

CENTRALE DPIA

Cameratoezicht

Colofon

DPIA uitgevoerd door:	Coöperatie Samen Innoveren/Inkopen/ICT voor Onderwijs Nederland U.A. (SIVON) www.sivon.nl info@sivon.nl
Auteurs van deze DPIA:	Dimitri Wouters (privacy professional en lead IBP adviseur - SIVON) Ashley Hoogendoorn (jurist en support IBP adviseur - SIVON) Job Vos (jurist en sr. adviseur IBP - SIVON)
Met dank aan:	Stichting Onderwijscentrum Leijpark - Tilburg Stichting Openbaar Verenigd Onderwijs - Gorinchem Stichting Katholiek Onderwijs Volendam
Auteurs model DPIA (v2.5):	Dimitri Wouters (privacy professional en lead IBP adviseur - SIVON) Job Vos (jurist en sr. adviseur IBP - SIVON) IBP team SIVON

Deze DPIA is gebaseerd op de *Model DPIA Rijksdienst versie 3.0* en de voormalige *Handleiding uitvoeren data protection impact assessment (DPIA) voor het po en vo (1.0)*.

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden SIVON en de auteur(s) geen aansprakelijkheid voor eventuele fouten, onvolkomenheden of schade als gevolg van het gebruik van dit document. Deze DPIA helpt schoolbesturen als verwerkingsverantwoordelijke om zelf een DPIA uit te voeren en een oordeel te vormen over risico's voor de rechten en vrijheden van betrokkenen. Consulteer bij twijfel een in privacy gespecialiseerde specialist, jurist of advocaat voor advies over de toepassing van DPIA voor uw eigen organisatie.

Versiebeheer

Datum	Versie	Wijziging
Oktober 2026	1.0	Definitieve versie voor publicatie



De gebruiker is in het kader van deze publicatie vrij om:

- **Delen** - het materiaal te kopiëren, te verspreiden en door te geven via elk medium of bestandsformaat voor alle doeleinden, inclusief commerciële doeleinden.
- **Bewerken** - te remixen, te veranderen en afgeleide werken te maken voor alle doeleinden, inclusief commerciële doeleinden.

Onder de volgende voorwaarden:

- **Naamsvermelding** - De gebruiker dient:
 - de maker van het werk te vermelden¹: SIVON de “Coöperatie Samen Innoveren/Inkopen/ICT voor Onderwijs Nederland U.A. en de namen van de betrokken auteurs van de DPIA
 - een link naar de licentie te plaatsen
 - aan te geven of het werk veranderd² is.

Je mag dat op redelijke wijze doen, maar niet zodanig dat de indruk gewekt wordt dat de licentiegever instemt met je werk of je gebruik van het werk.

- **Geen aanvullende restricties** - Je mag geen juridische voorwaarden of technologische voorzieningen³ toepassen die anderen er juridisch in beperken om iets te doen wat de licentie toestaat

¹ Wanneer beschikbaar is het verplicht om de naam van de maker en andere rechthebbenden, een auteursrechtenvermelding, de toepasselijke licentie, een disclaimer en een link naar het materiaal te vermelden.

² In 4.0 moet je aangeven of je materiaal gewijzigd hebt en een vermelding van vorige versies bijhouden.

³ De licentie staat niet toe dat er effectieve technologische voorzieningen ingezet worden, zoals gedefinieerd in artikel 11 van het WIPO Auteursrecht Verdrag.

Inhoudsopgave

1. Leeswijzer	6
2. Managementsamenvatting	7
3. Uitleg en achtergrond DPIA	9
1. Informatiebeveiliging en privacy (IBP)	9
2. Privacyconvenant en toetsing verwerkersovereenkomsten.....	9
3. DPIA	9
4. Verplichte uitvoering DPIA	10
5. Centrale en lokale DPIA.....	10
6. Methodiek DPIA.....	11
7. Toepassing op cameratoezicht	12
8. Funderend onderwijs referentie architectuur (FORA)	12
4. Motivering DPIA Cameratoezicht	13
1. Verplichting uitvoeren DPIA	13
2. Scope van deze DPIA	13
3. Buiten scope	14
4. Aandachtspunten.....	14
5. Deel A: Gegevensverwerkingsanalyse	16
1. Beschrijving van het gegevensverwerkende proces.....	16
2. Persoonsgegevens.....	18
3. Gegevensverwerkingen.....	19
4. Verwerkingsdoeleinden	24
5. Betrokken partijen	26
6. Belangen bij de gegevensverwerking.....	27
7. Verwerkingslocaties	27
8. Data Transfer Impact Assessment (DTIA)	28
9. Technieken en methoden van gegevensverwerking	28
a. Technisch onderzoek.....	28
b. ROSA-certificeringsschema en BIV-classificatie	29
c. Algoritmes en AI	29
d. Bevindingen.....	29
10. Juridisch en beleidsmatig kader	29
11. Bewaartermijnen	31
6. Deel B: Beoordeling rechtmatigheid gegevensverwerkingen	33
12. Rechtsgrond	33
13. Bijzondere persoonsgegevens.....	35

14. Doelbinding.....	35
15. Kinderrechten-afweging (Best Interests Assessment Children)	36
16. Noodzakelijkheid.....	38
17. Proportionaliteit en subsidiariteit	38
18. Rechten van de betrokkenen	41
19. Beoordeling verwerkersovereenkomst	44
7. Deel C: Beschrijving en beoordeling risico's voor de betrokkenen	45
Beoordelingskader risico's	45
20. Risico's.....	46
8. Deel D: Beschrijving voorgenomen maatregelen	56
Beoordelingskader maatregelen.....	56
21. Maatregelen.....	56
9. Deel E: MODEL lokale DPIA	74
Lokale Management Samenvatting.....	74
A. Uitvoering lokale DPIA	75
B. Overwegingen centrale DPIA, lokaal maken	75
C. Overwegingen lokale DPIA, aanvullende risico's en maatregelen	98
D. Verklaring en advies functionaris voor gegevensbescherming (FG)	99
E. Raadplegen betrokkenen	99
F. Conclusie	100
G. Risico-mitigerende maatregelen schoolbestuur.....	100
H. Verklaring schoolbestuur.....	100
10. Bijlagen	102
Bijlage 1: Gebruikte termen en definities	102
Bijlage 2: Instructies voor het uitvoeren van de lokale DPIA	104
Bijlage 3: Vragenlijst vaststellen risico's en getroffen maatregelen	104
Bijlage 4: Cameraoverzicht.....	104
Bijlage 5: Voorbeeldborden cameratoezicht die aan de eisen van de EDPB voldoen	104

1. Leeswijzer

Dit DPIA-rapport bestaat uit de volgende opbouw en hoofdstukken.

Inleiding

- Hoofdstuk 1: betreft deze leeswijzer.
- Hoofdstuk 2: betreft de samenvatting van de uitkomsten van deze DPIA voor interne communicatiedoeleinden (Bestuur, GMR, betrokkenen).
- Hoofdstuk 3: betreft een algemene uitleg over wat een DPIA is, wanneer deze verplicht is, wat het gevolgde model is en wat de door SIVON gevolgde methodiek is.
- Hoofdstuk 4: beschrijft de verwerking waarop deze DPIA ziet en wat er wel en niet meegenomen is in het onderzoek (scope en buiten scope).

Centrale DPIA

- Hoofdstuk 5: deel A bevat de gegevensverwerkingsanalyse (beschrijving van de gegevensverwerkingen).
- Hoofdstuk 6: deel B bevat de beoordeling van de rechtmatigheid van de gegevensverwerkingen.
- Hoofdstuk 7: deel C bevat de beschrijving en beoordeling van de risico's.
- Hoofdstuk 8: deel D bevat de beschrijving van de voorgenomen maatregelen die de gevonden risico's beperken.

Lokale DPIA

- Hoofdstuk 9: deel E is het model "lokale DPIA" die schoolbesturen gebruiken voor het zelf uitvoeren van deze DPIA binnen hun eigen organisatie. Deel E begint met de lokale managementsamenvatting. Gebruik hierbij het instructieblad (Bijlage 2).

Bijlagen

- Bijlage 1 bevat veelgebruikte termen en definities
- Bijlage 2 bevat het instructieblad voor het uitvoeren van de lokale DPIA, met een toelichting en per onderdeel van Deel E een instructie
- Bijlage 3 bevat de vragenlijst bij het uitvoeren van de DPIA
- Bijlage 4 bevat de verwijzing naar het cameraoverzicht
- Bijlage 5 bevat voorbeeldborden cameratoezicht die aan de eisen van de EDPB voldoen

! Instructie

Bij dit rapport hoort een apart instructieblad (Bijlage 2). Dit instructieblad is een zeer belangrijk hulpmiddel om het uitvoeren van de lokale DPIA makkelijker te maken. Lees het daarom aan het begin, voordat met de lokale DPIA wordt gestart. Het bevat een praktische toelichting op het uitvoeren van de lokale DPIA: waarom een centrale én een lokale DPIA, wat centraal al is gedaan en wat het schoolbestuur zelf doet, wat vooraf nodig is, wie erbij wordt betrokken, hoeveel tijd het ongeveer kost en in welke stappen de DPIA wordt uitgevoerd. Daarnaast bevat het per onderdeel van Deel E (hoofdstuk 9) een instructie, die bij het invullen naast dit rapport wordt gebruikt.

2. Managementsamenvatting

Op basis van het uitgevoerde onderzoek in het kader van de DPIA voor cameratoezicht is de conclusie dat de verwerking van persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen.

Cameratoezicht op schoolterreinen en in schoolgebouwen wordt uitsluitend ingezet als laatste redmiddel, nadat minder ingrijpende maatregelen onvoldoende effect hebben gehad. De inzet is gericht op het tegengaan van vandalisme, inbraak, diefstal en ongeregelde heden en op de bescherming van medewerkers, leerlingen en bezoekers. Wanneer de toepassing zorgvuldig is afgewogen op basis van proportionaliteit en subsidiariteit en beperkt blijft tot locaties en momenten met het hoogste risico, is cameratoezicht een gerechtvaardigde maatregel.

Wanneer alle in deze DPIA voorgestelde maatregelen worden doorgevoerd en geborgd, resteert geen hoog risico: het restrisico is voor alle 36 geïdentificeerde risico's laag of zeer laag. In dat geval is een voorafgaande raadpleging van de Autoriteit Persoonsgegevens (artikel 36 AVG) niet nodig. Onderstaand overzicht brengt de risico's samen in tien risicogebieden.

1. Onrechtmatige of ondoelmatige verwerking

Camera's gericht op de openbare ruimte buiten de eigendomsgrens, inzet buiten de vastgestelde doeleinden, gebruik van niet-toegestane opnametechnieken zoals AI-gestuurde gezichtsherkenning of geluidsoptname, het ontbreken van een aantoonbare doelbinding per camera, het buiten het wijzigingsproces om verplaatsen van losse camera's, waardoor deze zonder herbeoordeling op een andere locatie of een specifieke persoon kunnen worden gericht, het door medewerkers buiten het systeem vastleggen van beelden, of niet-noodzakelijke camerafuncties die niet zijn uitgeschakeld.

2. Onvoldoende technische en fysieke beveiliging

Geen netwerksegmentatie, ontbrekende versleuteling van beeldtransport, geen of onvoldoende authenticatie (MFA of wachtwoorden van minimaal 15 tekens) en achterstanden in beveiligingsupdates verhogen de kans op beveiligingsincidenten en datalekken aanzienlijk. Daarnaast kunnen beelden via een app, laptop of tablet ook buiten het schoolgebouw toegankelijk zijn. Dit vergroot het aanvalsoppervlak en vereist aangescherpte infrastructuurbeveiliging, zoals de beperking van online beelden tot beheerde apparaten. Ook een niet of onvoldoende afgesloten technische ruimte, waarin recorder en switches voor onbevoegden bereikbaar zijn, maakt ongeautoriseerde toegang tot het camerasysteem mogelijk.

3. Ongereguleerde bewaartermijnen en opslag van incidentbeelden

Het ontbreken van een technisch ingestelde bewaartermijn voor reguliere opnames, met automatische overschrijving na standaard drie weken (gemotiveerd maximaal vier weken, tijdens de zomervakantie maximaal zes weken), vormt een structureel risico. Daarnaast ontbreken bij veel schoolbesturen heldere richtlijnen voor het bewaren van beelden van incidenten: wanneer dit is toegestaan, hoe lang beelden worden bewaard, waar ze worden opgeslagen en op welk moment ze worden verwijderd. Bij cloudopslag ontbreekt bovendien geregeld een verwerkersovereenkomst.

4. Gebrek aan transparantie richting betrokkenen

Ontbrekende of onvoldoende zichtbare bebording, het niet opnemen van cameratoezicht in de privacyverklaring en een reglement cameratoezicht dat niet vindbaar of niet actueel is voor leerlingen, ouders, medewerkers en bezoekers. Ook wanneer in de huurovereenkomst niet is vastgelegd dat huurders hun gebruikers namens het schoolbestuur informeren over het cameratoezicht, bereikt de informatie deze betrokkenen niet.

5. Ontbrekend of onvolledig reglement cameratoezicht

Geen vastgesteld reglement, of een reglement dat niet voldoet aan de AVG-minimumvereisten, niet is goedgekeurd door de (G)MR, de rechten van betrokkenen niet beschrijft, niet bekend is bij de betrokken medewerkers en stakeholders, of waarvan de naleving niet wordt gecontroleerd.

6. Onjuiste of ongecontroleerde toegang tot beelden

Er is geen bovenschoolse autorisatiematrix, er wordt gewerkt met gedeelde accounts, het accountbeheer is niet gekoppeld aan HR-processen en het vier-ogenprincipe wordt niet toegepast bij het terugkijken, bewaren of delen van beelden. Evenmin is vastgelegd in welke situaties beelden teruggekeken mogen worden. Daarnaast ontbreken bij veel schoolbesturen richtlijnen voor het live bekijken van beelden (wie, met welk account en vanuit een ruimte die is afgeschermd voor omstanders) en voor het terugkijken op afstand buiten Schooltijd, dat beperkt hoort te blijven tot calamiteiten. Ook ontbreekt vaak zicht op Structurele toegang tot het systeem door een externe onderhoudspartij.

7. Onvoldoende registratie en logging

Het ontbreken van adequate systeemlogging (audittrail) én van logboeken voor wijzigingen aan camera-instellingen, afwijkingen van het reglement en het gebruik van beeldmateriaal, maakt toezicht op het gebruik van het camerasysteem onmogelijk en incidentonderzoek onuitvoerbaar. Ook wanneer logging wel aanwezig is, blijft onrechtmatige inzage onopgemerkt als de logging niet periodiek en naar aanleiding van incidenten wordt gecontroleerd.

8. Onvoldoende organisatorisch eigenaarschap en beheer

Het ontbreken van een aangewezen proces- en systeemeigenaar op bestuursniveau, onduidelijke verantwoordelijkheden voor onderhoud, een ontbrekende verwerkersovereenkomst met een externe onderhoudspartij met Structurele toegang en het ontbreken van een incidentresponsproces specifiek voor het camerasysteem, maken beheer en controle onvoldoende. Een niet-gecentraliseerde inkoop, ook wanneer camera's bij nieuwbouw via het bestek van de bouwaanbesteding worden meegenomen, leidt tot uiteenlopende systemen en leveranciers met elk een eigen beveiligingsniveau en updatebeleid, die moeilijk uniform te beheren en te beveiligen zijn. Zonder vooraf vastgestelde technische en organisatorische inkoop-eisen kan bovendien pas na ingebruikname blijken dat een systeem de noodzakelijke maatregelen niet ondersteunt.

9. Onvoldoende bewustwording/instructies bij medewerkers met toegang

Medewerkers die niet aantoonbaar op de hoogte zijn van de geldende kaders, het vier-ogenprincipe, de verbodsbepaling op eigen opnames en de logboekplicht, vormen een risico dat niet door technische maatregelen alleen kan worden ondervangen.

10. Cameratoezicht als enige maatregel, zonder subsidiariteitstoets

Cameratoezicht is het zwaarste middel en mag niet worden ingezet als enige maatregel: zonder aantoonbaar getroffen, geëvalueerde en ook na installatie actief blijvende preventieve maatregelen en zonder gedocumenteerde subsidiariteitsafweging per camera in het cameraoverzicht, ontbreekt de rechtvaardiging voor de inzet. Ook het niet betrekken van leerlingen (via de (G)MR of leerlingenraad) bij besluitvorming over cameraplaatsing en -beleid en het niet schriftelijk vastleggen van die consultatie, vormt onderdeel van dit risico. Daarnaast kan een gebouwonwerp waarin de ruimte-indeling niet is meegewogen, leiden tot een onevenredig groot aantal camera's of tot onoverzichtelijke plekken buiten het zicht van camera's.

Deze managementsamenvatting betreft de centrale DPIA en wordt door het schoolbestuur niet aangepast. Het schoolbestuur vult de lokale managementsamenvatting in aan het begin van Deel E - lokale DPIA.

3. Uitleg en achtergrond DPIA

Dit hoofdstuk legt uit wat een Data Protection Impact Assessment (DPIA), in het Nederlands gegevensbeschermingseffectbeoordeling, is, wanneer die verplicht is en volgens welke methodiek SIVON de centrale DPIA uitvoert namens schoolbesturen. Ook wordt toegelicht waarom het schoolbestuur als verwerkingsverantwoordelijke daarnaast altijd zelf een lokale DPIA uitvoert en hoe het centrale en het lokale deel op elkaar aansluiten. Zo is duidelijk wat SIVON in dit rapport al heeft uitgewerkt en wat het schoolbestuur zelf nog moet invullen en vaststellen.

1. Informatiebeveiliging en privacy (IBP)

In het onderwijs maken we steeds meer gebruik van persoonsgegevens en ICT. We slaan steeds meer informatie op en wisselen digitaal steeds meer informatie uit. Dit doen niet alleen scholen, maar ook de leveranciers van digitale leermiddelen. Leerlingen, ouders en medewerkers willen erop kunnen vertrouwen dat scholen zorgvuldig met hun gegevens omgaan en de privacy waarborgen.

Privacy is enerzijds het recht om met rust te worden gelaten en anderzijds gaat het over het recht om gegevens over jezelf te kunnen controleren. Als je bij alles wat je doet, gevolgd wordt én je denkt of weet dat dit gevolgen voor jou kan hebben, dan pas je jouw gedrag daarop aan. Zonder het recht op privacy kan een mens niet vrij zijn. Privacy is daarmee een randvoorwaarde in een democratische samenleving. Daarom blijft het belangrijk dat scholen privacy goed organiseren. Het beschermen van privacy gaat niet zonder het beschermen van persoonsgegevens: gegevens van betrokkenen mogen immers niet in verkeerde handen vallen. Daarom spreken we vaak over IBP: Informatiebeveiliging en privacy.

2. Privacyconvenant en toetsing verwerkersovereenkomsten

Volgens de Europese privacywet Algemene Verordening Gegevensbescherming (AVG) is een schoolbestuur eindverantwoordelijk voor de bescherming van de privacy en persoonsgegevens van leerlingen, hun ouders en medewerkers. Het schoolbestuur wordt **verwerkingsverantwoordelijke** genoemd. Het schoolbestuur moet de controle houden over het gebruik van deze persoonsgegevens en zij bepaalt dus voor welke doelen deze gegevens mogen worden gebruikt. Een leverancier van software waarin al deze persoonsgegevens zijn opgenomen, wordt in de AVG **verwerker** genoemd. Deze mag die persoonsgegevens niet zomaar voor eigen doeleinden gebruiken. In een **verwerkersovereenkomst** legt het schoolbestuur afspraken vast met deze leverancier. In het onderwijs wordt hiervoor gebruik gemaakt van de model verwerkersovereenkomst van het Privacyconvenant onderwijs⁴.

Scholen kunnen gemakkelijk verwerkersovereenkomsten goedkeuren en digitaal ondertekenen met behulp van de Dienst Verwerkersovereenkomsten van Kennisnet⁵. SIVON toetst voor het primair en voortgezet onderwijs vooraf of de verwerkersovereenkomsten van leveranciers van de meestgebruikte applicaties voldoen aan de eisen van het Privacyconvenant⁶. Deze rapportages zijn onder andere beschikbaar in de Dienst Verwerkersovereenkomsten.

3. DPIA

Om vast te stellen of de gegevens van leerlingen en medewerkers (persoonsgegevens) in een applicatie, software of ICT-middel veilig en verantwoord gebruikt worden, is volgens de AVG verplicht om een Data

⁴ <https://www.privacyconvenant.nl/>

⁵ <https://www.kennisnet.nl/dienst-verwerkersovereenkomsten/>

⁶ <https://sivon.nl/toetsen-verwerkersovereenkomsten/>

Protection Impact Assessment (DPIA) uit te voeren. In de AVG wordt dit een gegevensbeschermingseffectbeoordeling (GEB) genoemd. Een DPIA wordt uitgevoerd op een proces, applicatie of verwerking van persoonsgegevens. Meestal gaat het om een applicatie van een leverancier (verwerker). De DPIA wordt uitgevoerd volgens de eisen van artikel 35 van de AVG. Met een DPIA wordt beoordeeld wat de risico's en (mogelijke) gevolgen zijn van het gebruik van de applicatie voor de bescherming van de persoonsgegevens van de leerlingen, hun ouders en medewerkers. Er wordt vastgesteld of het gebruik van persoonsgegevens (verwerking) een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen. Als de privacyrisico's (te) hoog zijn, moet er worden gezocht naar maatregelen om deze risico's te beperken. Dit worden mitigerende maatregelen genoemd. Als de hoge risico's niet weggenomen kunnen worden, dan mag volgens de AVG deze verwerking (gebruik applicatie) niet worden uitgevoerd of voortgezet.

De uitkomst van de DPIA is onder andere een rapportage met daarin een overzicht van geclassificeerde risico's voor de rechten en vrijheden van betrokkenen. In het rapport staan ook de nodige mitigerende maatregelen benoemd. De verwerkingsverantwoordelijke stelt uiteindelijk de DPIA vast. Hiermee wordt vastgelegd welke maatregelen nog moeten worden uitgevoerd en dat het schoolbestuur de resterende vastgestelde risico's accepteert.

4. Verplichte uitvoering DPIA

Deze privacytoets is verplicht als de verwerking van persoonsgegevens, gelet op de aard, de omvang, de context en de doeleinden van die verwerking, waarschijnlijk een hoog risico inhoudt voor de 'rechten en vrijheden' (privacy) van leerlingen, ouders en medewerkers.

Ook is het mogelijk dat het uitvoeren van een DPIA verplicht is volgens de regels van de privacytoezichthouder Autoriteit Persoonsgegevens (AP) die een heeft lijst gepubliceerd met verwerkingen waarvoor het uitvoeren van een DPIA verplicht is⁷. In het onderwijs betekent dit dat een DPIA altijd verplicht is op tenminste het leerlingvolg- en/of -administratiesysteem (LVS/LAS), personeelsadministratiesysteem en breed ingezette applicaties met digitaal leermateriaal.

