aan de eisen van de huidige stand van de techniek (bijvoorbeeld 2 factor authenticatie)? Zijn er processen en instructies hoe verantwoordelijke medewerkers met de gegevens om moeten gaan?	Ja	
24.	Als de verwerking bij een andere partij plaatsvindt, is deze aangesloten bij het privacyconvenant?	Ja	
25.	Voldoet de andere partij aan de beveiligingseisen die in het privacyconvenant zijn vastgelegd en zijn deze vastgelegd in een verwerkersovereenkomst?	Ja	