Ook de EDPB⁸ benadrukt dit:

'Een gegevensbeschermingseffectbeoordeling kan ook nuttig zijn om het gegevensbeschermingseffect van een technologisch product te beoordelen, bijvoorbeeld hardware of software, indien dit waarschijnlijk door verschillende verwerkingsverantwoordelijken zal worden gebruikt om verschillende verwerkingen uit te voeren. Natuurlijk blijft de verwerkingsverantwoordelijke die het product lanceert verplicht om zijn eigen gegevensbeschermingseffectbeoordeling uit te voeren met betrekking tot de specifieke implementatie, al kan hij zich hiervoor baseren op een door de productaanbieder uitgevoerde gegevensbeschermingseffectbeoordeling, in voorkomend geval.'

5. Centrale en lokale DPIA

Bij applicaties die door veel schoolbesturen op dezelfde wijze worden gebruikt, is het zinvol om een DPIA gezamenlijk uit te voeren, zo hoeft niet elk schoolbestuur afzonderlijk dezelfde analyse te maken. SIVON voert daarom in opdracht van OCW **centrale DPIA's** uit namens het primair en voortgezet onderwijs. Door expertise en praktijkervaring van verschillende schoolbesturen samen te brengen ontstaat een sterkere en bredere analyse. Bovendien maakt een gezamenlijke aanpak het eenvoudiger

⁷ <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf>

⁸ EDPB: European Data Protection Board (de Europese privacy toezichthouder): https://www.edpb.europa.eu/edpb_en.

om met leveranciers afspraken te maken over beheersmaatregelen, omdat SIVON namens de gehele sector spreekt. De EDPB bevestigt uitdrukkelijk dat het uitvoeren van één DPIA voor een applicatie die door meerdere verwerkingsverantwoordelijken wordt gebruikt is toegestaan en zinvol is, maar benadrukt tegelijkertijd dat iedere verwerkingsverantwoordelijke verplicht blijft zijn eigen DPIA uit te voeren voor de specifieke implementatie binnen zijn organisatie.

Schoolbesturen moeten altijd zelf de lokale DPIA uitvoeren, omdat de AVG de uitvoeringsplicht expliciet bij de verwerkingsverantwoordelijke legt, het schoolbestuur (art. 35 lid 1). Daarnaast moet het schoolbestuur zelf aantoonbaar kunnen maken dat het aan zijn privacyverplichtingen voldoet, deze verantwoordingsplicht kan niet worden overgedragen (art. 5 lid 2). Tot slot schrijft de AVG voor dat betrokkenen in voorkomend geval worden geraadpleegd. Wie niet raadpleegt, moet dat motiveren en documenteren. Die raadpleging is per definitie lokaal, omdat alleen het schoolbestuur weet wie zijn betrokkenen zijn (art. 35 lid 9).

SIVON richt zich in de centrale DPIA op applicatiespecifieke risico's en neemt de meest voorkomende risico's voor lokaal gebruik mee in een advies aan de schoolbesturen. De uiteindelijke beoordeling daarvan ligt echter altijd bij het schoolbestuur zelf, omdat de lokale implementatie en schoolspecifieke context niet universeel zijn voor alle schoolbesturen in Nederland. Dat is precies waarom SIVON een centraal deel aanbiedt en het schoolbestuur zelf het lokale deel invult en vaststelt.

6. Methodiek DPIA

SIVON volgt bij de uitvoering van de centrale DPIA het model van de Rijksoverheid⁹, aangevuld met onderwijs-specifieke informatie uit de voormalige *Handleiding uitvoeren data protection impact assessment (DPIA) voor het po en vo (versie 1.0)*¹⁰. Het model is daarnaast aangepast aan specifieke informatie over de applicatie en aangevuld met een model lokale DPIA voor schoolbesturen. Er wordt rekening gehouden met Europese richtlijnen van de gezamenlijke Europese toezichthouders (EDPB) waaronder de "Richtsnoeren voor gegevensbeschermingseffectbeoordelingen (2016/679, 4 april 2017)"¹¹.

SIVON voert bij de uitvoering van de centrale DPIA de volgende activiteiten uit:

- Beschrijving van de (methoden van) gegevensverwerkingen: (gegevensverwerkingsanalyse) en toegepaste (beveiligings-)technieken.
- Beoordeling van de rechtmatigheid van de gegevensverwerkingen, inclusief afweging van kinderrechten.
- Beschrijving en beoordeling risico's voor de betrokkenen.
- Beschrijving en beoordeling van (eventuele) voorgenomen maatregelen die de gevonden (privacy)risico's beperken.
- Beoordeling beveiligingsmaatregelen aan de hand van de BIV-classificatie.
- Beoordeling van de mogelijkheden om te voldoen aan rechten van betrokkenen.
- Overleg met betrokken schoolbesturen over mitigerende maatregelen.
- Opstellen en bespreken DPIA-rapportage.

⁹ [Model DPIA Rijksdienst v3.0.pdf \(kcbr.nl\)](#)

¹⁰ Aanpak IBP Kennisnet (2021)

¹¹ https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_nl.pdf

7. Toepassing op cameratoezicht

Een centrale DPIA van SIVON richt zich normaal gesproken op een proces binnen een applicatie van een leverancier, zoals hierboven beschreven. Bij cameratoezicht ligt het zwaartepunt net wat anders. De meeste risico's en maatregelen liggen bij wat het schoolbestuur zelf organisatorisch en technisch moet inregelen, zoals beleid, procedures, autorisatiebeheer, bewaartermijnen en informatievoorziening aan betrokkenen. Dat komt ook omdat in verreweg de meeste gevallen de opslag volledig lokaal plaatsvindt en de verwerking onder eigen verantwoording plaatsvindt. De leverancier van het camerasysteem heeft lang niet altijd toegang tot de beelden. Waar dat niet het geval is, is een verwerkersovereenkomst met de leverancier niet nodig. Fabrikanten van camerasystemen bieden bovendien doorgaans weinig ruimte om het product aan te passen naar aanleiding van een DPIA. Deze DPIA beoordeelt het cameratoezicht daarom volledig als proces. Een technische beveiligingsbeoordeling van individuele systemen is niet uitgevoerd. Het schoolbestuur beoordeelt de eigen situatie in de lokale DPIA, op basis van de generieke risico's die voor alle systemen gelden.

8. Funderend onderwijs referentie architectuur (FORA)

Bij de uitvoering van de DPIA wordt gebruik gemaakt van FORA: Funderend Onderwijs Referentie Architectuur.

Applicatie landschap

Het hebben van een architectuur helpt bij het tijdig en goed reageren op zakelijke of juridische (AVG) eisen en/of (externe) dreigingen die een (mogelijke) aanpassing in de informatiehuishouding vragen. (Norm GO.04 informatiearchitectuur van het Normenkader IBP).

Voor het funderend onderwijs is de FORA (Funderend Onderwijs Referentie Architectuur) ontwikkeld. FORA is een gestandaardiseerde methodiek die inzicht geeft in verplichte processen en onderwijsactiviteiten in het primair en voortgezet onderwijs.

De FORA biedt inzicht in wat de bedrijfsfuncties zijn van een po en vo school. Het hoofdbedrijfsfunctiemodel beschrijft op hoofdlijnen wat een onderwijsorganisatie doet. Deze beschrijving wordt verdiept in het bedrijfsfunctiemodel, waarin nader wordt uitgewerkt hoe invulling wordt gegeven aan deze activiteiten. Op basis daarvan is het mogelijk om 'referentiecomponenten' toe te voegen. Referentiecomponenten zijn typen systemen, zoals een LAS, een toetsstelsel, of een ELO, met bijbehorende functionaliteiten ('applicatiefuncties').

SIVON voert centrale DPIA's uit op een applicatie. Een applicatie kan in de FORA vertaald worden naar één of meerdere referentie componenten. Een referentiecomponent is een functionele afbakening van een modulaar, zelfstandig inzetbaar en vervangbaar (deel van een) systeem.

In deze DPIA gebruiken we FORA om een applicatie te kunnen plaatsen in het applicatielandschap: welke plaats neemt de applicatie in het totaal aan applicaties die een school gebruikt.

4. Motivering DPIA Cameratoezicht

Dit hoofdstuk onderbouwt waarom voor cameratoezicht een DPIA verplicht is, bakent de reikwijdte van deze DPIA af en benoemt aandachtspunten die buiten de scope vallen maar wel relevant zijn voor informatiebeveiliging en privacy. De verplichting volgt uit de AVG, de lijst van de Autoriteit Persoonsgegevens en de criteria van de EDPB.

1. Verplichting uitvoeren DPIA

Bij gebruik van cameratoezicht door schoolbesturen is het uitvoeren van een DPIA verplicht omdat sprake is van:

- *Artikel 35 lid 3 AVG:*
 - De school volgt mensen op grote schaal en systematisch in een publiek toegankelijk gebied (bijvoorbeeld cameratoezicht).
- *Lijst van de Autoriteit Persoonsgegevens voor verwerkingen waarvoor uitvoeren van een DPIA verplicht is:*
 - Cameratoezicht
- *Lijst van de gezamenlijke EU privacytoezichthouders (EDPB) met criteria waarbij een DPIA verplicht is (twee of meer criteria zijn vereist):*
 - Stelselmatige en grootschalige monitoring
 - Gegevens over kwetsbare personen (zoals jonge leerlingen of leerlingen met een beperking)

2. Scope van deze DPIA

Deze DPIA heeft betrekking op de inzet van cameratoezicht door schoolbesturen binnen het funderend onderwijs (primair onderwijs en voortgezet onderwijs) en omvat alle verwerkingen van persoonsgegevens die daarmee samenhangen. De DPIA beoordeelt het cameratoezicht als proces: van de besluitvorming over de inzet van camera's tot en met de opslag, toegang, bewaartermijnen en verwijdering van beeldmateriaal. Daarbij worden zowel de juridische als organisatorische en technische maatregelen beoordeeld die het schoolbestuur als verwerkingsverantwoordelijke dient te treffen.

Binnen scope

- Cameratoezicht op en rond schoollocaties, zowel binnen- als buitenruimtes, uitgevoerd onder verantwoordelijkheid van het schoolbestuur.
- Alle bijbehorende organisatorische maatregelen, waaronder: beleid, procedures, autorisatiebeheer, bewaartermijnen en informatievoorziening aan betrokkenen.
- De technische maatregelen die het schoolbestuur als verwerkingsverantwoordelijke dient te treffen, waaronder: de wijze van opslag van beeldmateriaal, netwerkarchitectuur en -segmentatie en overige beveiligingsmaatregelen.
- De verwerkersrelatie met leveranciers van camerasystemen en opslagoplossingen.
- De toetsing van de rechtmatigheid van de verwerking geldt voor publiek bekostigd onderwijs in het PO/VO.

Scholen die niet onder de WPO of de WVO vallen, zoals niet-bekostigde, particuliere of internationale scholen, kunnen geen beroep doen op de taak van algemeen belang (art. 6 lid 1 sub e AVG). Zij kunnen de risico's en maatregelen uit deze DPIA wel gebruiken, maar moeten de grondslag voor het cameratoezicht zelf onderbouwen op basis van het gerechtvaardigd belang (art. 6 lid 1 sub f AVG), met een eigen belangenafweging (LIA). De grondslagen die berusten op een wettelijke verplichting (art. 6 lid 1 sub c AVG), zoals de zorg voor de veiligheid en gezondheid van medewerkers (art. 3

Arbowet) en de verstrekking op een vordering van politie of justitie, blijven ook voor deze scholen van toepassing.

3. Buiten scope

- De technische beveiligingsbeoordeling van specifieke camerasystemen, merken of productgeneraties. Deze DPIA is niet leverancier specifiek en beoordeelt geen individuele producten of infrastructuurcomponenten.
- Cameratoezicht uitgevoerd door of onder verantwoordelijkheid van derden, zoals ingehuurde beveiligingsdiensten die zelfstandig als verwerkingsverantwoordelijke optreden.
- Camerasystemen met geautomatiseerde analyse of AI-functionaliteit (zoals gezichtsherkenning of gedragsdetectie).
- Overige vormen van beeldregistratie die niet vallen onder permanent cameratoezicht, zoals opnames in de klas voor beoordeling van studenten op een docentenopleiding en interne opleiding van collega's, camera's voor toegang tot parkeerfaciliteiten, dashcams in schoolvoertuigen of bodycams.
- Cameratoezicht uitgevoerd door een verhuurder in gehuurde ruimtes waar het schoolbestuur geen verwerkingsverantwoordelijke is (zie aandachtspunt hieronder).
- Diepgaand technisch informatiebeveiligingsonderzoek naar het cameratoezicht viewer software systeem, anders dan het configureren/beoordelen van aanwezige/bestaande instellingen. Er zijn geen penetratietesten uitgevoerd.
- Heimelijk cameratoezicht (toezicht met verborgen en/of niet-zichtbare camera's, of toezicht dat niet kenbaar is gemaakt aan betrokkenen). Deze DPIA beoordeelt uitsluitend transparant, kenbaar gemaakt cameratoezicht

4. Aandachtspunten

Als een schoolbestuur ruimtes huurt van een derde partij waar door die partij cameratoezicht wordt uitgevoerd, valt dit toezicht buiten de directe scope van deze DPIA. Het schoolbestuur treedt in dat geval niet op als verwerkingsverantwoordelijke. Het schoolbestuur heeft echter wel een verantwoordelijkheid om te beoordelen of dit cameratoezicht verenigbaar is met de rechten en belangen van de eigen leerlingen, medewerkers en bezoekers.

In de praktijk betekent dit dat het schoolbestuur de verhuurder vraagt om diens DPIA, als die voor de verhuurder verplicht is en diens reglement voor het cameratoezicht. Zijn die er niet, dan spreekt het schoolbestuur met de verhuurder af dat ze er binnen drie maanden na het verzoek zijn. Daarnaast doet het schoolbestuur navraag naar het doel, de reikwijdte en de waarborgen van het betreffende cameratoezicht en controleert het dat er niet wordt gefilmd op niet toegestane plekken en niet in lokalen of gymzalen zolang de eigen leerlingen die gebruiken. Aanbevolen wordt om hierover concrete afspraken te maken en deze vast te leggen in de huurovereenkomst of een bijlage daarbij. Denk daarbij aan: welke ruimtes worden bewaakt, wie heeft toegang tot het beeldmateriaal, wat zijn de bewaartermijnen en op welke wijze worden betrokkenen geïnformeerd. Op basis van deze informatie maakt het bestuur een afweging of gebruik van de betreffende ruimte verantwoord is.

Wanneer een schoolbestuur heimelijk cameratoezicht overweegt, valt dit buiten de reikwijdte van deze DPIA. Heimelijke inzet vormt een aanzienlijk zwaardere inbreuk op de privacy van betrokkenen dan regulier, transparant cameratoezicht en is onder de AVG en de richtsnoeren van de Autoriteit Persoonsgegevens alleen toegestaan onder aanvullende, strikte voorwaarden.

In de praktijk betekent dit dat het schoolbestuur voorafgaand aan de inzet van heimelijk cameratoezicht een aanvullende, specifiek daarop gerichte risicobeoordeling uitvoert als zelfstandige beoordeling.

5. Deel A: Gegevensverwerkingsanalyse

Dit hoofdstuk beschrijft het cameratoezicht als gegevensverwerkend proces, van vastlegging tot en met verwijdering van beeldmateriaal. Op gestructureerde wijze worden de persoonsgegevens, gegevensverwerkingen, verwerkingsdoeleinden, betrokken partijen en belangen beschreven. Deze beschrijving vormt de basis voor de beoordeling in de volgende hoofdstukken.

1. Beschrijving van het gegevensverwerkende proces

Cameratoezicht binnen het funderend onderwijs is een gegevensverwerkend proces waarbij persoonsgegevens worden vastgelegd, opgeslagen, geraadpleegd, gedeeld en uiteindelijk verwijderd. Onderstaande beschrijving volgt de levenscyclus van beeldmateriaal van vastlegging tot verwijdering. Waar de situatie per locatie kan verschillen, is een invultabel opgenomen. Overige onderdelen gelden op bestuursniveau en worden eenmalig ingevuld.

1. Vastlegging

Het schoolbestuur zet cameratoezicht in op de door hen aangewezen locaties. De camera's leggen continu, volgens een tijdschema of op basis van bewegingsdetectie beelden vast van de binnen- en/of buitenruimtes van de schoollocatie. Camera's die uitsluitend zijn ingezet voor de doeleinden 3 en/of 4 nemen alleen buiten de Gebruikstijden van de locatie op (zie hoofdstuk 17). De camera's zijn geïnstalleerd door een installateur en bestaan uit een combinatie van camera's en een recorder (lokaal of cloud).

Een overzicht van alle cameraposities, de daarbij vastgelegde ruimtes en het per camera vastgestelde doel is opgenomen in het cameraoverzicht (bijlage 4).

Het camerasysteem legt automatisch systeemlogging (audittrail) vast, die uitsluitend toegankelijk is voor de systeemeigenaar. Daarnaast houdt het schoolbestuur drie logboeken bij: het logboek wijzigingen camera-instellingen (wijzigingen aan privacygevoelige instellingen, waaronder de bewaartermijn en het tijdschema), het logboek reglement afwijkingen (afwijkingen van het reglement, uitsluitend na voorafgaande toestemming van het bestuur) en het logboek beeldgebruik (terugkijken, bewaren en verwijderen, inzage door en delen met derden). De systeemeigenaar controleert de systeemlogging en de logboeken periodiek en naar aanleiding van incidenten en rapporteert de uitkomsten aan de proceseigenaar.

2. Opslag

Na vastlegging worden de beelden opgeslagen voor de duur van de vastgestelde bewaartermijn. De technische componenten van het camerasysteem (recorder, switches e.d.) bevinden zich in een afgesloten technische ruimte, toegankelijk voor de systeemeigenaar en daartoe bevoegde medewerkers.

3. Toegang en raadpleging

Toegang tot het camerasysteem is voorbehouden aan medewerkers die zijn opgenomen in de autorisatiematrix. Iedere gebruiker beschikt over een persoonlijk account en accounts worden niet gedeeld. Voordat beelden teruggekeken kunnen worden, dient altijd opnieuw te worden ingelogd, ook als de recorder actief is en live beelden worden getoond.

Het terugkijken van beelden vindt plaats in aanwezigheid van minimaal twee bevoegde medewerkers. Een medewerker van de onderhoudspartij telt daarbij niet mee en bekijkt beelden uitsluitend bij storingen of onderhoud. Alleen bij een calamiteit buiten Schooltijd, zoals een inbraak(poging), een brandalarm of een geweldsincident, mag een bevoegde medewerker individueel en zo nodig op afstand beelden terugkijken, volgens de daarvoor vastgestelde richtlijnen. Elke raadpleging van beelden wordt geregistreerd in het logboek beeldgebruik.

Waar online toegang tot het systeem mogelijk is, gelden aanvullende beveiligingsvereisten, waaronder MFA. Online toegang vindt uitsluitend plaats vanaf door de organisatie beheerde apparaten. Toegang op afstand is daarnaast beperkt tot calamiteiten buiten Schooltijd en tot de daartoe in de autorisatiematrix opgenomen medewerkers, met uitsluitend kijkrechten.

4. Delen met derden

Beelden worden in beginsel niet gedeeld met derden. Uitsluitend in de daarvoor vastgestelde situaties, zoals het doen van aangifte bij de politie, kunnen derden inzage krijgen of kunnen beelden worden gedeeld. Bij een gerechtvaardigd inzageverzoek van een betrokkene worden beelden alleen getoond en niet gedeeld. Inzage door en delen met derden vereist altijd een vooraf genomen besluit. Delen vindt plaats op een beveiligde wijze, bij voorkeur via een vanuit het camerasysteem gegenereerde beveiligde link met een beperkte geldigheid, anders via een versleutelde gegevensdrager of een beveiligde uploadvoorziening van de ontvanger. Het versturen van beelden per e-mail of via openbaar toegankelijke platforms is niet toegestaan.

De ontvanger van beelden identificeert zich voordat inzage of overdracht plaatsvindt. Elke inzage door en verstrekking aan derden wordt geregistreerd in het logboek beeldgebruik, inclusief wie het besluit heeft genomen en hoe de ontvanger zich heeft geïdentificeerd.

5. Verwijdering en bewaartermijnen

Beelden worden automatisch overschreven na een bewaartermijn die technisch is ingesteld in het camerasysteem: standaard drie weken, met een gemotiveerde reden te verlengen tot maximaal vier weken. Tijdens de zomervakantie geldt een maximale bewaartermijn van zes weken. Daarna valt de bewaartermijn automatisch terug naar de reguliere termijn. Ondersteunt het camerasysteem dat niet, dan zet de systeemeigenaar de bewaartermijn na de eerste schooldag en uiterlijk op de tweede schooldag handmatig terug en legt hij dit vast in het logboek wijzigingen camera-instellingen. Beelden die in het kader van een incident worden bewaard, blijven bewaard totdat het incident is afgehandeld of de beelden zijn overgedragen aan politie of justitie. Daarna worden deze beelden, ook kopieën buiten het camerasysteem, zo spoedig mogelijk en uiterlijk binnen drie weken verwijderd.

Elke beslissing tot bewaren of verwijderen van beelden buiten de reguliere cyclus wordt geregistreerd in het logboek beeldgebruik, inclusief het moment van uiteindelijke verwijdering.

Systeemloggegevens worden dertien maanden bewaard. De logboeken worden ten minste dertien maanden en ten hoogste twee jaar bewaard. Na afloop van deze termijnen worden de gegevens verwijderd.

6. Beheer en onderhoud

Het camerasysteem wordt beheerd door de systeemeigenaar, die ook verantwoordelijk is voor het doorvoeren van updates, upgrades en beveiligingspatches. Het systeem past beveiligingsupdates

automatisch toe of deze worden minimaal eens per kwartaal handmatig gecontroleerd en toegepast. Onderhoud wordt intern uitgevoerd of door een externe partij, waarbij afspraken zijn vastgelegd in een SLA, waarin een geheimhoudingsclausule is opgenomen die de onderhoudspartij verbiedt beelden te bekijken, op te slaan of te delen, tenzij strikt noodzakelijk op verzoek van de proces- of systeemeigenaar. Heeft de onderhoudspartij Structurele toegang tot het camerasysteem, dan is ook een verwerkersovereenkomst van kracht. De SLA wordt minimaal jaarlijks geëvalueerd door de proceseigenaar en de systeemeigenaar.

De proceseigenaar is bestuursbreed de verantwoordelijke voor het cameratoezicht en controleert steekproefsgewijs het gebruik van het camerasysteem. Eén rol is formeel verantwoordelijk voor het accountbeheer. Het aanvragen, toewijzen en intrekken van toegangsrechten is daarbij belegd bij verschillende rollen (functiescheiding). Het verwijderen van accounts bij uitdiensttreding of functiewijziging is opgenomen in het HR-proces.

2. Persoonsgegevens

Bij cameratoezicht worden beelden vastgelegd van personen die zich binnen en/of buiten bevinden op de locatie van het schoolbestuur. De volgende categorieën betrokkenen kunnen in beeld komen:

- Medewerkers en tijdelijke medewerkers
- Leerlingen, waaronder minderjarigen
- Ouders en verzorgers
- Bezoekers
- Leveranciers
- Opvangkinderen
- Huurders van de locatie
- Gebruikers van de gymzaal

Het beeldmateriaal betreft een visuele weergave van personen en hun gedrag op een bepaald moment en op een bepaalde locatie. Dit is aan te merken als een gewoon persoonsgegeven.

Tabel 2.1 Persoonsgegevens

Categorie persoonsgegevens	Leerling/ Opvang kinderen	(Tijdelijke) Medewerker	Ouder/ Verzorger	Bezoekers/ Leveranciers	Huurders/ Gebruikers van de gymzaal
Videobeelden van betrokkene zonder geluid van de activiteiten op de locatie van het schoolbestuur	X	X	X	X	X
Logboekgegevens (<i>naam van medewerker(s) die een handeling uitvoeren, een besluit nemen of toestemming verlenen en bij inzage of delen ook naam en wijze van identificatie van de ontvangende derde</i>)		X		X*	
Metadata/ Logging		X		X*	

* alleen in geval van de leverancier van het camerasysteem tijdens lokaal onderhoud

Gevoelige persoonsgegevens

Hoewel het cameratoezicht niet is gericht op het vastleggen van gevoelige kenmerken, kunnen beelden in de praktijk informatie bevatten die als gevoelig kan worden beschouwd, zoals het gedrag of de emotionele toestand van een persoon. Dergelijke gegevens worden niet gericht verwerkt en er worden geen conclusies aan verbonden.

Bijzondere persoonsgegevens

Het cameratoezicht is niet gericht op het verwerken van bijzondere persoonsgegevens als bedoeld in artikel 9 AVG, zoals gegevens over gezondheid, religie of etnische afkomst. In de praktijk kunnen beelden echter incidenteel zichtbare kenmerken bevatten die tot deze categorieën behoren, bijvoorbeeld een persoon in een rolstoel of met religieuze kleding. Deze gegevens worden niet gericht vastgelegd, niet apart opgeslagen en er worden geen conclusies aan verbonden. Het verwerkingsdoel omvat uitdrukkelijk niet het verwerken van bijzondere persoonsgegevens.

Strafrechtelijke persoonsgegevens

Het cameratoezicht is mede gericht op het tegengaan en opsporen van diefstal en vandalisme. Gelet op het verwerkingsdoel, het beschermen van de veiligheid van personen en zaken en niet het vaststellen van strafbare feiten, kwalificeert beeldmateriaal dat in dit kader wordt vastgelegd op zichzelf niet als strafrechtelijk persoonsgegeven in de zin van artikel 10 AVG. Op de beelden kan een vermeende gedraging zijn vastgelegd, maar het oordeel daarover is niet aan de school. De school verwerkt de beelden op grond van haar eigen grondslag en doeleinden. Worden beelden overgedragen aan een opsporings- of rechterlijke instantie, dan verwerkt die instantie de verstrekte beelden onder haar eigen verwerkingsverantwoordelijkheid. Een kopie die de school na overdracht behoudt, blijft onder de verwerkingsverantwoordelijkheid van de school. Die kopie dient niet om strafrechtelijke gegevens te bewaren, maar om te voldoen aan wettelijke verplichtingen, inzageverzoeken af te handelen en interne richtlijnen na te leven. Voor zover het beeldmateriaal toch als strafrechtelijk persoonsgegeven zou kwalificeren, biedt artikel 33 lid 2 sub b UAVG een uitzondering op het verwerkingsverbod. Die uitzondering geldt voor verwerking ter bescherming van de eigen belangen van de school, voor zover het gaat om strafbare feiten die zijn of naar verwachting zullen worden gepleegd naar de school of naar personen die in haar dienst zijn. Deze uitzondering ziet niet op strafbare feiten naar leerlingen of bezoekers, zoals een vechtpartij tussen leerlingen. Voor die beelden is het verwerkingsdoel bepalend: de school legt een veiligheidsincident vast en velt daarover zelf geen strafrechtelijk oordeel.

3. Gegevensverwerkingen

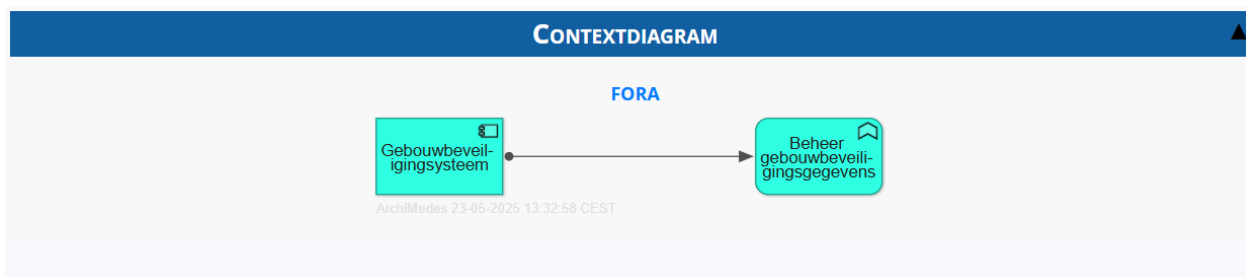
Voor het schetsen van de reikwijdte van de gegevensverwerkingsanalyse wordt aangesloten bij de FORA (Funderend Onderwijs Referentie Architectuur) voor het primair en voortgezet onderwijs.

Cameratoezicht valt binnen het FORA-domein Gebouwbeveiligingssysteem en maakt geen onderdeel uit van de onderwijskundige of administratieve processen van het schoolbestuur.

Applicatielandschap

Het camerasysteem bestaat uit de volgende componenten: de camera's zelf (IP-camera's dan wel analoge camera's), een lokale recorder (NVR of DVR) waarop beelden worden opgeslagen, en beheer- en viewsoftware waarmee geautoriseerde gebruikers toegang krijgen tot de beelden. Deze toegang vindt plaats via een monitor direct aangesloten op de recorder, of via een workstation, laptop, tablet of mobiel apparaat. In de meest voorkomende situatie is de opslag volledig lokaal ingericht op de schoollocatie. In een beperkt aantal gevallen maakt de beheer- of viewsoftware gebruik van een cloudcomponent bij de leverancier, dit wordt per implementatie in de DPIA vastgelegd.

Het camerasysteem staat los van de overige systemen binnen het applicatielandschap van het schoolbestuur.



Koppelingen

Het camerasysteem heeft geen koppelingen met andere interne systemen of externe partijen. Beelden worden niet automatisch doorgezonden naar derden. Overdracht van beelden aan derden, zoals een opsporingsinstantie, vindt uitsluitend handmatig plaats op incidentele basis en altijd op basis van een expliciete beslissing van een daartoe bevoegde functionaris.

Levenscyclus van de verwerking

Voor de levenscyclus van de verwerking, zijn er twee mogelijke opties:

- Scenario A: lokale opslag
- Scenario B: cloudopslag

Uitwerking Scenario A - Lokale opslag

Verzameling

De camera's leggen continu, volgens een tijdschema of op basis van bewegingsdetectie beeldmateriaal vast van personen die zich binnen en/of buiten bevinden op de locatie van het schoolbestuur. Camera's die uitsluitend zijn ingezet voor de doeleinden 3 en/of 4 nemen alleen buiten de Gebruikstijden van de locatie op (zie hoofdstuk 17). In leslokalen en gymzalen wordt nooit gefilmd terwijl de ruimte in gebruik is. Buiten de Gebruikstijden is cameratoezicht alleen toegestaan in praktijklokalen met kostbare apparatuur en in gymzalen, ter beveiliging van de ruimte en de daarin aanwezige eigendommen. In toiletten, kleedkamers en andere ruimtes met een fundamenteel privacykarakter vindt nooit cameratoezicht plaats.

Gebruik

Geautoriseerde medewerkers, opgenomen in de autorisatiematrix, kunnen beelden live zien en/of raadplegen op één of, afhankelijk van de inrichting, beide van de volgende manieren. Binnen het fysiek of logisch gescheiden netwerk kan rechtstreeks worden ingelogd op de recorder via de beheer- en viewsoftware, bijvoorbeeld op een direct aangesloten monitor en/of workstation. Daarnaast kan raadpleging op afstand zijn ingericht, bijvoorbeeld vanaf een laptop, tablet of mobiele telefoon via een app, waarbij een verbinding van buiten het gescheiden netwerk tot stand komt en de gescheiden netwerkgrens passeert. Indien toegang op afstand is ingericht, blijft deze beperkt tot calamiteiten buiten Schooltijd en tot geautoriseerde gebruikers met uitsluitend kijkrechten, en verloopt zij uitsluitend via een beveiligde verbinding met MFA en op beheerde apparatuur. Van het terugkijken van beelden wordt een logboekregel bijgehouden in het logboek beeldgebruik. Bij het gebruik van het systeem ontstaat daarnaast systeemlogging, waarin technische handelingen zoals inloggen en het wijzigen van

instellingen worden vastgelegd. Wijzigingen aan privacygevoelige camera-instellingen worden bovendien vastgelegd in het logboek wijzigingen camera-instellingen.

Opslag

Het beeldmateriaal wordt via een fysiek of logisch gescheiden netwerk doorgestuurd naar de lokale recorder, waar het wordt opgeslagen en beschikbaar gesteld via de beheer- en viewsoftware. De verwerking vindt volledig plaats binnen de eigen infrastructuur van het schoolbestuur. De beelden worden gedurende een vastgestelde bewaartermijn bewaard. Wanneer wordt besloten beelden langer te bewaren vanwege een incident dat vraagt om intern of extern onderzoek, wordt dit vastgelegd in het logboek beeldgebruik. De systeemlogging die bij het gebruik van het systeem ontstaat, wordt eveneens binnen dit systeem opgeslagen, met een eigen bewaartermijn los van die van de videobeelden.

Verstrekking

In reguliere situaties verlaten beelden het systeem niet. Bij een incident kan beeldmateriaal worden overgedragen aan een opsporings- of rechterlijke instantie. Een opsporings- of rechterlijke instantie die beelden ontvangt, treedt op als zelfstandig verwerkingsverantwoordelijke voor die beelden vanaf het moment van overdracht. Wanneer inzage wordt verleend aan derden of beelden met derden worden gedeeld, wordt dit vastgelegd in het logboek beeldgebruik.

Verwijdering

Na afloop van de vastgestelde bewaartermijn worden de videobeelden automatisch overschreven. Wanneer beelden die gericht zijn bewaard vanwege een incident worden verwijderd, wordt ook dit vastgelegd in het logboek beeldgebruik. Systeemloggegevens en logboekgegevens hebben ieder een eigen bewaartermijn, los van die van de videobeelden.

Uitwerking Scenario B - Cloudopslag

Verzameling en verstrekking van beelden, de registratie in de logboeken en de systeemlogging verlopen bij cloudopslag gelijk aan scenario A. De verschillen zitten in het gebruik, de opslag en de verwijdering.

Gebruik

Geautoriseerde medewerkers, opgenomen in de autorisatiematrix, kunnen beelden live zien en/of raadplegen via de beheer- en viewsoftware, die verbinding maakt met de cloudomgeving van de leverancier. Dit kan via lokaal geïnstalleerde software op een workstation, laptop of tablet, of volledig online via een browser. In beide gevallen wordt de grens van het fysiek of logisch gescheiden netwerk waarop de camera's zijn aangesloten gepasseerd. Toegang blijft beperkt tot geautoriseerde gebruikers en verloopt uitsluitend via een beveiligde verbinding met MFA en op beheerde apparatuur. Toegang op afstand, buiten de locatie, is daarnaast beperkt tot calamiteiten buiten Scholttijd, met uitsluitend kijkrechten.

Opslag

Het beeldmateriaal wordt via een fysiek of logisch gescheiden netwerk doorgezonden naar een cloudomgeving van de leverancier. De opslag en beschikbaarstelling van beelden vinden daarmee (deels) buiten de eigen infrastructuur van het schoolbestuur plaats. De bewaartermijn wordt contractueel vastgelegd in de verwerkersovereenkomst. Vindt de opslag plaats buiten de Europese Economische Ruimte (EER) in een land zonder adequaatheidsbesluit van de Europese Commissie, dan zijn aanvullende waarborgen (zoals modelcontractbepalingen) en een Data Transfer Impact Assessment (DTIA) nodig.

Verwijdering

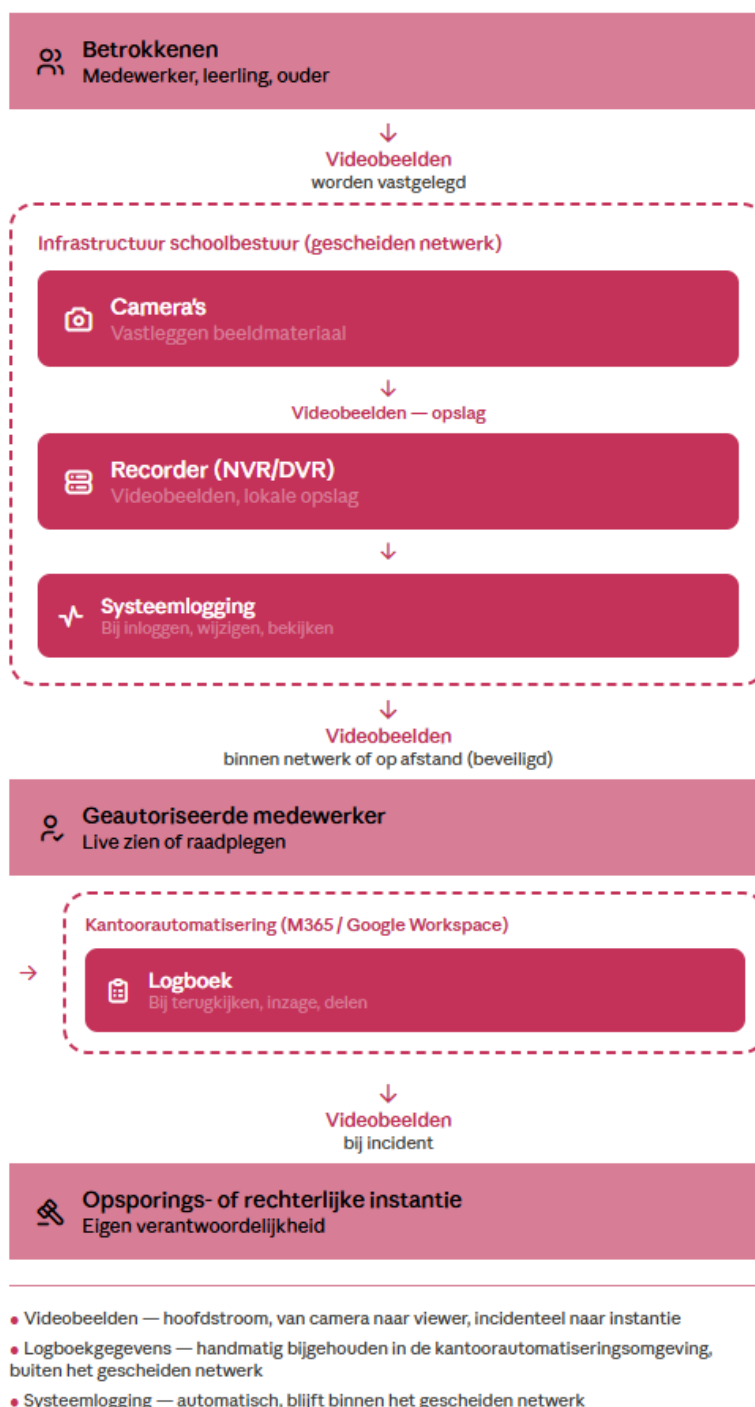
Het overschrijfbeleid voor videobeelden wordt contractueel vastgelegd in de verwerkersovereenkomst. Na afloop van de overeengekomen bewaartermijn worden de beelden overschreven.

Architectuurschets/Gegevensstroomdiagram

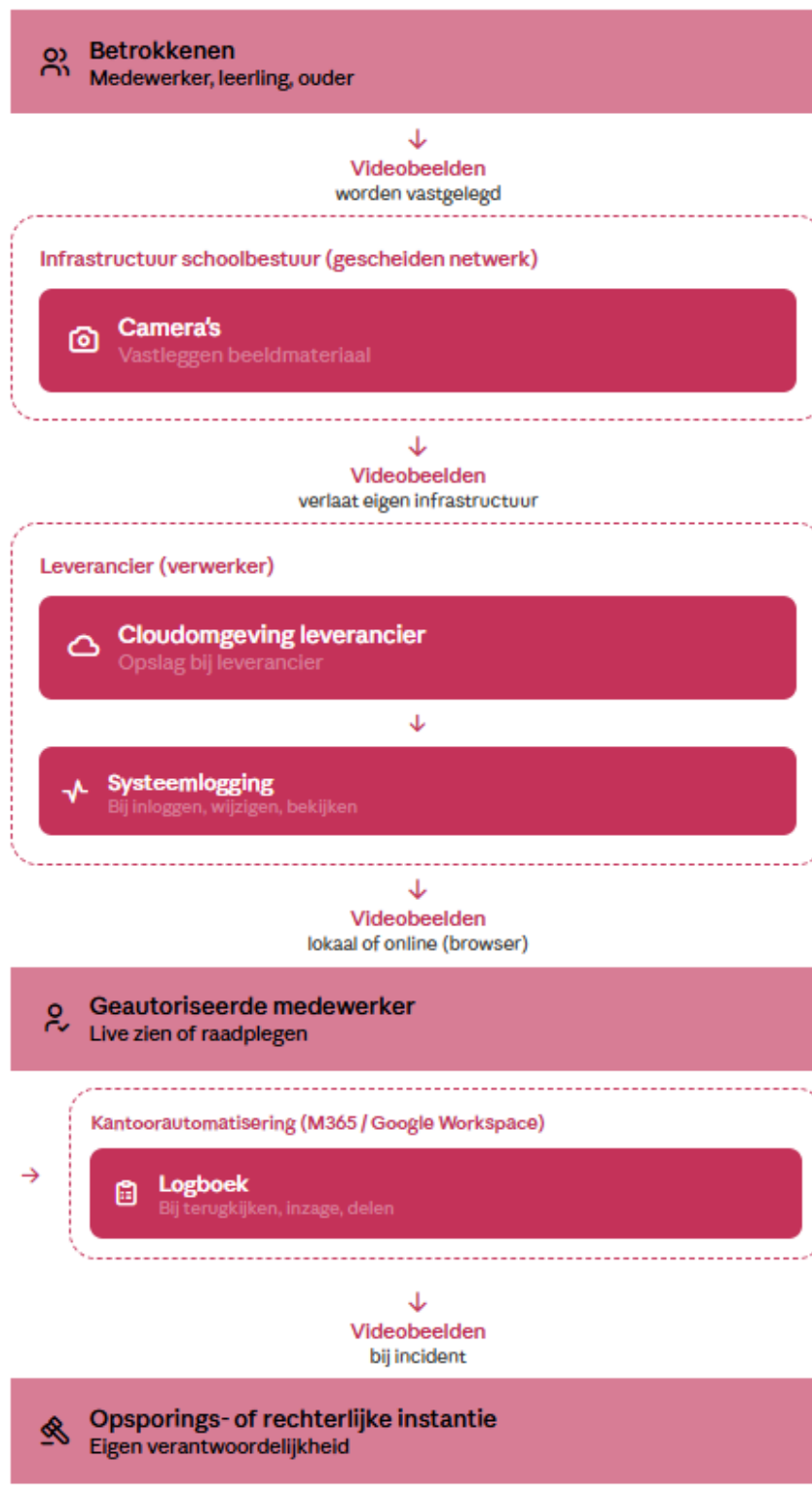
Voor de architectuurschets/gegevensstroomdiagram, zijn er twee mogelijke opties:

- Scenario A: lokale opslag
- Scenario B: cloudopslag

Uitwerking Scenario A - Lokale opslag



Uitwerking Scenario B - Cloudopslag



- Videobeelden — hoofdstroom, van camera naar leverancier naar viewer, incidenteel naar instantie
- Logboekgegevens — handmatig bijgehouden in de kantoorautomatiseringsomgeving, buiten de leverancierscloud
- Systeemlogging — automatisch, blijft binnen de cloudomgeving van de leverancier

4. Verwerkingsdoeleinden

De AVG heeft het uitgangspunt dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld. De vaststelling van de verwerkingsdoeleinden is een noodzakelijke voorwaarde om te kunnen beoordelen of de gegevensverwerkingen rechtmatig zijn (Deel B) en om vast te stellen welke maatregelen getroffen dienen te worden om de risico's (Deel C) te voorkomen of te verkleinen (Deel D).

De doeleinden 1 tot en met 5 zijn samengesteld op basis van de doeleinden waarvoor videobewaking volgens de EDPB-richtsnoeren 3/2019 doorgaans wordt ingezet (par. 15 en 137), mede geïnspireerd op artikel 38 van het vervallen Vrijstellingsbesluit Wbp. De doeleinden 6 en 7 zijn hierop een aanvulling, voortkomend uit de technische en organisatorische maatregelen in deze DPIA. De doeleinden 1 tot en met 4 worden per camera vastgesteld in het cameraoverzicht. De doeleinden 5 tot en met 7 gelden voor het cameratoezicht als geheel.

De verwerkingsdoeleinden zijn schematisch weergegeven en gekoppeld aan de verwerking.

Tabel 4.1 Verwerkingsdoeleinden en verwerking

Doeleinde verwerking	Gegevensverwerkingen	Toelichting
De bescherming van de veiligheid en gezondheid van leerlingen, medewerkers en bezoekers	Vastleggen, opslaan, raadplegen, gebruiken, verwijderen van beeldmateriaal van alle betrokkenen die zich in of rond de schoollocatie bevinden	Scholen hebben een zorgplicht voor de veiligheid van iedereen op het schoolterrein. Cameratoezicht kan bijdragen aan het vroegtijdig signaleren van gevaarlijke situaties en het achteraf reconstrueren van incidenten waarbij de veiligheid of gezondheid van betrokkenen in het geding was
De beveiliging van de toegang tot gebouwen en terreinen, waaronder mede begrepen het weren van onbevoegden	Vastleggen, opslaan, raadplegen, gebruiken, verwijderen van beeldmateriaal van personen die de school betreden of verlaten	Scholen zijn in beginsel toegankelijk voor leerlingen, medewerkers en genodigden. Cameratoezicht bij ingangen en toegangspunten maakt het mogelijk om de toegang te monitoren en onbevoegde aanwezigheid te signaleren en te documenteren
Het voorkomen en registreren van overlast en strafbare feiten zoals vandalisme, diefstal en inbraak	Vastleggen, opslaan, raadplegen, gebruiken, verwijderen van beeldmateriaal van alle betrokkenen die zich in of rond de schoollocatie bevinden	Schoolgebouwen en -terreinen zijn kwetsbaar voor vandalisme, diefstal en inbraak, met name buiten de Gebruikstijden. Cameratoezicht heeft een preventieve werking en biedt bij een incident de mogelijkheid om beelden als bewijsmateriaal ter beschikking te stellen aan de politie of justitie. Camera's die uitsluitend voor dit doeleinde en/of doeleinde 4 worden ingezet, nemen alleen buiten de Gebruikstijden op (zie hoofdstuk 17)
De bewaking van zaken die zich in de gebouwen of op de terreinen bevinden	Vastleggen, opslaan, raadplegen, gebruiken, verwijderen van beeldmateriaal van ruimtes en terreinen waar zich eigendommen van de school of van betrokkenen bevinden	Scholen beheren eigendommen van aanzienlijke waarde, zowel in de gebouwen als op de terreinen, zoals ICT-apparatuur, kostbare apparatuur in praktijklokalen, muziekinstrumenten, sportmaterialen en materialen op het schoolplein. Cameratoezicht op relevante ruimtes en terreinen ondersteunt de bewaking daarvan en maakt het mogelijk om bij vermissing of beschadiging de

		toedracht te achterhalen. Camera's die uitsluitend voor dit doeleinde en/of doeleinde 3 worden ingezet, nemen alleen buiten de Gebruikstijden op (zie hoofdstuk 17)
Het vastleggen van incidenten ten aanzien van de in punt 1 t/m 4 genoemde doeleinden	Vastleggen, opslaan, raadplegen, gebruiken en verwijderen van beeldmateriaal van een incident dat zich voordoet binnen de doeleinden 1 tot en met 4, en ook het gericht bewaren van dat beeldmateriaal buiten de reguliere bewaartermijn totdat het incident is afgehandeld	Wanneer zich een incident voordoet, moet het schoolbestuur dit kunnen vastleggen om het te onderzoeken, af te handelen en zo nodig maatregelen te treffen. Zonder vastlegging kan een incident achteraf niet worden gereconstrueerd en kunnen de doeleinden 1 tot en met 4 niet daadwerkelijk worden gerealiseerd. Dit doeleinde geldt voor het cameratoezicht als geheel en wordt niet per camera vastgesteld. Het gericht bewaren en het latere verwijderen van beeldmateriaal wordt vastgelegd in het logboek beeldgebruik
Beveiliging, controle en ook verantwoording van de verwerking	Automatisch vastleggen, opslaan, raadplegen en verwijderen van systeemdata (metadata/logging) over toegang tot en handelingen binnen het camerasysteem, en ook het vastleggen, opslaan, raadplegen en verwijderen van gestructureerde registraties in het logboek wijzigingen camera-instellingen, het logboek reglement afwijkingen en het logboek beeldgebruik	Het schoolbestuur is als verwerkingsverantwoordelijke gehouden om de beveiliging en het rechtmatig gebruik van het camerasysteem te waarborgen en hierover verantwoording af te leggen. Dit doeleinde omvat zowel de technische maatregelen (automatische logging van inlogpogingen, handelingen, instellingswijzigingen, rechtenwijzigingen en exports) als de organisatorische maatregelen (gestructureerde registratie van wijzigingen aan privacygevoelige camera-instellingen in het logboek wijzigingen camera-instellingen, van (tijdelijke) afwijkingen van het reglement in het logboek reglement afwijkingen en van raadplegingen, besluiten tot bewaren of verwijderen, inzage aan derden en delingen met derden in het logboek beeldgebruik, telkens inclusief wanneer, door wie, de reden en wie het besluit heeft genomen). Samen maken deze maatregelen ongeautoriseerd of afwijkend gebruik detecteerbaar en aantoonbaar
Verstrekking van incidentgegevens aan derden (op eigen besluit - op vordering)	Raadplegen, gebruiken en verstrekken van beeldmateriaal aan politie of justitie, en ook het vastleggen van de verstrekking in het logboek beeldgebruik	Bij incidenten kan het noodzakelijk zijn om beeldmateriaal te verstrekken aan derden (zoals politie of justitie). Dit doeleinde omvat het selecteren en verstrekken van relevante beelden naar aanleiding van een concreet incident, op basis van een formele vordering of een eigen besluit van het schoolbestuur om aangifte te ondersteunen. Elke verstrekking wordt geregistreerd in het logboek beeldgebruik, inclusief aan wie is verstrekt, op wiens besluit, de reden en het tijdstip. Het schoolbestuur beoordeelt per verstrekking of hiervoor een rechtmatige grondslag bestaat

De doeleinden in tabel 4.1 zijn limitatief: cameratoezicht wordt uitsluitend voor deze doeleinden ingezet en voor geen enkel ander doel. Wat niet onder een van deze doeleinden valt, is niet toegestaan, ook niet als het praktisch of wenselijk lijkt. Ter verduidelijking staan hieronder voorbeelden van doeleinden waarvoor cameratoezicht in geen geval mag worden ingezet. Deze voorbeelden zijn niet uitputtend: zij illustreren de grens, maar trekken die niet. De grens wordt uitsluitend bepaald door tabel 4.1.

- Het beoordelen van het functioneren of de prestaties van leerlingen of medewerkers, of het structureel volgen van hun gedrag
- De handhaving van de openbare orde, dat is een taak van de gemeente
- Het vastleggen of reconstrueren van verkeersongevallen of andere voorvallen op de openbare weg. Camera's behoren ook niet op de openbare ruimte te zijn gericht
- Commerciële doeleinden, zoals marketing of het publiceren of verkopen van beelden
- Analytische doeleinden, zoals het tellen of profileren van personen of het analyseren van gedragspatronen
- Onderwijskundige doeleinden, zoals het observeren of evalueren van lessen
- De handhaving van gedragsregels die niet onder één van de doeleinden in tabel 4.1 vallen, zoals het rookverbod of het telefoonverbod
- Het verstrekken van beelden aan ouders, media of verzekeraars. Bij een gerechtvaardigd inzageverzoek worden beelden alleen getoond en niet verstrekt (zie hoofdstuk 14 en 18)

5. Betrokken partijen

De betrokken partijen en hun AVG-rol verschillen per inrichtingsscenario:

- In scenario A1 - de meest voorkomende situatie - is de opslag volledig lokaal en heeft de leverancier of onderhoudspartij geen Structurele toegang tot het systeem. Het schoolbestuur treedt op als verwerkingsverantwoordelijke en verwerkt de beelden volledig binnen de eigen organisatie. Een verwerkersovereenkomst met de leverancier is in dit scenario niet vereist.
- In scenario A2 is de opslag volledig lokaal en heeft de externe onderhoudspartij Structurele toegang tot het systeem. Het schoolbestuur treedt op als verwerkingsverantwoordelijke en de externe onderhoudspartij als verwerker. Een verwerkersovereenkomst met de externe onderhoudspartij is in dit scenario vereist.
- In scenario B1 maakt de opslag, beheer- en/of viewsoftware gebruik van een cloudcomponent bij de externe onderhoudspartij of cloudleverancier. Een verwerkersovereenkomst met de externe onderhoudspartij of cloudleverancier is dan vereist.
- In scenario B2 is gelijk aan B1, maar daarnaast heeft de externe onderhoudspartij Structurele toegang tot het systeem. Ook daarvoor is een verwerkersovereenkomst vereist. Is er met de externe onderhoudspartij al een verwerkersovereenkomst voor cloudopslag, dan kunnen beide worden samengevoegd.

Een opsporings- of rechterlijke instantie die beelden ontvangt, treedt op als zelfstandig verwerkingsverantwoordelijke voor die beelden vanaf het moment van overdracht.

De hieronder benoemde partijen zijn betrokken bij de gegevensverwerking.

Tabel 5.1 Betrokken partijen en gegevensverwerking

Naam partij	AVG-rol	Functie/taak	Betrokken persoonsgegevens	Verstrekker of ontvanger	De volgende personen hebben directe toegang tot deze persoonsgegevens
Schoolbestuur	Verwerkingsverantwoordelijke	Beveiliging van personen en middelen	Beeldmateriaal, metadata/logging, logboekgegevens	Verstrekker	Medewerkers die zijn opgenomen in de autorisatiematrix
Externe onderhoudspartij	Verwerker, uitsluitend bij Structurele toegang	Onderhoud van het camera-systeem	Beeldmateriaal, metadata/logging	Ontvanger	Door de onderhoudspartij aangewezen technisch medewerkers die betrokken zijn bij onderhoud
Cloudopslag leverancier	Verwerker	Verzorgt de opslag van beeldmateriaal op een extern platform	Beeldmateriaal, metadata/logging	Ontvanger	Technisch beheerders van de cloudleverancier, uitsluitend voor zover noodzakelijk voor de uitvoering van de overeenkomst

6. Belangen bij de gegevensverwerking

Het schoolbestuur (verwerkingsverantwoordelijke) heeft belang bij een goed werkend en betrouwbaar digitaal systeem, waardoor zij de veiligheid van personen en eigendommen kan borgen.

Tabel 6.1 Belangen bij de gegevensverwerking

Naam partij	Belangen
Schoolbestuur	Het waarborgen van de veiligheid en gezondheid van leerlingen, medewerkers en bezoekers op het schoolterrein. Het beschermen van eigendommen van de school tegen diefstal, vandalisme en inbraak. Het kunnen reconstrueren van incidenten en het ondersteunen van juridische procedures, zoals het doen van aangifte. Het voldoen aan de zorgplicht die voortvloeit uit de arbeidsomstandighedenwetgeving en de onderwijswetgeving. Het handhaven van de toegangsbeveiliging van gebouwen en terreinen.
Schoolbestuur/ Externe Onderhoudspartij	Het goed werkend en onderhouden van het camerasysteem van het schoolbestuur. Een commercieel belang: een betrouwbaar product en goede dienstverlening ondersteunen de reputatie en marktpositie. Het kunnen uitvoeren van onderhoud en updates ter borging van de continuïteit en veiligheid van het systeem.
Cloudopslag leverancier	Het leveren van een betrouwbare en veilige opslagomgeving aan het schoolbestuur. Een commercieel belang: een goed functionerende dienst ondersteunt de reputatie en marktpositie. Het borgen van de continuïteit en beschikbaarheid van de opgeslagen gegevens.

7. Verwerkingslocaties

De verwerkingslocaties zijn volledig lokaal gebonden en zijn daarom alleen in de lokale DPIA terug te vinden.

8. Data Transfer Impact Assessment (DTIA)

De AVG bevat specifieke regels voor de doorgifte van persoonsgegevens naar landen buiten de Europese Economische Ruimte (EER). In beginsel mogen persoonsgegevens alleen worden overgedragen aan landen buiten de EER als het land een 'passend beschermingsniveau' heeft. Dat niveau kan op verschillende manieren worden bepaald: een multinational kan bindende bedrijfsvoorschriften vaststellen (BCR's), de EU-standaardcontractbepalingen (SCC) toepassen of alleen overdragen aan landen waarvoor de Europese Commissie een zogeheten adequaatheidsbesluit¹² heeft genomen.

Als het schoolbestuur gebruikmaakt van een verwerker die persoonsgegevens buiten de EER opslaat of verwerkt, of daar toegang toe heeft, bijvoorbeeld via een cloudleverancier, is sprake van doorgifte buiten de EER. Valt het ontvangende land niet onder een adequaatheidsbesluit en vindt de doorgifte plaats op basis van passende waarborgen, zoals SCC's, dan is een DTIA vereist. De verantwoordelijkheid voor het uitvoeren van de DTIA ligt bij de exporteur: de partij binnen de EER die de overeenkomst sluit met de partij buiten de EER.

- Sluit het schoolbestuur zelf een overeenkomst met een verwerker buiten de EER, dan is het schoolbestuur de exporteur. Het voert de DTIA dan zelf uit, met medewerking van die verwerker.
- Schakelt een verwerker binnen de EER een subverwerker buiten de EER in, dan is de verwerker de exporteur en voert die de DTIA uit. Het schoolbestuur vraagt de DTIA dan als verwerkingsverantwoordelijke op bij de verwerker en beoordeelt en legt de uitkomsten vast.

De DTIA is een afzonderlijk document waarnaar in de lokale DPIA wordt verwezen.

9. Technieken en methoden van gegevensverwerking

Artikel 32 AVG schrijft voor dat passende technische en organisatorische maatregelen worden getroffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Om te beoordelen in hoeverre hieraan wordt voldaan, is voor het camerasysteem zowel een technisch onderzoek als een BIV-classificatie uitgevoerd. Daarnaast is beoordeeld of het systeem gebruikmaakt van AI of algoritmes.

a. Technisch onderzoek

Het camerasysteem bestaat uit fysieke en digitale componenten: camera's, een recorder, beheerssoftware en in sommige gevallen cloudopslag. Voor een rechtmatig en veilig camerasysteem gelden de volgende technische beveiligingsmaatregelen als norm (SOLL):

Het camerasysteem is geplaatst op een fysiek of logisch gescheiden netwerk (VLAN) dat niet rechtstreeks toegankelijk is vanuit het reguliere schoolnetwerk of internet. Toegang tot het camerasysteem en beeldmateriaal is beperkt tot geautoriseerde functionarissen. Accounts zijn persoonsgebonden, bij online of remote toegang beveiligd met MFA en verder met MFA of wachtzinnen van minimaal 15 tekens. Opgeslagen beeldmateriaal is versleuteld (encryption at rest) en bij transport over een netwerk, waaronder cloudopslag en remote toegang, wordt eveneens versleuteling toegepast (encryption in transit). Autorisaties worden direct ingetrokken bij functiewijziging of uitdiensttreding en er is een actueel overzicht van alle accounts met toegang tot het camerasysteem. Firmware van camera's en recorder en software van het beheersysteem worden tijdig bijgewerkt. Er is een proces voor het signaleren en doorvoeren van beveiligingsupdates. De recorder en eventuele server bevinden zich in een afgesloten ruimte die alleen toegankelijk is voor geautoriseerd personeel. Het camerasysteem registreert wie wanneer beelden heeft bekeken, geëxporteerd of verwijderd en de logbestanden worden periodiek gecontroleerd.

¹² https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

b. ROSA-certificeringsschema en BIV-classificatie

Het ROSA-certificeringsschema is formeel niet van toepassing op camerasystemen, aangezien deze geen digitaal onderwijsmiddel zijn. Het schema biedt echter wel een bruikbaar referentiekader voor de beoordeling van technische beveiligingsmaatregelen.

Het schoolbestuur stelt de BIV-classificatie vast voor het camerasysteem. Voor cameratoezicht in het funderend onderwijs geldt het volgende als uitgangspunt:

- *Beschikbaarheid: Midden.* Het camerasysteem moet beschikbaar zijn om het beoogde doel te realiseren. Kortstondige uitval is aanvaardbaar. Langdurige onbeschikbaarheid ondermijnt de doelstelling. Een hoog niveau is niet noodzakelijk omdat cameratoezicht een aanvullende maatregel is naast fysiek toezicht en andere veiligheidsmaatregelen.
- *Integriteit: Midden.* Beeldmateriaal moet authentiek en ongewijzigd zijn om bruikbaar te zijn als bewijsmateriaal. De kans op daadwerkelijke manipulatie van beelden op de recorder is in de praktijk zeer klein: dit vereist fysieke toegang tot de recorder én technische kennis om beelden op bestandsniveau te wijzigen zonder sporen achter te laten. De bestaande maatregelen: fysieke beveiliging van de recorder, autorisatie en logging, beperken dit risico.
- *Vertrouwelijkheid: Hoog.* Camerabeelden bevatten onder andere persoonsgegevens van minderjarigen in een kwetsbare positie. Ongeautoriseerde toegang tot beeldmateriaal kan leiden tot ernstige schade voor betrokkenen. De vertrouwelijkheid vereist het hoogste beschermingsniveau.

c. Algoritmes en AI

Het gebruik van geautomatiseerde analyse, algoritmes of AI-functionaliteit, waaronder: gezichtsherkenning, gedragsdetectie of andere vormen van geautomatiseerde besluitvorming op basis van beeldmateriaal, is binnen de scope van deze DPIA uitgesloten. Camerasystemen met dergelijke functionaliteit zijn in de onderwijscontext niet toegestaan, gelet op de disproportionele inbreuk op de grondrechten van minderjarigen en het ontbreken van een toereikende wettelijke grondslag. Als een schoolbestuur overweegt een camerasysteem met AI-functionaliteit in te zetten, valt dit buiten deze DPIA en dient een afzonderlijke beoordeling plaats te vinden.

d. Bevindingen

De in onderdeel a. beschreven technische maatregelen vormen de norm (SOLL) voor een rechtmatig ingericht camerasysteem. Afwijkingen van deze norm komen aan het licht bij het doorlopen van de risicotabel (hoofdstuk 20) en de maatregelentabel (hoofdstuk 21): het schoolbestuur beoordeelt per risico of de bijbehorende maatregelen zijn getroffen. Waar dat niet het geval is, volgen daaruit concrete verbeterpunten.

10. Juridisch en beleidsmatig kader

Hieronder wordt alle wet- en regelgeving benoemd met mogelijke gevolgen voor de gegevensverwerkingen

(Inter-)Nationale wetgeving

De AVG vormt het primaire juridische kader voor cameratoezicht. Camerabeelden zijn persoonsgegevens zodra daarop natuurlijke personen herkenbaar in beeld zijn. Het schoolbestuur is als verwerkingsverantwoordelijke verplicht een rechtmatige grondslag te hebben, betrokkenen te informeren, bewaartermijnen te hanteren en passende technische en organisatorische maatregelen te treffen. De UAVG werkt de AVG uit voor de Nederlandse context en regelt onder meer het toezicht door de Autoriteit Persoonsgegevens.

Op grond van de WPO en WVO 2020 heeft het schoolbestuur een wettelijke zorgplicht voor de veiligheid van leerlingen. Deze zorgplicht vormt de feitelijke aanleiding voor cameratoezicht. Daarnaast heeft het schoolbestuur als werkgever een zorgplicht voor de veiligheid en gezondheid van medewerkers op grond van de Arbowetgeving. Inzet van cameratoezicht in het kader van het arbobeleid vereist instemming van de personeelsgeleding van de medezeggenschapsraad.

Indien beeldmateriaal wordt verstrekt aan politie of justitie, zijn de bepalingen van het Wetboek van Strafvordering van toepassing. Het schoolbestuur dient procedures te hebben voor de beveiligde overdracht en registratie van verstrekt beeldmateriaal.

Richtsnoeren en toezichtkader

De AP¹³ licht op haar website toe welke eisen de AVG stelt aan cameratoezicht door organisaties, waaronder scholen, zoals noodzaak, het uitschakelen van niet-noodzakelijke functies, beveiliging, instemming van de medezeggenschapsraad, transparantie en bewaartermijnen.

Op Europees niveau vormen de EDPB-Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur (versie 2.0, 29 januari 2020)¹⁴ het overkoepelende kader. De richtsnoeren behandelen het toepassingsgebied, de rechtmatigheid van de verwerking (waaronder de doelbepaling per camera, de grondslagen en de noodzaak), de verstrekking van beelden aan derden en aan rechtshandavingsinstanties, de verwerking van bijzondere categorieën van persoonsgegevens waaronder biometrische gegevens, de rechten van betrokkenen (inzage, wissing en bezwaar), gelaagde transparantie via waarschuwingsborden en een tweede informatielaag, opslagtermijnen, technische en organisatorische maatregelen waaronder gegevensbescherming door ontwerp en door standaardinstellingen en de gegevensbeschermingseffectbeoordeling. Al deze onderwerpen zijn in deze DPIA als toetsingskader meegenomen. De verwerkingsdoeleinden zijn mede gebaseerd op de doeleinden die de EDPB noemt (par. 15 en 137).

Hoewel juridisch niet bindend, vormen de richtsnoeren van de EDPB en de uitleg van de AP de gezaghebbende interpretatie van de AVG-vereisten. Zij zijn in deze DPIA bepalend voor de beoordeling van de rechtmatigheid, noodzaak en proportionaliteit van het cameratoezicht, voor de inschatting van de risico's en voor de keuze van de maatregelen.

Intern beleid

Het IBP-beleid legt de uitgangspunten vast voor informatiebeveiliging en privacy binnen het schoolbestuur. Cameratoezicht dient te passen binnen de kaders van dit beleid, dat onder meer bepaalt welke rollen verantwoordelijk zijn voor de beveiliging van persoonsgegevens en hoe incidenten worden afgehandeld.

Het normenkader IBP werkt de beveiligings- en privacynormen concreet uit. De technische en organisatorische maatregelen rond cameratoezicht zoals: netwerksegmentatie, toegangsbeveiliging en bewaartermijnen, worden aan dit normenkader getoetst en vormen daarmee de meetlat voor de beoordeling van maatregelen in deze DPIA.

¹³ [Regels cameratoezicht voor organisaties | Autoriteit Persoonsgegevens](#)

¹⁴ EDPB, *Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur*, versie 2.0, 29 januari 2020. Beschikbaar via: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_nl.pdf

Het reglement cameratoezicht is een vereiste voorwaarde voor rechtmatig cameratoezicht. Hierin legt het schoolbestuur vast voor welk doel camera's worden ingezet, op welke locaties, wie toegang heeft tot de beelden, wat de bewaartermijnen zijn en hoe betrokkenen worden geïnformeerd.

Cameratoezicht dient te zijn opgenomen in de privacyverklaring van de school, zodat betrokkenen weten dat zij worden gefilmd, voor welk doel en wat hun rechten zijn. Het autorisatiebeleid regelt daarnaast welke functionarissen toegang hebben tot het camerasysteem en de beelden, waarbij autorisaties worden ingetrokken bij functiewijziging of uitdiensttreding.

11. Bewaartermijnen

Het uitgangspunt is dat het schoolbestuur zelf als verwerkingsverantwoordelijke doel en middelen van de verwerking van persoonsgegevens bepaalt en daarom ook verantwoordelijk is voor het vaststellen en nakomen van de bewaartermijnen op basis van geldende wet- en regelgeving, sectorale vaststellingen en best practices.

Motivatie voor de bewaartermijnen

De EDPB-richtsnoeren 3/2019 (par. 121) gaan uit van een korte standaardtermijn en stellen dat een bewaartermijn langer dan 72 uur nader moet worden gemotiveerd. De Autoriteit Persoonsgegevens heeft voor de Nederlandse context vier weken vastgesteld als bovengrens. Deze vier weken geldt als maximum, niet als standaard. Buiten de zomervakantie kunnen schoolbesturen beelden in de praktijk altijd binnen drie weken beoordelen. Een bewaartermijn van drie weken is in die periode de meer gepaste keuze. Langere bewaring is zonder specifieke aanleiding disproportioneel.

Tijdens de zomervakantie, de enige schoolvakantie die langer duurt dan de standaardbewaartermijn, kan de bewaartermijn tijdelijk worden verlengd tot maximaal zes weken. Het voorbeeld dat de EDPB bij de motivering van langere termijnen geeft (par. 121), laat zien dat het langer gesloten zijn van een locatie wegens vakantie een langere opslagperiode kan rechtvaardigen, omdat schade of incidenten dan pas later worden vastgesteld. Voor leerlingen duurt de zomervakantie doorgaans zes weken, maar (een deel van de) medewerkers is in de praktijk vaak al eerder terug op school en kan binnen deze termijn vaststellen of er schade is ontstaan of een incident heeft plaatsgevonden en of het noodzakelijk is beelden terug te kijken. Een langere bewaartermijn dan zes weken is daarom niet nodig. De verlenging geldt uitsluitend voor reguliere beelden en wordt technisch ingesteld in het camerasysteem. Na de zomervakantie valt de bewaartermijn automatisch terug naar de reguliere termijn of, als het camerasysteem dat niet ondersteunt, handmatig door de systeemeigenaar na de eerste schooldag en uiterlijk op de tweede schooldag, vastgelegd in het logboek wijzigingen camera-instellingen.

Bij incidenten, of het nu gaat om een veiligheids- of gezondheidsincident, een onbevoegde toegang, of vandalisme, diefstal of inbraak, worden de betreffende beelden langer bewaard zolang dat aantoonbaar noodzakelijk is. De bewaartermijn loopt door tot het incident volledig is afgehandeld, de beelden zijn overgedragen aan een opsporingsinstantie, of de beelden anderszins geen aantoonbaar doel meer dienen. Na afhandeling van het incident of overdracht aan politie en/of justitie worden de bij de school aanwezige kopieën zo spoedig mogelijk (maar uiterlijk binnen drie weken) verwijderd.

Systeemloggegevens worden bewaard om ongeautoriseerd gebruik detecteerbaar te maken en de integriteit van het systeem te borgen. Dertien maanden is een gangbare praktijknorm: onderzoek toont aan dat een datalek gemiddeld zeven maanden onopgemerkt blijft, waardoor deze termijn voldoende ruimte biedt voor forensisch onderzoek. De logboeken dienen als verantwoordingsinstrument voor het

gebruik van het camerasysteem en het beeldmateriaal. Een minimale bewaartermijn van dertien maanden waarborgt dat raadplegingen, besluiten en verstrekkingen aantoonbaar zijn bij klachten, bezwaar of toezicht. Na twee jaar hebben logboekgegevens geen aantoonbaar verantwoordingsdoel meer.

Tabel 11.1 Bewaartermijnen

Gegevensverwerking	Bewaartermijn
Bescherming veiligheid en gezondheid	• Standaard drie weken, die met een gemotiveerde reden kan worden verlengd tot maximaal vier weken, waarna automatisch overschreven • Tijdens de zomervakantie maximaal zes weken, waarna automatisch overschreven. Na de zomervakantie terugval naar de reguliere termijn: automatisch als het camerasysteem dit ondersteunt, anders handmatig door de systeemeigenaar na de eerste schooldag en uiterlijk op de tweede schooldag • Bewaard totdat het incident volledig is afgehandeld, waarna zo spoedig mogelijk (maar uiterlijk binnen drie weken) verwijderd
Beveiliging toegang gebouwen en terreinen	
Voorkomen en registreren overlast en strafbare feiten	
Bewaking van zaken in gebouwen en op terreinen	
Vastleggen van incidenten	
Beveiliging, controle en ook verantwoording van de verwerking	• Dertien maanden voor systeemloggegevens • Minimaal dertien maanden en maximaal twee jaar voor logboekgegevens
Verstrekking van incidentgegevens aan derden (op eigen besluit/ op vordering)	• Geen zelfstandige bewaartermijn. De bewaartermijn van het beeldmateriaal wordt bepaald door de doeleinden 1-5. De registratie van de verstrekking in het logboek beeldgebruik wordt bewaard volgens de bewaartermijn van de logboekgegevens (doeleinde 6). Bij een vordering tot bewaring op grond van art. 126ni Sv geldt de in de vordering bepaalde termijn.

6. Deel B: Beoordeling rechtmatigheid gegevensverwerkingen

Dit hoofdstuk beoordeelt of het cameratoezicht rechtmatig is, op basis van de beschrijving in Deel A. Het toetst de rechtsgrond, doelbinding, noodzakelijkheid, proportionaliteit en subsidiariteit, de belangen van kinderen en de rechten van betrokkenen. Ook wordt toegelicht in welke situaties een verwerkersovereenkomst nodig is.

12. Rechtsgrond

Als onderdeel van de verantwoordingsplicht dient te worden aangetoond dat de verwerking van persoonsgegevens op een rechtmatige grondslag berust. Deze grondslag moet worden bepaald voordat het schoolbestuur begint met het verwerken van persoonsgegevens.

Artikel 6 AVG kent 6 grondslagen:

- a) Toestemming van de betrokkene (art. 6, eerste lid, sub a, AVG)
- b) Uitvoering van een overeenkomst (art. 6, eerste lid, sub b, AVG)
- c) Wettelijke verplichting¹⁵ (art. 6, eerste lid, sub c, AVG)
- d) Vitaal belang van de betrokkene (art. 6, eerste lid, sub d, AVG)
- e) Taak van algemeen belang¹⁶ (of openbaar gezag) (art. 6, eerste lid, sub e, AVG)
- f) Gerechtvaardigd belang (art. 6, eerste lid, sub f, AVG)

Voor cameratoezicht door schoolbesturen in het funderend onderwijs geldt als verwerkingsgrondslag de **taak van algemeen belang** in de zin van artikel 6, eerste lid, sub e, van de AVG. Schoolbesturen voeren op grond van de Wet op het primair onderwijs (WPO) respectievelijk de Wet voortgezet onderwijs 2020 (WVO 2020) een wettelijk opgedragen taak uit. De AVG staat toe dat zij zich bij de uitvoering van die taak op artikel 6, eerste lid, sub e, beroepen. Ook de EDPB-richtsnoeren voor videoapparatuur erkennen deze grondslag voor cameratoezicht in het kader van een wettelijk opgedragen publieke taak (par. 41).

De wettelijke zorgplicht voor de veiligheid op school is verankerd in artikel 4c WPO respectievelijk artikel 3.40 WVO 2020. Op grond van deze bepalingen zorgt het schoolbestuur voor de sociale, psychische en fysieke veiligheid van leerlingen. Voor medewerkers geldt daarnaast als **wettelijke verplichting** (artikel 6, eerste lid, sub c, AVG) de zorgplicht van de werkgever voor veiligheid en gezondheid op grond van artikel 3 Arbowet.

De doeleinden gericht op het voorkomen en registreren van vandalisme, diefstal en inbraak en op de bewaking van zaken (doeleinden 3 en 4) zijn niet afzonderlijk in de onderwijswetgeving opgenomen. Zij zijn wel noodzakelijk voor de uitvoering van de wettelijke taak. Vandalisme en inbraak leiden tot fysiek onveilige situaties, zoals glasschade, brandgevaar en de aanwezigheid van onbevoegden. Daarnaast tasten zij de veiligheidsbeleving van leerlingen en medewerkers aan: een school waar regelmatig wordt ingebroken of vernield, voelt niet als een veilige plek. De zorgplicht ziet niet alleen op de feitelijke veiligheid, maar ook op de ervaren veiligheid en ook daaraan dragen deze doeleinden bij. Dat deze

¹⁵ De wettelijke verplichting (rechtsgrond c) hoeft niet noodzakelijkerwijs te bestaan uit een expliciete verplichting om persoonsgegevens te verwerken. Ook is mogelijk dat de verwerking van persoonsgegevens een basis vindt in een ruimer geformuleerde zorgplicht of wettelijke verplichting. Zonder verwerking van de persoonsgegevens moet het uitvoeren van een wettelijke verplichting redelijkerwijs niet goed mogelijk zijn.

¹⁶ Met betrekking tot rechtsgrond taak van algemeen belang geldt dat deze taak zal moeten blijken uit regelgeving die op de verwerkingsverantwoordelijke van toepassing is. Niet noodzakelijk is dat in de regelgeving expliciet is opgenomen dat ten behoeve van de vervulling van de wettelijke taak persoonsgegevens verwerkt mogen worden. Indien het noodzakelijk is om voor de uitvoering van de publieke taak persoonsgegevens te verwerken, kan de wettelijke grondslag voor de publieke taak ook worden beschouwd als grondslag voor de verwerking van persoonsgegevens.

doeleinden onder de zorgplicht vallen, betekent niet dat opnemen voor deze doeleinden tijdens de Gebruikstijden van de locatie noodzakelijk is (zie hoofdstuk 17).

Voor de beveiliging, controle en verantwoording van de verwerking, waaronder logging, geldt als grondslag de **wettelijke verplichting** (artikel 6, eerste lid, sub c, AVG) tot passende beveiliging en tot het kunnen aantonen van naleving (artikelen 5, tweede lid, 24 en 32 AVG). Verstrekking van beelden op een vordering van politie of justitie berust eveneens op een **wettelijke verplichting** (artikel 6, eerste lid, sub c, AVG). Verstrekking op eigen besluit van het schoolbestuur berust op de **taak van algemeen belang** (artikel 6, eerste lid, sub e, AVG).

DSB Oostenrijk. De Oostenrijkse toezichthouder (DSB, 6 september 2023, 2022-0.858.901) oordeelde dat een openbare school tijdens schooluren geen camera's mocht gebruiken in gangen en bij de ingang. Een openbare school is in Oostenrijk een overheidsinstantie. De school beriep zich op het gerechtvaardigd belang, wat zij als overheidsinstantie voor haar taken niet kon (art. 6 lid 1, tweede alinea, AVG). Daarnaast eist het Oostenrijkse grondrecht op gegevensbescherming voor overheidsinstanties een uitdrukkelijke en voldoende bepaalde wettelijke machtiging voor de verwerking (§ 1 lid 2 DSG). In Nederland is het bevoegd gezag doorgaans geen overheidsinstantie, maar een rechtspersoon die een wettelijke taak uitvoert. De AVG vereist voor die taak wel een wettelijke basis, maar geen specifieke wet per verwerking (art. 6 lid 3 en overweging 45 AVG). De zorgplicht voor de veiligheid op school (art. 4c WPO, art. 3.40 WVO 2020) kan daarom op grond van art. 6 lid 1 sub e jo. lid 3 AVG de grondslag voor cameratoezicht zijn, voor zover dat noodzakelijk is om de taak te vervullen (EDPB 3/2019, par. 41). Of die noodzaak tijdens de Gebruikstijden van de locatie bestaat, wordt beoordeeld in hoofdstuk 17.

Tabel 12.1 Rechtsgrond

Verwerkingsdoeleinden (zie hiervoor 4. Verwerkingsdoeleinden)	Grondslag AVG	Onderbouwing
Bescherming van de veiligheid en gezondheid van leerlingen, medewerkers en bezoekers	Art. 6 lid 1 sub e AVG - Algemeen belang voor medewerkers ook art. 6 lid 1 sub c AVG - Wettelijke verplichting	Zorgplicht veiligheid op school (art. 4c WPO / art. 3.40 WVO) Zorgplicht werkgever voor veiligheid en gezondheid (art. 3 Arbowet)
Beveiliging van de toegang tot gebouwen en terreinen, waaronder mede begrepen het weren van onbevoegden	Art. 6 lid 1 sub e AVG - Algemeen belang	Zorgplicht veiligheid op school (art. 4c WPO / art. 3.40 WVO)
Voorkomen en registreren van overlast en strafbare feiten zoals vandalisme, diefstal en inbraak	Art. 6 lid 1 sub e AVG - Algemeen belang	Zorgplicht veiligheid op school (art. 4c WPO / art. 3.40 WVO)
Bewaking van zaken die zich in de gebouwen of op de terreinen bevinden	Art. 6 lid 1 sub e AVG - Algemeen belang	Zorgplicht veiligheid op school (art. 4c WPO / art. 3.40 WVO)
Vastleggen van incidenten ten aanzien van de in punt 1 t/m 4 genoemde doeleinden	Art. 6 lid 1 sub e AVG - Algemeen belang voor medewerkers ook art. 6 lid 1 sub c	Zorgplicht veiligheid op school (art. 4c WPO / art. 3.40 WVO) Zorgplicht werkgever voor veiligheid en gezondheid (art. 3 Arbowet)

	AVG - Wettelijke verplichting	
Beveiliging, controle en ook verantwoording van de verwerking	Art. 6 lid 1 sub c AVG - Wettelijke verplichting	Passende beveiliging en aantoonbare naleving (art. 5 lid 2, 24 en 32 AVG)
Verstreking van incidentgegevens aan derden: • op eigen besluit • op vordering	Art. 6 lid 1 sub e AVG - Algemeen belang Art. 6 lid 1 sub c AVG - Wettelijke verplichting	Bij eigen besluit de zorgplicht veiligheid op school (art. 4c WPO / art. 3.40 WVO 2020) Vordering politie of justitie (art. 126nd / 126nda / 126ni Sv)

13. Bijzondere persoonsgegevens

De AVG kent een verzwaarde bescherming voor bijzondere categorieën persoonsgegevens, zoals gegevens over ras of etnische afkomst, gezondheid, religie, seksuele gerichtheid of biometrische gegevens die worden verwerkt met het oog op de unieke identificatie van personen. De verwerking van dergelijke gegevens is in beginsel verboden, tenzij een uitdrukkelijke uitzondering van toepassing is.

Cameratoezicht legt beeldmateriaal vast van personen die zich in of rond de schoollocatie bevinden. Hoewel beeldmateriaal in theorie bijzondere kenmerken zichtbaar kan maken, zoals huidskleur of het dragen van religieuze kleding, worden deze kenmerken niet gericht vastgelegd, niet geanalyseerd en niet als zodanig verwerkt. Het doel van het cameratoezicht is uitsluitend het bewaken van de veiligheid en het registreren van incidenten, niet het in kaart brengen van persoonskenmerken van betrokkenen.

Van biometrische verwerking is geen sprake: het camerasysteem bevat geen gezichtsherkenning of andere technologie die beeldmateriaal verwerkt met het oog op unieke identificatie.

Verwerking van bijzondere persoonsgegevens is daarom **niet van toepassing**.

Dit is in lijn met de EDPB-richtsnoeren voor videoapparatuur, die uitdrukkelijk stellen dat het incidenteel zichtbaar worden van bijzondere kenmerken op camerabeelden, zoals het dragen van een bril of het gebruik van een rolstoel, niet kwalificeert als gerichte verwerking van bijzondere persoonsgegevens.

14. Doelbinding

Doelbinding is het beginsel dat persoonsgegevens alleen mogen worden verwerkt voor het doel waarvoor ze oorspronkelijk zijn verzameld, of voor een doel dat daarmee verenigbaar is. Dit vloeit voort uit artikel 5, eerste lid, onderdeel b, van de AVG. Het betekent dat beeldmateriaal dat is vastgelegd voor cameratoezicht niet zomaar voor andere doeleinden mag worden gebruikt. Wanneer beeldmateriaal wordt gebruikt voor een ander doel dan waarvoor het is verzameld, dient te worden beoordeeld of dat nieuwe gebruik verenigbaar is met het oorspronkelijke doel.

Primair gebruik

De persoonsgegevens worden verwerkt voor de zeven verwerkingsdoeleinden zoals omschreven in onderdeel "4. Verwerkingsdoeleinden".

Verstreking aan derden

Verstreking van beeldmateriaal aan derden is een van de zeven verwerkingsdoeleinden (doeleinde 7) en is daarmee geen verdere verwerking voor een nieuw doel. De grondslag is bepaald in hoofdstuk 12: verstreking op een vordering van politie of justitie berust op een wettelijke verplichting, verstreking op eigen besluit van het schoolbestuur op de taak van algemeen belang.

Omdat beeldmateriaal met verstreking de eigen organisatie verlaat, gaat het schoolbestuur hier terughoudend mee om. Verstreking op eigen besluit vindt alleen plaats als dit in het concrete geval strikt noodzakelijk is in verband met een incident binnen de doeleinden 1 tot en met 4. De verstreking blijft beperkt tot het beeldmateriaal dat daarvoor nodig is en wordt vastgelegd in het logboek beeldgebruik.

Verstreking voor doelen die buiten de zeven verwerkingsdoeleinden vallen, zoals aan ouders, media of verzekeraars, is niet toegestaan (zie de uitgesloten doeleinden onder tabel 4.1). Bij een gerechtvaardigd inzageverzoek worden beelden alleen getoond en niet verstrekt (zie hoofdstuk 18).

15. Kinderrechten-afweging (Best Interests Assessment Children)

Artikel 3 van het Verdrag inzake de rechten van het kind schrijft voor dat bij alle maatregelen over kinderen de belangen van het kind de eerste overweging vormen. Deze afweging gaat verder dan een veilige gegevensverwerking en ziet ook op de bredere gevolgen van de verwerking voor het kind. SIVON geeft hieraan invulling door te beoordelen of cameratoezicht en de daarmee samenhangende gegevensverwerkingen in het belang zijn van leerlingen als betrokkenen. Daarbij wordt gebruik gemaakt van de systematiek van de Best Interests Assessment Children van de Britse ICO.

Cameratoezicht is geen systeem dat leerlingen zelf gebruiken, maar een systeem dat hen wel vastlegt. De betrokken leerlingen zijn veelal tussen de 4 en 18 jaar oud en zijn zich in wisselende mate bewust van het feit dat zij worden gefilmd en van hun rechten in dat verband. Er is geen KIA van een leverancier beschikbaar, deze afweging is daarom zelfstandig uitgevoerd.

1. Relevante rechten van kinderen

Recht op privacy (art. 16 IVRK). Cameratoezicht legt het gedrag van leerlingen vast op en rond de schoollocatie en raakt daarmee direct aan hun persoonlijke levenssfeer.

Recht op veiligheid en bescherming (art. 19 en 36 IVRK). Cameratoezicht kan bijdragen aan de fysieke veiligheid van leerlingen en aan het signaleren van gevaarlijke situaties.

Recht op vrijheid van meningsuiting en vergadering (art. 13 en 15 IVRK). Cameratoezicht kan een remmend effect (chilling effect) hebben op het gedrag van leerlingen, met name waar zij vrij met leeftijdsgenoten omgaan.

Recht op identiteitsontwikkeling en autonomie (art. 8 IVRK). De schoolomgeving speelt een centrale rol in de persoonlijke ontwikkeling van kinderen. Cameratoezicht kan de ervaring van autonomie beperken, met name voor oudere leerlingen.

Recht op participatie (art. 12 IVRK). Kinderen hebben het recht gehoord te worden in zaken die hen aangaan. Bij besluitvorming over cameratoezicht is het wenselijk dat leerlingen, via leerlingenraad of (G)MR, een stem hebben.

Vrijwaring van uitbuiting (art. 36 IVRK). Beeldmateriaal van minderjarigen mag niet worden gebruikt voor commerciële doeleinden of worden verstrekt aan partijen zonder directe betrokkenheid bij de schoolveiligheid.

Recht op toegang tot informatie (art. 17 IVRK). Leerlingen hebben recht op begrijpelijke, leeftijdsadequate informatie over het cameratoezicht op hun school.

2. Effect op deze rechten

Privacy. De inbreuk is structureel: leerlingen kunnen zich niet aan de vastlegging onttrekken omdat schoolbezoek verplicht is. De ernst hangt af van de plaatsing, buiten- en toegangsgebieden zijn minder ingrijpend dan gangen of andere binnenruimtes.

Veiligheid. Cameratoezicht heeft een potentieel positief effect op de veiligheid. Het kan bijdragen aan het voorkomen en oplossen van incidenten. Dit effect is afhankelijk van de concrete inrichting en het gebruik.

Vrijheid van meningsuiting en vergadering. Het bewustzijn van cameratoezicht kan een remmend effect hebben op het gedrag van leerlingen. Dit effect is moeilijk kwantificeerbaar maar dient meegewogen te worden, in het bijzonder in minder formele ruimtes.

Identiteitsontwikkeling en autonomie. Jongere kinderen zijn minder bewust van de camera's maar kwetsbaarder bij datalekken. Oudere leerlingen kunnen het toezicht als controlerend ervaren, wat de verhouding tussen school en leerling kan beïnvloeden.

Participatie. In de meeste gevallen worden leerlingen niet actief betrokken bij besluitvorming over cameratoezicht. Het participatierecht blijft in de praktijk vaak niet ingevuld.

Commerciële uitbuiting. Er zijn geen aanwijzingen voor commercieel gebruik. Het risico is beperkt mits toegang adequaat is beveiligd en verstrekking aan derden strikt is beperkt tot de gevallen die onder doeleinde 7 vallen.

Toegang tot informatie. Leerlingen worden doorgaans geïnformeerd via cameraborden en het privacybeleid. De vraag is of deze informatie voldoende begrijpelijk is voor jongere leerlingen.

3. Is dit effect wenselijk?

Het effect is tweeledig. Enerzijds draagt cameratoezicht bij aan de veiligheid van leerlingen. Anderzijds brengt het een structurele inbreuk op het privacyrecht met zich mee en heeft het potentiële effecten op de vrijheid van meningsuiting, autonomie en identiteitsontwikkeling.

De wenselijkheid hangt af van drie factoren: de plaatsing van de camera's, de inrichting van het systeem en de mate waarin leerlingen worden geïnformeerd en betrokken.

Cameratoezicht dat beperkt blijft tot buitenruimtes en toegangspunten, strikt doelgebonden wordt gebruikt en adequaat wordt gecommuniceerd, heeft een aanvaardbaar effect op de rechten van kinderen.

Cameratoezicht in leslokalen en gymzalen terwijl de ruimte in gebruik is, heeft geen aanvaardbaar effect op de rechten van kinderen: in leslokalen maakt het controle en beoordeling van leerlingen mogelijk en in gymzalen legt het leerlingen vast in sportkleding of, bij de jongsten, in hun ondergoed. Buiten de

Gebruikstijden vervallen deze bezwaren. Cameratoezicht in toiletten, kleedkamers of andere ruimtes met een fundamenteel privacykarakter is, ongeacht het doel, nooit aanvaardbaar.

4. Aanvullende maatregelen

Camera's worden uitsluitend geplaatst op buitenruimtes, toegangspunten en gemeenschappelijke ruimtes waar een concrete veiligheidsnoodzaak bestaat. In leslokalen en gymzalen wordt nooit gefilmd terwijl de ruimte in gebruik is door leerlingen, medewerkers of gebruikers van huurders. Buiten de Gebruikstijden is cameratoezicht in praktijklokalen met kostbare apparatuur en in gymzalen alleen toegestaan ter beveiliging van de ruimte en de daarin aanwezige eigendommen, en alleen als het camerasysteem per camera een tijdschema technisch afdwingt. Handmatig aan- en uitzetten is geen toegestaan alternatief. In toiletten, kleedkamers of andere ruimtes met een fundamenteel privacykarakter vindt nooit cameratoezicht plaats.

Leerlingen worden via de leerlingenraad of (G)MR betrokken bij besluitvorming over de inzet en plaatsing van cameratoezicht, voor zover dit redelijkerwijs mogelijk is.

Beeldmateriaal van minderjarigen wordt alleen verstrekt binnen doeleinde 7: op een vordering van politie of justitie, of op eigen besluit van het schoolbestuur wanneer dit strikt noodzakelijk is. Verstrekking aan ouders, media of verzekeraars is niet toegestaan. Bij een gerechtvaardigd inzageverzoek worden beelden alleen getoond.

De bewaartermijn wordt zo kort mogelijk gehouden, passend bij de doeleinden waarvoor de beelden zijn vastgelegd.

16. Noodzakelijkheid

De verwerking van persoonsgegevens in het kader van cameratoezicht is noodzakelijk voor de verwezenlijking van de zeven verwerkingsdoeleinden, onder de voorwaarde dat de camera's uitsluitend worden ingezet op locaties en voor situaties waarvoor een concrete noodzaak bestaat. Een verdergaande of bredere inzet dan strikt vereist voor de genoemde doeleinden is niet gerechtvaardigd en dient te worden voorkomen. De noodzaak van cameratoezicht wordt per camera jaarlijks herbeoordeeld door de proceseigenaar, de systeemeigenaar en de lokale kerngebruiker(s), op advies van de privacy officer, bij de actualisering van het cameraoverzicht, mede aan de hand van de geregistreerde incidenten. Voor iedere camera wordt de aanleiding vastgelegd in het cameraoverzicht. Voor camera's die ook tijdens de Gebruikstijden opnemen, gelden daarbij zwaardere eisen dan voor camera's die alleen buiten de Gebruikstijden opnemen.

17. Proportionaliteit en subsidiariteit

Proportionaliteit

Cameratoezicht op een schoollocatie vormt een structurele inbreuk op de persoonlijke levenssfeer van leerlingen, medewerkers en bezoekers. Anders dan bij incidentele verwerking worden persoonsgegevens doorlopend vastgelegd van personen die zich in een verplichte of institutionele omgeving bevinden en die zich aan de vastlegging niet kunnen onttrekken. Dit maakt de inbreuk ingrijpender dan bij verwerkingen waarbij betrokkenen een reële keuzevrijheid hebben.

De ernst van de inbreuk is echter sterk afhankelijk van de concrete inrichting van het cameratoezicht. De volgende factoren bepalen of de inbreuk proportioneel is:

Plaatsing van de camera's. Camera's op buitenruimtes en toegangspunten leveren een beperktere inbreuk op dan camera's in binnenruimtes. De inbreuk is proportioneel wanneer camera's worden geplaatst op locaties waar een concrete en aantoonbare veiligheidsnoodzaak bestaat. Cameratoezicht in leslokalen en gymzalen terwijl de ruimte in gebruik is, is disproportioneel: in leslokalen vanwege de mogelijkheid tot controle en beoordeling van leerlingen en medewerkers, in gymzalen omdat leerlingen zich daar in sportkleding of, bij de jongste leerlingen, in hun ondergoed bevinden. Buiten de Gebruikstijden, ook bij verhuur, is cameratoezicht in praktijklokalen met kostbare apparatuur en in gymzalen proportioneel, mits het uitsluitend dient ter beveiliging van de ruimte en de daarin aanwezige eigendommen en het camerasysteem het tijdschema technisch afdwingt. Plaatsing in ruimtes waar leerlingen zich in een besloten of kwetsbare context bevinden, zoals toiletten of kleedkamers, is disproportioneel en niet toegestaan.

Cameratoezicht tijdens de Gebruikstijden. In het besluit van de DSB Oostenrijk (zie hoofdstuk 12) speelde ook mee dat de Oostenrijkse wet het toezicht in pauzes uitdrukkelijk aan leraren opdraagt (§ 51 lid 3 SchUG) en dat de incidenten zich buiten schooltijd afspeelden. De Nederlandse zorgplicht voor de sociale, psychische en fysieke veiligheid op school is een open norm waarbij het bevoegd gezag zelf de middelen kiest.

De kern van de redenering rust echter op de AVG zelf en wordt in deze DPIA overgenomen: leerlingen zijn verplicht op school aanwezig en kunnen het cameratoezicht niet ontwijken, doorlopend minderjarigen filmen is niet vanzelf het minst ingrijpende middel en voor de bescherming van eigendommen volstaat doorgaans bewaking buiten de normale uren (EDPB 3/2019, par. 26). Camera's die uitsluitend zijn ingezet voor de doeleinden 3 en/of 4 nemen daarom alleen buiten de Gebruikstijden van de locatie op, dus niet tijdens Schooltijd en niet tijdens verhuur, zoals ook geldt voor praktijklokalen en gymzalen. Ook voor deze camera's is een aanleiding nodig: het probleem moet reëel zijn en niet speculatief. Omdat er buiten de Gebruikstijden op het eigen terrein geen personen aanwezig zijn die daar mogen zijn, volstaan incidenten op of rond de locatie, of een aantoonbaar dreigend gevaar, zoals de aanwezigheid van kostbare apparatuur (EDPB 3/2019, par. 19 t/m 22). Camera's die (mede) zijn ingezet voor doeleinde 1 en/of 2 mogen ook tijdens de Gebruikstijden opnemen, mits dat doeleinde per camera is onderbouwd met daadwerkelijke voorvallen of een aantoonbaar dreigend gevaar op die specifieke plek (EDPB 3/2019, par. 20 en 22). Een voorval op één plek rechtvaardigt alleen een camera op die plek, niet op andere plekken in het gebouw (par. 26 en 27). Bij de jaarlijkse evaluatie wordt per camera getoetst of de aanleiding nog actueel is.

Toegang tot beeldmateriaal. Een brede toegang tot het camerasysteem vergroot de inbreuk op de privacy van betrokkenen. Proportionaliteit vereist dat toegang strikt wordt beperkt tot medewerkers met een aantoonbare taak in het kader van het cameratoezicht, op basis van een vastgestelde autorisatiematrix.

Gebruik van de beelden. Beeldmateriaal dat uitsluitend wordt geraadpleegd naar aanleiding van een concreet incident levert een beperktere inbreuk op dan beeldmateriaal dat routinematig of preventief wordt bekeken. Actieve monitoring van leerlingen zonder concrete aanleiding is disproportioneel.

Leeftijd van de betrokkenen. Leerlingen in het funderend onderwijs zijn minderjarigen die op grond van de leerplicht verplicht aanwezig zijn. Dit verhoogt de kwetsbaarheid en de ernst van de inbreuk. De proportionaliteitsafweging dient hier extra gewicht aan toe te kennen, in het bijzonder voor jongere leerlingen in het primair onderwijs.

Wanneer het cameratoezicht wordt ingericht volgens de randvoorwaarden die in deze DPIA zijn vastgesteld, beperkte plaatsing, korte bewaartermijnen, strikte toegangscontrole en doelgebonden gebruik, staat de inbreuk op de persoonlijke levenssfeer in evenredige verhouding tot de verwerkingsdoeleinden. Bij afwijking van deze randvoorwaarden vervalt de proportionaliteit.

Subsidiariteit

De subsidiariteitstoets vereist dat wordt beoordeeld of de verwerkingsdoeleinden niet op een minder ingrijpende wijze kunnen worden verwezenlijkt. De EDPB-richtsnoeren benadrukken dat cameratoezicht geen standaardmaatregel mag zijn: wanneer minder ingrijpende middelen het doel kunnen bereiken, dient van cameragebruik te worden afgezien. Hieronder worden de relevante alternatieven beoordeeld.

Toezicht door personeel. Fysiek toezicht is minder ingrijpend maar niet toereikend buiten Schooltijd, op grotere terreinen of wanneer reconstructie van incidenten noodzakelijk is. Het kan cameratoezicht aanvullen maar niet volledig vervangen.

Fysieke toegangsbeveiliging. Hekken, slagbomen, intercomsystemen en toegangspassen dragen bij aan de beveiliging zonder beeldmateriaal vast te leggen, maar bieden geen mogelijkheid tot reconstructie van incidenten. Dit is een zinvolle aanvullende maatregel maar geen volledig substituuut.

Aanwezigheidsregistratie en alarmsystemen. Deze systemen leggen geen beeldmateriaal vast en zijn daarmee minder ingrijpend, maar bieden geen reconstructiemogelijkheid en zijn ontoereikend voor doeleinden die zien op de veiligheid van personen.

Geen cameratoezicht. Het volledig afzien van cameratoezicht is het minst ingrijpende alternatief. Bij een concrete aanleiding kan de wettelijke zorgplicht voor een veilige schoolomgeving echter niet afdoende worden ingevuld zonder enige vorm van technische bewaking, met name buiten Schooltijd en op grotere terreinen.

De overwogen alternatieven zijn elk afzonderlijk dan wel gecombineerd ontoereikend om alle verwerkingsdoeleinden te verwezenlijken. Cameratoezicht is het enige middel dat zowel preventief werkt, toegangscontrole ondersteunt als reconstructie van incidenten mogelijk maakt. De verwerkingsdoeleinden kunnen in redelijkheid niet volledig op een minder ingrijpende wijze worden verwezenlijkt. Dit laat onverlet dat cameratoezicht moet worden beperkt tot wat strikt noodzakelijk is én altijd wordt gecombineerd met aanvullende maatregelen. Per camera wordt daarom, mede op basis van het effect van de getroffen maatregelen, beoordeeld of het doel zonder cameratoezicht kan worden bereikt. De uitkomst wordt vastgelegd in het cameraoverzicht en jaarlijks opnieuw beoordeeld.

De volgende aanvullende maatregelen zijn voorbeelden die in combinatie met cameratoezicht worden gehanteerd en dienen door het schoolbestuur te worden vastgelegd in het cameraoverzicht en het reglement cameratoezicht:

- Surveillance door personeel of beveiligingspersoneel op het schoolterrein.
- Een operationeel alarmsysteem voor inbraak- en branddetectie.
- Het afsluiten van gebieden of terreinen buiten Schooltijd.
- Bebording en posters als preventieve communicatie richting bezoekers en leerlingen.
- Bewustwordingsacties en gesprekken met leerlingen over veiligheid en gedrag.
- Aansluiting bij een wijkapp ter ondersteuning van buurttoezicht. *Let op: de privacyaspecten van de gebruikte wijkapp zijn niet in deze DPIA getoetst, het schoolbestuur dient hiervoor een separate beoordeling uit te voeren.*

- Buurtpreventie in samenwerking met omwonenden.
- Overleg met gemeente, politie en/of wijkagent over veiligheid en toezicht rondom de schoollocatie.
- Bij nieuwbouw: aandacht voor het ontwerp zodat onoverzichtelijke hoeken worden vermeden.

18. Rechten van de betrokkenen

Art. 15, lid 1, van de AVG beschrijft dat iedere betrokkene het recht heeft om van de verwerkingsverantwoordelijke uitsluitend te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen in die persoonsgegevens¹⁷.

Het schoolbestuur is verwerkingsverantwoordelijke en dient daarom op de school- en/of bestuurswebsite een duidelijke privacyverklaring op te nemen. Hierin staat beschreven welke rechten betrokkenen hebben over de verwerking van hun persoonsgegevens en hoe men die rechten kan uitoefenen.

SIVON heeft onderzocht en vastgesteld dat, met betrekking tot de uitoefening van rechten van betrokkenen, schoolbesturen die cameratoezicht gebruiken, in de regel zelfstandig kunnen voorzien in de afhandeling van verzoeken van betrokkenen.

In de onderstaande tabel wordt aangegeven welke rechten het betreft en of er van enige beperking sprake is.

Tabel 18.1 Rechten van betrokkenen

Recht van betrokkene	Toelichting procedure	Evt. beperking verwerking*
Het recht op informatie	Betrokkenen worden volgens de richtlijnen van de EDPB tweelaags geïnformeerd: • 1^e laag: Cameraborden met cameralogo, de tekst cameratoezicht, de periode waarin wordt opgenomen, identiteit verwerkingsverantwoordelijke, doel, bewaartermijn, informatie die betrokkenen zouden kunnen verrassen (bijvoorbeeld: live monitoring, verstrekking aan derden) en verwijzing naar tweede laag. • 2^e laag: via de openbaar gepubliceerde privacyverklaring op de school- en/of bestuurswebsite en via een leeftijdsadequate toelichting aan leerlingen bij aanvang van het schooljaar.	n.v.t.
Het recht van inzage	Betrokkenen kunnen inzage verzoeken in beeldmateriaal waarop zij zelf zichtbaar zijn. Bij een inzageverzoek geeft de betrokkene datum, een zo nauwkeurig mogelijk tijdspad en de betreffende locatie op. Inzage mag niet leiden tot schending van rechten van andere betrokkenen door bijvoorbeeld	Beperking mogelijk op grond van art. 15 lid 4 AVG: inzage mag geen afbreuk doen aan de rechten en vrijheden van anderen. Beelden worden zo nodig afgeschermd of in

¹⁷ Zie Hoofdstuk III van de AVG 'Rechten van de betrokkene', artikel 12 – 23 AVG.

	het doorzoeken van een lange tijdslijn. Inzage wordt verleend voor zover dit technisch mogelijk is en voor zover de privacy van andere betrokkenen die op hetzelfde beeldmateriaal zichtbaar zijn niet wordt geschonden. Beelden worden alleen getoond en niet verstrekt.	beperkte vorm getoond. Het inzagerecht stelt de betrokkene in staat zich van de verwerking van zijn persoonsgegevens op de hoogte te stellen en de rechtmatigheid daarvan te controleren (overweging 63 AVG). Het is niet bedoeld om beeldmateriaal te verkrijgen voor andere doeleinden, zoals het aanwijzen van een andere partij of het onderbouwen van een civiele vordering. Een verzoek kan daarnaast worden afgewezen als de identiteit van de betrokkene, ook na een verzoek om aanvullende informatie, niet kan worden vastgesteld (art. 12 lid 6 AVG), het verzoek onvoldoende is gespecificeerd om de betrokkene in het beeldmateriaal te identificeren (art. 11 lid 2 AVG; EDPB 3/2019, par. 95 en 96), het verzoek kennelijk ongegrond of buitensporig is (art. 12 lid 5 AVG), of in het belang van de opsporing van strafbare feiten (art. 41 lid 1 sub d UAVG). Bij een afwijzing deelt het schoolbestuur de betrokkene de redenen mee en wijst het op de mogelijkheid een klacht in te dienen bij de AP en beroep in te stellen bij de rechter (art. 12 lid 4 AVG).
Het recht op rectificatie	Niet van toepassing. Camerabeelden betreffen een automatische en feitelijke registratie van beelden. Rectificatie van beeldmateriaal is technisch niet mogelijk en inhoudelijk niet aan de orde.	n.v.t.
Het recht op gegevensverwijdering	Beeldmateriaal wordt bij het verstrijken van de bewaartermijn automatisch overschreven of verwijderd. Betrokkenen kunnen een verzoek tot vroegtijdige verwijdering indienen bij het schoolbestuur via het daarvoor aangewezen contactpunt. Veiliggestelde beelden in het kader van een incident worden niet gewist zolang het incident nog in behandeling is.	Beperking mogelijk indien beelden zijn veiliggesteld voor gebruik in het kader van een incident of overdracht aan politie of justitie. Verwijdering is in dat geval opgeschort totdat het incident is afgehandeld.

Het recht op beperking van de verwerking	Beperking van de verwerking is uitsluitend mogelijk voor beelden die zijn veiliggesteld en waarvan bekend is dat een bepaalde betrokkene in beeld is. Voor regulier beeldmateriaal dat nog niet is geraadpleegd is beperking technisch niet uitvoerbaar. Betrokkenen kunnen een verzoek indienen via het daarvoor aangewezen contactpunt.	Beperking is technisch alleen uitvoerbaar voor veiliggesteld beeldmateriaal. Voor overige beelden vervalt de grond voor beperking door de korte bewaartermijn en automatische verwijdering.
Een kennisgevingsplicht over rectificatie of verwijdering van persoonsgegevens	Het schoolbestuur informeert betrokkenen over de opvolging van ingediende verzoeken tot verwijdering of beperking van de verwerking, voor zover dit in de gegeven omstandigheden mogelijk is.	n.v.t.
Het recht op overdraagbaarheid van gegevens	Niet van toepassing. Het recht op dataportabiliteit geldt uitsluitend voor verwerkingen op basis van toestemming of uitvoering van een overeenkomst. De grondslag voor cameratoezicht is de taak van algemeen belang (art. 6 lid 1 sub e AVG). Bovendien zijn camerabeelden niet overdraagbaar in een machineleesbaar gestandaardiseerd bestandsformaat.	n.v.t. op grond van art. 20 lid 3 AVG.
Het recht van bezwaar	Betrokkenen kunnen via het daarvoor aangewezen contactpunt bezwaar maken tegen de verwerking van hun persoonsgegevens om redenen die verband houden met hun specifieke situatie (art. 21 lid 1 AVG). Dit recht geldt omdat het cameratoezicht is gebaseerd op de taak van algemeen belang (art. 6 lid 1 sub e AVG). Bezwaar kan worden gemaakt bij het betreden, tijdens de aanwezigheid in of na het verlaten van het bewaakte gebied (EDPB-richtsnoeren 3/2019, par. 106). Het schoolbestuur beoordeelt elk bezwaar individueel en reageert onverwijld, uiterlijk binnen een maand (par. 105). Is het bezwaar gegrond, dan wordt de verwerking van de gegevens van de betrokkene gestaakt. Het recht van bezwaar geldt niet voor verwerkingen op grond van een wettelijke verplichting (art. 6 lid 1 sub c AVG), zoals logging en verstrekking op een vordering van politie of justitie.	Beperking mogelijk op grond van art. 21 lid 1 AVG: het schoolbestuur kan de verwerking voortzetten als het dwingende gerechtvaardigde gronden aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene. De afweging van noodzaak, proportionaliteit en subsidiariteit per camera in het cameraoverzicht vormt de basis voor die onderbouwing. Het schoolbestuur legt de afweging per bezwaar gemotiveerd vast en deelt de uitkomst aan de betrokkene mee.
Het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit	Niet van toepassing. Het camerasysteem bevat geen functionaliteit voor geautomatiseerde besluitvorming of profilering op basis van beeldmateriaal. AI-functionaliteit zoals gezichtsherkenning of gedragsdetectie valt expliciet buiten de scope van deze DPIA.	n.v.t.

** Er zijn uitzonderingen mogelijk op de uitoefening van deze rechten, op voorwaarde dat de wezenlijke inhoud van de grondrechten en fundamentele vrijheden niet wordt aangetast en dat het gaat om noodzakelijke en evenredige maatregelen ter waarborging van enkele expliciet opgesomde belangrijke doelstellingen van algemeen belang. Uitzonderingen moeten altijd op een nationale wet berusten, of in de AVG direct zijn toegestaan op grond van de bepalingen in de Europese privacyreggeving. Uitzonderingen op de rechten van betrokkenen zijn, onder meer, geregeld in artikel 23 AVG en artikel 41 UAVG.*

19. Beoordeling verwerkersovereenkomst

Deze DPIA is een sectorale model-DPIA voor cameratoezicht in het funderend onderwijs en is niet gericht op een specifieke leverancier of een specifiek camerasysteem. Er is in het kader van deze DPIA dan ook geen verwerkersovereenkomst beoordeeld. Een leveranciersspecifieke toetsing van de verwerkersovereenkomst maakt onderdeel uit van de lokale DPIA die het schoolbestuur op basis van deze model-DPIA uitvoert.

Of een verwerkersovereenkomst noodzakelijk is, hangt af van de inrichting van het camerasysteem. Bepalend is of er sprake is van cloudopslag of online beheer- of viewsoftware (niet lokaal geïnstalleerd) en of een externe partij Structurele toegang heeft tot het camerasysteem.

Geen verwerkersovereenkomst vereist wanneer:

- De opslag volledig lokaal plaatsvindt op een recorder die zich op de schoollocatie bevindt
- De leverancier of onderhoudspartij geen Structurele toegang heeft tot het camerasysteem

In dit scenario verwerkt het schoolbestuur de persoonsgegevens volledig binnen de eigen organisatie en treedt geen externe partij op als verwerker in de zin van de AVG.

Een verwerkersovereenkomst is wel vereist wanneer:

- De beheer- of viewsoftware online is (niet lokaal geïnstalleerd)
- De camerabeelden in de cloud worden opgeslagen
- De externe onderhoudspartij Structurele toegang heeft tot het camerasysteem

In dit scenario treedt de derde partij op als verwerker in de zin van artikel 28 AVG en is het schoolbestuur verplicht een verwerkersovereenkomst te sluiten voordat de verwerking aanvangt.

Wanneer een verwerkersovereenkomst vereist is, dient het schoolbestuur te beoordelen of de overeenkomst voldoet aan de eisen van de AVG.

7. Deel C: Beschrijving en beoordeling risico's voor de betrokkenen

Dit hoofdstuk beschrijft en beoordeelt de risico's van het cameratoezicht voor de rechten en vrijheden van de betrokkenen. Het legt eerst het beoordelingskader vast, waarin de kans en de impact van een risico worden gescoord. Daarna volgt de risicotabel met de risico's die voor cameratoezicht gelden.

Beoordelingskader risico's

Alle mogelijke risico's van de gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen worden hieronder beschreven en afgewogen. Het gaat hierbij om de negatieve gevolgen die de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen, de oorsprong van deze gevolgen, de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden en de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden: kans (waarschijnlijkheid) X impact (ernst) = risico.

De methodiek die wordt gevolgd, is beschreven door de Britse toezichthouder¹⁸ om risico's te classificeren. Hierbij wordt een objectieve inschatting gemaakt van de kans en impact van negatieve gevolgen (eventuele fysieke, emotionele of materiële schade).

Onderstaande matrix toont op een gestructureerde manier de classificatie van risico's:

RISICO	Kans Laag (1)	Kans Midden (2)	Kans Hoog (3)
Impact Hoog (3)	Risico Midden (Score: 3)	Risico Hoog (Score: 6)	Risico zeer hoog (Score: 9)
Impact Midden (2)	Risico Laag (Score: 2)	Risico Midden (Score: 4)	Risico Hoog (Score: 6)
Impact Laag (1)	Risico Zeer laag (Score: 1)	Risico Laag (Score: 2)	Risico Midden (Score: 3)

Hulpmiddel beoordelen score laag, midden en hoog:

Laag	Midden	Hoog
Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende meerdere dagen brengt geen merkbare (meetbare) schade toe. Blijvende juistheid van informatie (vanaf de bron tot het laatste gebruik) is gewenst, maar hoeft niet gegarandeerd te zijn.	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een of meerdere dagen brengt merkbare schade toe. Sommige afwijkingen in data zijn toelaatbaar, juistheid data is belangrijk maar niet kritisch.	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een werkdag brengt merkbare schade toe. Juistheid informatie moet gegarandeerd zijn, noodzakelijk dat data correct is.
Weinig tot geen schade	Enige schade of gevolgen	Grote - onvermijdelijke - ernstige schade en gevolgen; imago.

¹⁸ Zie voor de meest recente matrix van de ICO: 'How do we identify and assess risk'. De matrix zoals opgenomen in dit DPIA model is een eerder, nog steeds gevalideerd model om risico's te classificeren en wordt nog gebruikt ten behoeve van consistentie met eerdere DPIA's uitgevoerd door SIVON.

Kans = gebeurt bijna nooit; 1 maal per (school)jaar of minder	Kans = gebeurtenis kan zich voordoen; meerdere malen per (school)jaar	Kans = deze gebeurtenis zal zich bijna zeker voordoen; per maand, week of zelfs dag
---	---	---

Het gaat hier om een risicogerichte benadering en beoordelingsproces dat bestaat uit de volgende drie stappen:

1. Risico's identificeren.
2. Risico's inschatten/analyseren.
3. Risico's beoordelen/evalueren.

In het volgende hoofdstuk (Deel D: maatregelen) worden de geconstateerde risico's aangevuld met 2 vervolgstappen:

4. Mitigeren risico's: maatregelen die de aangetroffen risico's voorkomen of verminderen (mitigeren).
5. Herbeoordeling risico's: restrisico.

20. Risico's

In onderstaande risicotabel worden de risico's beschreven. Per risico worden de gevolgen aangegeven met daarbij de kans dat het zich voordoet en de impact, die samen leiden tot het risico. De volgorde waarin de risico's worden gepresenteerd, is afgestemd op de volgorde van de onderzochte aspecten en impliceert geen prioritering naar belangrijkheid.

Deze risicoanalyse is voor een belangrijk deel gebaseerd op de "Guidelines 3/2019 on processing of personal data through video devices Version 2.0 - Adopted on 29 January 2020" van de European Data protection Board (EDPB).



= Kans



= Impact



= Risico

20.1 Risicotabel

#	Risico	Gevolgen voor betrokkenen			
Technisch					
<i>Opname</i>					
T-1	Openbare ruimte Camera's zijn (al dan niet beweegbaar) gericht op de openbare ruimte buiten de eigendomsgrenzen van de school	Personen buiten de eigendomsgrenzen worden zonder hun medeweten gefilmd. Zij kunnen hun rechten (zoals bezwaar of informatie) niet uitoefenen, omdat zij niet weten dat zij worden gefilmd. Dit gebrek aan transparantie maakt het toezicht feitelijk heimelijk.	3	3	9
T-2	Geluid Camera's nemen (ook) geluid op	Geluidsopnames leggen gespreksinhoud vast, wat verder gaat dan het doel van cameratoezicht. Betrokkenen verliezen zo controle over gebruik van hun gegevens	2	3	6
T-3	Opnametechnieken Er worden andere opnametechnieken ingezet dan standaard	Opnametechnieken die verder gaan dan strikt noodzakelijk voor de vastgestelde doelbinding (standaard	2	3	6

#	Risico	Gevolgen voor betrokkenen			
	bewegingsdetectie, zoals AI-gestuurde gezichtsherkenning of gedragsanalyse	bewegingsdetectie) halen andere of meer informatie uit de beelden dan het gecommuniceerde doel omvat of betrokkenen redelijkerwijs konden verwachten. Betrokkenen verliezen daarmee controle over welke informatie over hen wordt verwerkt.			
T-4	Niet-noodzakelijke functies Bij aanschaf, installatie of configuratie zijn meer functies ingeschakeld dan strikt noodzakelijk zijn voor de vastgestelde verwerkingsdoeleinden per camera, zoals PTZ-beweging, optische zoom, analytische functies of draadloze verzending, zonder dat daarvoor een doelbinding bestaat	Actief blijvende, niet-noodzakelijke functies kunnen (on)bedoeld worden gebruikt voor iets buiten de vastgestelde doelbinding. Er zijn functies die het technisch aanvalsoppervlak kunnen vergroten, wat de kans op onbevoegde toegang door derden verhoogt. Betrokkenen hebben een grotere kans, of verliezen daarmee de controle over welke informatie over hen wordt verwerkt.	2	3	6
<i>Opslag & beveiliging</i>					
T-5	Opslag beelden Beelden worden in de cloud opgeslagen of via online beheer- of viewsoftware verwerkt, zonder verwerkersovereenkomst met de leverancier. Beelden worden opgeslagen buiten de EER zonder passende waarborgen	Zonder verwerkersovereenkomst heeft de verwerkingsverantwoordelijke geen afdwingbare afspraken met en dus geen controle over, de leverancier. Bij opslag buiten de EER zonder adequaatheidsbesluit, zonder passende waarborg (zoals SCC of BCR), of zonder DTIA ontbreekt een rechtmatige grondslag voor de doorgifte zelf. Betrokkenen verliezen daarmee de controle over hun gegevens, ongeacht of de feitelijke beveiliging bij de leverancier toereikend is.	2	3	6
T-6	Technische beveiliging Onvoldoende technische beveiligingsmaatregelen zijn genomen om het camerasysteem en het beeldmateriaal te beschermen, zoals toegang zonder MFA of met zwakke of standaardwachtwoorden, onversleutelde opslag of onversleuteld transport van beelden, of het uitblijven van securityupdates. Dit kan zich voordoen bij lokale opslag, bij cloudopslag, bij systemen die via een VLAN zijn aangesloten op de bredere IT-infrastructuur, of bij systemen die online bereikbaar zijn zonder adequate perimeterbescherming of netwerkmonitoring	Onvoldoende beveiliging vergroot de kans op een beveiligingsincident of datalek, waarmee betrokkenen de controle verliezen over wie hun beelden inziet. Voor minderjarige betrokkenen kan dit mogelijk leiden tot (o.a.) slachtofferschap van (groeps-)pesten, intimidatie of afpersing, of tot risico's voor hun fysieke veiligheid en vrijheid	2	3	6
Organisatorisch					

#	Risico	Gevolgen voor betrokkenen			
Beleid & rechten					
O-1	Doelbinding De organisatie hanteert geen eenduidige, toelaatbare of volledige doelbinding voor het gebruik van cameratoezicht. Voor een camera is geen aanleiding vastgesteld, of de aanleiding voldoet niet aan het vereiste niveau: voor camera's die alleen buiten de Gebruikstijden opnemen blijkt niet van incidenten op of rond de locatie of van een aantoonbaar dreigend gevaar, en voor camera's die ook tijdens de Gebruikstijden opnemen blijkt niet van daadwerkelijke voorvallen of een aantoonbaar dreigend gevaar op die plek. Ook wordt één voorval gebruikt om camera's op meerdere plekken te rechtvaardigen	Zonder vastgesteld en jaarlijks geëvalueerd toegestaan doel weten betrokkenen niet waarvoor hun beeltenis wordt gebruikt en verliezen zij controle over hun gegevens. Gebruik voor een ander doel, zoals bijvoorbeeld functioneringsbeoordeling, kan bovendien nadeel opleveren voor de beroeps-/arbeidspositie van de betrokkene	2	3	6
O-2	Bewaartermijnen Beelden worden te lang bewaard en/of er is geen of een te lange bewaartermijn ingesteld in het systeem	In strijd met het proportionaliteitsbeginsel en opslagbeperkingsbeginsel, vergroten beelden die langer worden bewaard dan nodig het tijdsvenster waarin ze kunnen uitlekken of misbruikt worden. Betrokkenen kunnen er daardoor niet op vertrouwen wanneer hun beeltenis daadwerkelijk wordt verwijderd, wat de controle over hun gegevens ondermijnt	3	3	9
O-3	Proportionaliteit en subsidiariteit Cameratoezicht vindt plaats in lokalen of andere privacygevoelige ruimten of wordt ingezet om leerlingen en/of medewerkers te beoordelen. Camera's filmen tijdens de Gebruikstijden terwijl dat niet is toegestaan, zoals camera's die uitsluitend voor de doeleinden 3 en/of 4 zijn ingezet en camera's in praktijklokalen of gymzalen, doordat het tijdschema niet technisch is afgedwongen maar afhankelijk is van handmatig aan- en uitzetten, of niet is afgestemd op de tijden van verhuur. Cameratoezicht in gemeenschappelijke ruimtes heeft een chilling effect op leerlingen: de aanwezigheid van camera's remt hun gedrag, vrije meningsuiting en identiteitsontwikkeling, ook wanneer	Cameratoezicht is het zwaarst mogelijke middel en mag nooit op zichzelf staan. Cameratoezicht in lokalen, beoordeling van leerlingen/medewerkers en preventieve maatregelen die niet zijn geëvalueerd of niet langer van toepassing zijn, zijn daarom disproportioneel. Voor leerlingen remt cameratoezicht in gemeenschappelijke ruimtes hun gedrag en vrije ontwikkeling (chilling effect). Zonder beoordeling bij de plaatsing van een camera en raadpleging van leerlingen hierover, blijft zo'n effect mogelijk onopgemerkt	2	3	6

#	Risico	Gevolgen voor betrokkenen			
	de plaatsing technisch binnen de kaders valt. Cameratoezicht is een op zichzelf staande oplossing zonder dat andere preventieve maatregelen vooraf zijn ingezet en geëvalueerd, of andere maatregelen zijn na installatie (grotendeels) gestopt. Leerlingen worden niet geconsulteerd bij de besluitvorming over cameraplaatsing of -beleid, waardoor de proportionaliteitsafweging niet mede vanuit hun perspectief is gemaakt				
O-4	Verplaatsbare camera's Camera's, in het bijzonder losse, vrij verplaatsbare (IP-) camera's waarvan de beelden op tablets of andere mobiele devices te bekijken zijn, kunnen door één persoon en zonder het reguliere wijzigingsproces (gezamenlijk besluit, herbeoordeling van doelbinding, aanpassing van het cameraoverzicht en de bebording) worden verplaatst naar een andere locatie of gericht worden op een ander object of een specifieke persoon	Doordat camera's fysiek verplaatst of anders ingesteld kunnen worden, is niet geborgd dat elke nieuwe positie opnieuw aan doelbinding en proportionaliteit wordt getoetst. Betrokkenen verliezen daarmee de controle over hun gegevens. Dat maakt misbruik lastiger te voorkomen en te controleren, tot en met, in het uiterste geval, gerichte surveillance van een individu dat zijn rechten daarover niet kan uitoefenen	2	3	6
O-5	Transparantie Betrokkenen worden niet of onvoldoende geïnformeerd over het cameratoezicht. Informatieverstrekking is niet afgestemd op het begrips- en leeftijdsniveau van leerlingen. Met name jongere leerlingen kunnen de privacyverklaring en bebording niet begrijpen	Zonder toereikende informatie kunnen betrokkenen hun rechten (b.v. bezwaar, inzage) niet uitoefenen, omdat zij niet weten dat, waarom of hoe zij worden gefilmd. Bij volledige afwezigheid is sprake van heimelijk toezicht. Voor leerlingen is dat onvermogen groter naarmate de informatie minder is afgestemd op hun leeftijdsfase, van eenvoudige/visuele uitleg in het PO tot volledige uitleg van hun rechten in het VO	2	3	6
O-6	Privacyrechten betrokkenen Er is geen procedure voor het afhandelen van privacyrechtverzoeken (inzage, verwijdering, beperking en bezwaar) van betrokkenen in relatie tot camerabeelden	Zonder procedure, proceseigenaar en vindbare informatie over hoe een rechtenverzoek in te dienen, kunnen betrokkenen hun rechten (inzage, correctie, verwijdering, bezwaar) niet daadwerkelijk uitoefenen, ook al hebben zij die rechten wel. Zonder zorgvuldige afweging bij verzoeken die de privacy van andere, op dezelfde beelden zichtbare betrokkenen raken, kan bovendien hún beeltenis worden prijsgegeven zonder hun medeweten	2	2	4

#	Risico	Gevolgen voor betrokkenen			
O-7	Datalekrespons en incidentafhandeling camerasysteem Het camerasysteem is niet expliciet opgenomen in het bestaande datalekresponsbeleid van het schoolbestuur, of er ontbreekt een beknopte aanvulling die beschrijft hoe bij een incident met het camerasysteem wordt omgegaan met het veiligstellen van beeldmateriaal	In strijd met de AVG-regels rond datalekrespons kunnen betrokkenen, zonder verankering in het datalekresponsbeleid, niet rekenen op tijdige melding of mededeling bij een incident. Hun recht daarop wordt zo niet erkend. Automatische overschrijving kan het bewijs bovendien onherstelbaar laten verdwijnen vóórdat de omvang van het datalek en daarmee welke betrokkenen zijn getroffen, kan worden vastgesteld	2	2	4
<i>Toegang & gebruik</i>					
O-8	Autorisatie Er is geen autorisatiematrix vastgesteld die regelt wie beelden mag bekijken, of er wordt gewerkt met gedeelde accounts	Zonder autorisatiematrix is niet vastgelegd wie welke acties binnen het camerasysteem mag uitvoeren, waardoor onrechtmatige inzage van betrokkenen niet wordt voorkomen. Bij gedeelde accounts is bovendien niet te achterhalen wíe specifiek heeft gekeken, waardoor controle op het gebruik onmogelijk is en misstanden niet goed te detecteren zijn. In beide gevallen verliezen betrokkenen de controle over wie hun gegevens bekijkt, zonder mogelijkheid dit op te sporen of terug te draaien	2	3	6
O-9	Hoe/wanneer beelden terugkijken Er zijn geen richtlijnen voor het terugkijken van beelden: wie mag dit doen, met welk account, onder het vier-ogenprincipe en met registratie. Er zijn geen vastgestelde uitzonderingen op het vier-ogenprincipe (bijv. bij calamiteiten)	Zonder vier-ogenprincipe, verplicht opnieuw inloggen, logboekregistratie en een kader voor uitzonderingen (bijv. calamiteiten buiten Schooltijd) ontstaat een willekeurige werkwijze waarbij beelden zonder aantoonbare noodzaak en zonder controle kunnen worden ingezien. Betrokkenen verliezen daarmee de controle over hun gegevens	2	3	6
O-10	Welke beelden terugkijken Er zijn geen richtlijnen in welke situaties beelden teruggekeken mogen worden	Zonder kaders voor wanneer beelden mogen worden teruggekeken, kunnen ze worden gebruikt voor iets anders dan het doel waarvoor betrokkenen ze verwachtten. Zij verliezen daarmee de controle over hun gegevens	2	2	4
O-11	Ongeautoriseerde eigen opnames van beelden Er is geen expliciete verbodsbepaling en geen bewustwordingsafpraak rondom het buiten het systeem vastleggen van camerabeelden door medewerkers (bijv. via mobiel het	Beelden die buiten het systeem worden vastgelegd (bijvoorbeeld door het scherm te filmen) zijn niet meer te herleiden naar wie dit deed. Betrokkenen verliezen daarmee de controle over hun gegevens. Voor leerlingen en medewerkers kan dit mogelijk leiden tot (o.a.)	2	3	6

#	Risico	Gevolgen voor betrokkenen			
	scherm filmen of exporteren naar een privéapparaat)	slachtofferschap van pesten, intimidatie of afpersing, zonder dit te kunnen terugdraaien of de verantwoordelijke aan te spreken			
O-12	Live beelden bekijken Er zijn geen richtlijnen voor het live bekijken van beelden, de richtlijnen worden niet nageleefd, of live beelden zijn voor omstanders zichtbaar	Zonder richtlijnen voor live kijken en beperking tot bevoegde medewerkers, kunnen live beelden onbedoeld zichtbaar zijn voor onbevoegden of omstanders. De in beeld gebrachte betrokkenen verliezen daarmee de controle over hun gegevens, op het moment dat dat gebeurt	2	3	6
O-13	Beelden online terugkijken Beelden zijn ook via laptop, app of tablet te bekijken (buiten de lokale recorder). Er is niet vastgesteld wie dit mag doen, wanneer, op welk apparaat en in welke situatie	Zonder vastgestelde richtlijnen voor wie, wanneer en op welk apparaat online mag worden ingelogd, vergroot online toegang het technisch aanvalsoppervlak en daarmee de kans op ongeautoriseerde inzage. Toegang via niet-beheerde privéapparaten maakt dit risico extra concreet (bijvoorbeeld een gehackt privéapparaat). Betrokkenen verliezen daarmee de controle over hun gegevens	3	3	9
O-14	Bewaren van beelden Er is geen richtlijn in welke gevallen beelden langer bewaard mogen worden, geen registratie van bewaarde of verwijderde beelden, en geen afspraken over bewaarplek, -termijn en feitelijke verwijdering	Zonder richtlijnen voor wanneer beelden langer bewaard mogen worden, registratie van bewaar-/verwijderbeslissingen, een vastgestelde bewaarplek en bewaartermijn, kan de school niet aantonen en kunnen betrokkenen niet vertrouwen, dat beelden daadwerkelijk binnen de toegestane termijn worden verwijderd. Dit vergroot het tijdsvenster waarin beelden kunnen uitlekken of oneigenlijk worden gebruikt, betrokkenen verliezen daarmee de controle over hun gegevens	2	2	4
O-15	Inzage beelden door derden Er is geen richtlijn voor wanneer inzage aan derden mag worden verleend en er is geen registratie van verleende inzage	Zonder richtlijnen voor wanneer inzage aan derden is toegestaan en zonder registratie van verleende inzage, kunnen derden onrechtmatig toegang krijgen tot beelden zonder dat dit ooit wordt opgemerkt. Betrokkenen verliezen daarmee de controle over hun gegevens, zonder hiervan op de hoogte te zijn	2	3	6
O-16	Delen beelden met derden Er is geen richtlijn voor wanneer en op welke wijze beelden gedeeld mogen worden met derden, geen registratie	Zonder richtlijnen voor het delen van beelden (wanneer, op welke manier en met wie) kunnen deze via onveilige kanalen bij onbevoegde derden terechtkomen, zelfs zonder registratie	2	3	6

#	Risico	Gevolgen voor betrokkenen			
	hiervan en geen identificatievereisten voor ontvangers	van de ontvanger. Betrokkenen verliezen daarmee onherleidbaar de controle over hun gegevens			
<i>Beheer</i>					
O-17	Technisch onderhoud Het onderhoud van het camerasysteem is niet geborgd: er zijn geen duidelijke afspraken met de onderhoudspartij, of bij uitval is geen herstelprocedure beschikbaar en zijn geen compenserende maatregelen voorzien. Bij onderhoud, op afstand of op locatie, kan de onderhoudspartij beelden zien zonder dat er afspraken over geheimhouding zijn gemaakt	Een onbeheerd systeem verhoogt het risico op een beveiligingsincident of datalek, waarmee betrokkenen de controle over hun gegevens kunnen verliezen, en het risico op uitval van de beveiligingsfunctie zelf, zonder compenserende maatregelen om die uitval op te vangen. Zonder geheimhoudingsafspraken kunnen medewerkers van de onderhoudspartij beelden bekijken, opslaan of verspreiden zonder dat het schoolbestuur hen daarop kan aanspreken	2	3	6
O-18	Externe onderhoudspartij Het camerasysteem is voor een externe onderhoudspartij toegankelijk via Structurele toegang, zonder dat hiervoor een verwerkersovereenkomst is afgesloten	Zonder verwerkersovereenkomst heeft de verwerkingsverantwoordelijke geen afdwingbare afspraken met, en dus geen controle over, de externe onderhoudspartij die Structurele toegang heeft. Zonder verificatie of deze partij voldoende technische en organisatorische maatregelen treft, is bovendien niet vastgesteld of die toegang wel voldoende beveiligd is. Betrokkenen verliezen daarmee de controle over hun gegevens, ongeacht of de feitelijke beveiliging bij de onderhoudspartij toereikend is	3	2	6
O-19	Fysieke beveiliging De ruimte met technische componenten (recorder, switches) is niet of onvoldoende beveiligd. De ruimte voor live- of terugkijken van beelden is vrij toegankelijk	Zonder afgesloten technische ruimte en zonder slot- of sleutelregistratie kunnen onbevoegden fysiek toegang krijgen tot het camerasysteem of tot ruimtes waar beelden worden bekeken. Betrokkenen verliezen daarmee de controle over hun gegevens, zonder dit te kunnen weten of beïnvloeden	2	3	6
Governance					
<i>Inrichting & beheer</i>					
G-1	Eigenaarschap Er is geen bestuursbrede proceseigenaar en/of systeemeigenaar voor cameratoezicht aangewezen	Zonder duidelijk eigenaarschap is niet geborgd dat beschermende maatregelen daadwerkelijk worden uitgevoerd en gecontroleerd en is niet belegd wie nieuwe camera's beoordeelt en goedkeurt vóór aanschaf. Dit vergroot structureel het risico dat andere risico's	3	3	9

#	Risico	Gevolgen voor betrokkenen			
		uit deze tabel zich voordoen en onopgemerkt blijven, waarmee betrokkenen de controle over hun gegevens kunnen verliezen			
G-2	Inkoopproces Er is geen centraal inkoopproces voor camerasystemen, verschillende locaties kunnen mogelijk zelfstandig aanschaffen buiten een vastgesteld proces om.	Versnipperde aanschaf zonder centraal proces bemoeilijkt uniform beheer en beveiliging, wat de kans vergroot dat individuele systemen niet aan dezelfde beschermingsnormen voldoen. Betrokkenen op de minder goed beveiligde locaties lopen daardoor een groter risico de controle over hun gegevens te verliezen	2	2	4
G-3	Inkoopeisen Er zijn geen vooraf vastgestelde technische en organisatorische inkoopeisen waaraan een nieuw camerasysteem moet voldoen	Een systeem dat niet vooraf op de vastgestelde eisen is getoetst, kan achteraf niet in staat blijken de noodzakelijke maatregelen te ondersteunen. Een risico dat pas aan het licht komt nadat het systeem al in gebruik is, met een verhoogd risico dat betrokkenen de controle over hun gegevens verliezen doordat noodzakelijke maatregelen ontbreken	3	2	6
G-4	Reglement cameratoezicht Er is geen, sterk verouderd, onvolledig of onjuist uitgewerkt reglement, het reglement bevat geen uitwerking van de rechten van betrokkenen, het is niet goedgekeurd door de (G)MR, het is niet bekend bij stakeholders, (tijdelijke) afwijkingen van het reglement worden niet vastgelegd, de naleving van het reglement wordt niet gecontroleerd, of het IBP-beleid verwijst er niet naar	Zonder adequaat, actueel en toegankelijk reglement (goedgekeurd door de (G)MR, bekend bij stakeholders en verankerd in het IBP-beleid) weten gebruikers niet volgens welke regels zij het camerasysteem moeten gebruiken. Zonder controle op de naleving blijft gebruik in strijd met het reglement onopgemerkt. Dit verhoogt het risico op incidenten en op verlies van controle van betrokkenen over hun gegevens	2	3	6
G-5	Accountbeheer Er vindt geen gestructureerd accountbeheer plaats, er is geen formeel verantwoordelijke aangewezen, of er is geen formeel aanvraag-, toewijzings- en toekenningsproces voor rechten	Zonder een formeel verantwoordelijke, een proces voor het toewijzen van rollen en rechten, en een koppeling aan het HR-proces bij uitdiensttreding of functiewijziging, kunnen personen zonder (langer) geldige reden toegang krijgen of houden tot het camerasysteem, of over meer rechten binnen het systeem beschikken dan nodig. Betrokkenen verliezen daarmee de controle over hun gegevens, doordat toegang en rechten niet beperkt blijven tot wie dat daadwerkelijk nodig heeft	3	3	9
Borging & controle					

#	Risico	Gevolgen voor betrokkenen			
G-6	Bewustwording medewerkers met toegang tot beelden Medewerkers met autorisatie voor het camerasysteem zijn niet of onvoldoende op de hoogte van de kaders waarbinnen zij beelden mogen bekijken, wat zij wel en niet mogen doen met wat zij zien en wat de gevolgen zijn van misbruik of onzorgvuldig gebruik	Onvoldoende bewustwording bij geautoriseerde medewerkers kan leiden tot (on)bewust ge-/misbruik van beelden. Bijvoorbeeld delen of bekijken buiten het toegestane doel. Betrokkenen verliezen daarmee de controle over hun gegevens, op een manier die technische maatregelen alleen niet voorkomen	2	2	4
G-7	Logging Het camerasysteem ondersteunt geen of onvoldoende logging, waardoor er geen sluitende audittrail beschikbaar is voor de systeemeigenaar	Zonder logging kan niet worden vastgesteld wie beelden heeft bekeken, geëxporteerd of verwijderd. Verlies van controle van betrokkenen over hun gegevens kan hierdoor onopgemerkt blijven en achteraf niet worden onderzocht of gemeld	2	2	4
G-8	Controle logging Er zijn geen richtlijnen voor de controle van logging en/of er vindt geen controle van logging plaats	Als logging wel bestaat maar niet periodiek of naar aanleiding van incidenten wordt gecontroleerd, blijft onrechtmatige inzage even onopgemerkt als zonder logging. Verlies van controle van betrokkenen over hun gegevens wordt niet (eerder) ontdekt	2	3	6
G-9	Verder gebruik locatie door huurders Bij verhuur van (een deel van) de locatie zijn de gebruikers van de huurder betrokkenen van het cameratoezicht van het schoolbestuur. In de huurovereenkomst is niet vastgelegd dat de huurder zijn gebruikers namens het schoolbestuur informeert over het cameratoezicht en de huurder beschikt niet over het geldende reglement cameratoezicht. De tijden van verhuur zijn niet bekend bij de systeemeigenaar, waardoor het tijdschema van de camera's niet is afgestemd op de verhuur	De gebruikers van de huurder worden niet tijdig en correct geïnformeerd over het cameratoezicht, waardoor het schoolbestuur niet voldoet aan zijn informatieplicht en deze betrokkenen hun rechten niet kunnen uitoefenen. Zonder afgestemd tijdschema nemen camera's die tijdens verhuur niet mogen opnemen, zoals camera's met uitsluitend doeleinde 3 en/of 4 en camera's in praktijklokalen en gymzalen, toch op terwijl de gebruikers van de huurder aanwezig zijn	3	2	6
<i>Nieuwbouw en verbouwing</i>					
G-10	Gebouwontwerp Bij het ontwerp van nieuwe of te verbouwen schoolgebouwen wordt geen rekening gehouden met de invloed van de bouwkundige indeling op de noodzaak voor cameratoezicht. Een ondoordachte ruimte-indeling (met veel nissen, hoeken en verspringingen) creëert onoverzichtelijke plekken, die	Een praktisch ondoordachte ruimte-indeling (met veel nissen, hoeken en verspringingen) creëert onoverzichtelijke plekken, wat een ongewenste noodzaak voor een onevenredig groot aantal camera's veroorzaakt om alsnog overzicht te houden. Met een verdergaande belemmering van de vrije ontwikkeling van leerlingen dan bij een doordacht	2	2	4

#	Risico	Gevolgen voor betrokkenen			
	enerzijds een onevenredig groot aantal camera's noodzakelijk maken om alsnog overzicht te houden en anderzijds als ze toch buiten het zicht van camera's blijven, plekken vormen waar ongewenst gedrag onopgemerkt kan plaatsvinden.	ontwerp nodig zou zijn geweest. Blijven onoverzichtelijke plekken toch buiten het zicht van camera's, dan kunnen leerlingen of medewerkers daar eerder worden blootgesteld aan ongewenst gedrag zoals pesten of intimidatie, zonder dat dit wordt opgemerkt. Het ontwerp en het aantal camera's houden elkaar zo in stand.			
G-11	Cameratoezicht via het bestek bij nieuwbouw Bij nieuwbouw wordt cameratoezicht meegenomen in het bestek van de bouwaanbesteding. Ook als het schoolbestuur bij het bestek betrokken is, wordt het cameratoezicht dan als onderdeel van het gebouw aanbesteed. Daarbij wordt vooraf niet getoetst of het cameratoezicht rechtmatig is en lopen de keuze van leverancier, merk en type camera's en recorder via de aanbesteding van het gebouw en niet via de inkoopbeisen en het inkoopproces van het schoolbestuur	Camera's worden geplaatst zonder vastgesteld doel, noodzaakafweging per camera of instemming van de (G)MR. Daarnaast kan een systeem worden geleverd dat niet voldoet aan de technische vereisten uit deze DPIA, zoals het tijdschema, het uitschakelen van niet-noodzakelijke functies en de logging, en dat niet aansluit bij het beheerprincipe van het schoolbestuur	3	2	6

8. Deel D: Beschrijving voorgenomen maatregelen

Dit hoofdstuk beschrijft de technische en organisatorische maatregelen waarmee de risico's uit Deel C worden gemitigeerd. Per risico is vastgelegd welke maatregelen dat risico aanpakken, met de bruto risicoscore vóór en de netto restrisicoscore ná uitvoering van de maatregelen. Er blijft altijd een restrisico over, dat is in alle gevallen acceptabel en wordt per risico toegelicht.

Beoordelingskader maatregelen

De AVG bepaalt in artikel 5 lid 1 sub f dat persoonsgegevens door het nemen van passende technische en organisatorische maatregelen op dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is en dat de persoonsgegevens onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Risico's kunnen worden beperkt door maatregelen te nemen. Deze maatregelen zullen de kans en/of impact verkleinen. Daarmee blijft er een risico over: het restrisico. Rekenkundig uitgelegd betekent dit: [kans (waarschijnlijkheid) X impact (ernst)] -/ [risico-mitigerende maatregelen] = **restrisico**.

21. Maatregelen

Hierna wordt beschreven welke technische en organisatorische maatregelen in redelijkheid dienen te worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Daarbij is opgenomen welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Als de maatregel het risico niet volledig afdekt, is een motivering opgenomen waarom het restrisico acceptabel is.

Alle maatregelen in deze DPIA dienen beleidsmatig in ieder geval vastgelegd te worden in het reglement cameratoezicht. Technische maatregelen worden daarnaast geïmplementeerd in het camerasysteem zelf en de onderliggende infrastructuur.



= Risico



= Restrisico

21.1 Maatregelentabel

#	Risico kort		Maatregelen		Toelichting restrisico
Technisch					
<i>Opname</i>					
T-1	Openbare ruimte	9	- Vaste camera's gericht op de openbare ruimte buiten de eigendomsgrens worden bijgesteld of softwarematig (zwart/wazig) afgeschermd. Alleen de systeemeigenaar kan deze instelling aanpassen. Wijzigingen worden gelogd en vastgelegd in het logboek wijzigingen camera-instellingen - Beweegbare camera's worden softwarematig vastgezet zodat de openbare ruimte buiten de eigendomsgrens niet in beeld kan komen. Alleen de systeemeigenaar kan deze	2	Door fysieke bijstelling of softwarematige afscherming, gecombineerd met logging en vastlegging van wijzigingen in het logboek wijzigingen camera-instellingen, is de kans op onrechtmatige opname van de openbare ruimte

#	Risico kort		Maatregelen		Toelichting restrisico
			instelling aanpassen. Wijzigingen worden gelogd en vastgelegd in het logboek wijzigingen camera-instellingen		verwaarloosbaar geworden
T-2	Geluid	6	Geluidsopname wordt uitgeschakeld in het camerasysteem. Alleen de systeemeigenaar kan deze instelling aanpassen. Wijzigingen worden gelogd en vastgelegd in het logboek wijzigingen camera-instellingen	2	Door het uitschakelen van geluidsopname en het borgen van die instelling via logging, vastlegging in het logboek wijzigingen camera-instellingen en beperkte beheerbevoegdheid is het risico op onrechtmatige geluidsverwerking aanzienlijk verminderd
T-3	Opname technieken	6	AI-technieken bij opname (zoals gezichtsherkenning of gedragsanalyse) worden uitgeschakeld. Alleen de systeemeigenaar kan deze instelling aanpassen. Wijzigingen worden gelogd en vastgelegd in het logboek wijzigingen camera-instellingen <i>Opmerking: deze maatregel betreft geen beoordeling van AI-camerasystemen als zodanig - die vallen buiten de scope van deze DPIA - maar een controlemaatregel voor het geval een regulier camerasysteem ongevraagd over AI-gestuurde opnametechnieken beschikt</i>	2	Door het uitschakelen van AI-opnametechnieken, beperkte wijzigingsbevoegdheid, logging en vastlegging in het logboek wijzigingen camera-instellingen is de kans op onrechtmatige verwerking aanzienlijk verminderd
T-4	Niet-noodzakelijke functies	6	Bij de aanschaf, installatie en configuratie van het camerasysteem worden uitsluitend de functies ingeschakeld die strikt noodzakelijk zijn voor de vastgestelde verwerkingsdoeleinden per camera (privacy by default, art. 25 lid 2 AVG). Aanwezige maar niet-noodzakelijke functies, zoals onbeperkte PTZ-beweging, optische zoom, geluidsopname, analytische functies en draadloze verzending, worden technisch uitgeschakeld of geblokkeerd. Alleen de systeemeigenaar kan dergelijke functies activeren. Elke activering wordt gelogd, vastgelegd in het logboek wijzigingen camera-instellingen en vereist een aantoonbare relatie met een vastgesteld verwerkingsdoel	2	Door privacy by default bij aanschaf en configuratie, technische blokkering van onnodige functies en beperkte activeringsrechten is de kans op onrechtmatige verwerking aanzienlijk verminderd. Logging en vastlegging in het logboek wijzigingen camera-instellingen maken afwijkend gebruik detecteerbaar.
<i>Opslag & beveiliging</i>					
T-5	Opslag beelden	6	Sluit een verwerkersovereenkomst met de cloudopslag leverancier en met de	2	Met een getoetste verwerkersovereenko

#	Risico kort		Maatregelen		Toelichting restrisico
			leverancier van online beheer- of viewsoftware. Verifieer dat de leverancier voldoende technische en organisatorische maatregelen heeft genomen en opslaat of verwerkt binnen de EER, een land met adequaatheidsbesluit, dan wel beschikt over een passende doorgifte-waarborg (bijv. SCC) inclusief DTIA OF Stap over op goed ingerichte lokale opslag met lokaal geïnstalleerde beheer- en viewsoftware. Het schoolbestuur verwerkt de beelden dan volledig binnen de eigen organisatie en een verwerkersovereenkomst is dan niet vereist		mst of overstap naar lokale opslag en software is de juridische grondslag voor de verwerking geborgd en heeft de verwerkingsverantwoordelijke voldoende grip op de verwerking
T-6	Technische beveiliging	6	- Het camerasysteem is aangesloten op een compleet fysiek of logisch gescheiden netwerk. Bij een logisch gescheiden netwerk (VLAN) is een firewall actief tussen het camerasegment en de overige netwerksegmenten, zodat alleen strikt noodzakelijk verkeer is toegestaan. Bij een volledig fysiek gescheiden netwerk zonder internetverbinding is deze maatregel niet van toepassing - Waar het camerasysteem online bereikbaar is, is altijd een firewall aanwezig die inkomend en uitgaand verkeer beperkt tot wat strikt noodzakelijk is voor het beoogde gebruik. Waar het camerasysteem is verbonden met bredere IT-infrastructuur of online bereikbaar is, zijn aanvullende beveiligingsmaatregelen getroffen, zoals netwerkinbraakdetectie (IDS/IPS) of gelijkwaardige monitoring. Bij een volledig fysiek gescheiden netwerk zonder internetverbinding is deze maatregel niet van toepassing - Bij online of remote toegang tot het camerasysteem is MFA verplicht ingesteld. Bij uitsluitend lokale toegang is MFA ingesteld waar het systeem dit ondersteunt. Is dat niet het geval, dan worden wachtwoorden of wachtzinnen van minimaal 15 tekens gebruikt. Standaardwachtwoorden van de fabrikant zijn bij ingebruikname gewijzigd. Er gelden geen verplichte samenstellingsregels en geen periodieke wijziging, een wachtwoord	2	Door netwerksegmentatie, verplichte MFA bij online en remote toegang, lange wachtzinnen, automatische sessievergrendeling, versleuteling van opslag en transport en actueel patchbeheer zijn de technische beveiligingsrisico's tot een aanvaardbaar niveau teruggebracht

#	Risico kort		Maatregelen		Toelichting restrisico
			wordt direct gewijzigd bij (vermoeden van) compromittering. Veelgebruikte of eerder gelekte wachtwoorden en hergebruik van wachtwoorden zijn niet toegestaan - Een sessie waarin live wordt meegekeken, beelden worden teruggekeken of camera-instellingen worden gewijzigd, vergrendelt automatisch na maximaal vijf minuten inactiviteit, waarna opnieuw inloggen vereist is. Bij live kijken blijven de beelden daarna wel zichtbaar - Opgeslagen beeldmateriaal is versleuteld (versleuteling in rust). Ondersteunt een bestaande recorder dit aantoonbaar niet, dan staat de recorder in een afgesloten ruimte, wordt dit vastgelegd in de lokale DPIA en is versleuteling in rust een eis bij vervanging van het systeem - Beelden worden versleuteld getransporteerd bij overdracht via een logisch gescheiden netwerk (VLAN), een cloudverbinding of een internetverbinding. Bij een volledig fysiek gescheiden netwerk zonder internetverbinding is deze maatregel niet van toepassing - Het systeem past securityupdates automatisch toe OF Securityupdates worden minimaal eens per kwartaal handmatig gecontroleerd en toegepast		
Organisatorisch					
<i>Beleid & rechten</i>					
O-1	Doelbinding	6	- Stel duidelijke doeleinden vast voor het gebruik van cameratoezicht. De doeleinden (1) tot en met (4) worden per camera vastgesteld in het cameraoverzicht, de doeleinden (5) tot en met (7) gelden voor het cameratoezicht als geheel: (1) De bescherming van de veiligheid en gezondheid van leerlingen, medewerkers en bezoekers. (2) De beveiliging van de toegang tot gebouwen en terreinen, waaronder mede begrepen het weren van onbevoegden. (3) Het voorkomen en registreren van overlast en strafbare feiten zoals vandalisme, diefstal en inbraak. (4) De bewaking van zaken die zich in de gebouwen of op de terreinen bevinden.	1	Door per camera een vastgesteld en gedocumenteerd doeleinde te vereisen is doelbeperking geborgd en is willekeurig gebruik aantoonbaar in strijd met het vastgestelde beleid

#	Risico kort		Maatregelen		Toelichting restrisico
			(5) Het vastleggen van incidenten ten aanzien van de onder (1) tot en met (4) genoemde doeleinden. (6) Beveiliging, controle en ook verantwoording van de verwerking door middel van systeemlogging (audittrail) en logboeken (logboek wijzigingen camera-instellingen, logboek reglement afwijkingen en logboek beeldgebruik). (7) Verstrekking van incidentgegevens aan derden, op eigen besluit of op vordering (bijvoorbeeld aan politie of justitie) • Ieder jaar worden de doeleinden van alle camera's in het cameraoverzicht opnieuw getoetst, inclusief de actualiteit van de voor iedere camera vastgelegde aanleiding • Kan er geen toelaatbaar doel (meer) worden vastgesteld voor een camera, dan wordt die camera verwijderd of buiten gebruik gesteld		
O-2	Bewaar-termijnen	9	• Het camerasysteem is ingesteld op een automatische bewaartermijn van standaard drie weken, die met een gemotiveerde reden kan worden verlengd tot maximaal vier weken. Tijdens de zomervakantie geldt een maximale bewaartermijn van zes weken. Na de zomervakantie valt de bewaartermijn terug naar de reguliere bewaartermijn. Ondersteunt het camerasysteem dit, dan gebeurt dit automatisch. Is dat niet het geval, dan zet de systeemeigenaar de bewaartermijn na de eerste schooldag en uiterlijk op de tweede schooldag handmatig terug en legt deze wijziging vast in het logboek wijzigingen camera-instellingen. Beelden worden na afloop van de ingestelde termijn automatisch overschreven	2	Door automatische overschrijving na de ingestelde termijn is naleving van de opslagbeperking technisch geborgd. Ondersteunt het camerasysteem de terugval na de zomervakantie niet automatisch, dan is de handmatige terugval belegd bij de systeemeigenaar, met een vast moment en vastlegging in het logboek, zodat naleving controleerbaar blijft
O-3	Proportionaliteit en Subsidiariteit	6	• Voor iedere camera is in het cameraoverzicht een aanleiding vastgelegd. Hoe zwaar die aanleiding moet zijn, hangt af van het moment waarop de camera opneemt. Camera's die uitsluitend zijn ingezet voor de doeleinden 3 en/of 4 nemen alleen buiten de Gebruikstijden van de locatie op, dus niet tijdens Schooltijd en niet tijdens verhuur. Buiten de Gebruikstijden zijn er op het eigen terrein geen personen aanwezig die daar mogen	2	Door het verbod op cameratoezicht in leslokalen en gymzalen tijdens gebruik van de ruimte, het per camera technisch afgedwongen tijdschema zonder handmatige tussenkomst, de verplichte

#	Risico kort		Maatregelen		Toelichting restrisico
			zijn, zoals leerlingen, medewerkers of gebruikers van huurders. De inbreuk is daardoor beperkt en als aanleiding volstaan incidenten op of rond de locatie, of een aantoonbaar dreigend gevaar, zoals de aanwezigheid van kostbare apparatuur. Camera's die (mede) zijn ingezet voor doeleinde 1 en/of 2 mogen ook tijdens de Gebruikstijden opnemen. Omdat leerlingen, medewerkers en bezoekers dan in beeld komen, geldt voor deze camera's een zwaardere eis: het doeleinde is per camera onderbouwd met daadwerkelijke voorvallen of een aantoonbaar dreigend gevaar op die plek. Een voorval op één plek rechtvaardigt alleen een camera op die plek • In leslokalen en gymzalen wordt nooit gefilmd terwijl de ruimte in gebruik is door personen die daar mogen zijn, zoals leerlingen, medewerkers en gebruikers van huurders. Buiten de Gebruikstijden is cameratoezicht daar uitsluitend toegestaan in praktijklokalen met kostbare apparatuur en in gymzalen, ter beveiliging van de ruimte en de daarin aanwezige eigendommen • Leg per camera het tijdschema vast in het cameraoverzicht, rekening houdend met de Gebruikstijden van de locatie. Het camerasysteem dwingt dit tijdschema per camera technisch af. Handmatig aan- en uitzetten is geen toegestaan alternatief. Kan het tijdschema niet technisch worden ingericht, dan is cameratoezicht niet toegestaan met een camera die uitsluitend is ingezet voor de doeleinden 3 en/of 4. Wijzigingen in het tijdschema worden vastgelegd in het logboek wijzigingen camera-instellingen • Cameratoezicht in toiletten, kleedkamers of andere ruimtes met een fundamenteel privacykarakter is, ongeacht het doel, nooit aanvaardbaar • Cameratoezicht om leerlingen en/of medewerkers te beoordelen is niet toegestaan. Bij constatering hiervan worden camera's per direct buiten gebruik gesteld of verwijderd		subsidiariteitsafweging per camera, de borging dat andere preventieve maatregelen actief blijven en de verplichte consultatie van leerlingen via de oudergeleding van de (G)MR of de leerlingenraad, is de proportionaliteitseis procedureel aantoonbaar geborgd

#	Risico kort		Maatregelen		Toelichting restrisico
			• Stel per camera een overzicht op van andere preventieve maatregelen die de organisatie heeft getroffen om hetzelfde doel te bereiken. Beoordeel per camera, mede op basis van het effect dat deze maatregelen hebben gehad, of het doel zonder cameratoezicht kan worden bereikt. Leg het overzicht en de uitkomst van de beoordeling vast in het cameraoverzicht en herhaal de beoordeling bij de jaarlijkse toets van de doeleinden • Ontbreken andere preventieve maatregelen volledig, dan worden deze opnieuw vastgesteld en ingevoerd voordat het cameratoezicht wordt voortgezet • Laat bij de initiële plaatsing van camera's of aanvullende cameraplaatsing deze beoordelen door de betrokkenen (m.n. de leerlingen) op o.a. een onaanvaardbaar chilling effect bij leerlingen (PO via de oudergeleding van de MR, VO via de leerlingenraad). Leg de uitkomst vast in het cameraoverzicht • Raadpleeg leerlingen bij de vaststelling of wijziging van het reglement cameratoezicht, voor het PO via de oudergeleding van de MR en voor het VO via de leerlingenraad. Leg de uitkomst van de consultatie schriftelijk vast		
O-4	Verplaatsbare camera's	6	• Zorg ervoor dat camera's fysiek zijn bevestigd op een vaste locatie, zodanig dat verplaatsing niet mogelijk is zonder (speciaal) gereedschap • Een camera wordt alleen verplaatst of anders gericht na een gezamenlijk besluit van de proceseigenaar en de systeemeigenaar, op advies van de privacy officer. Vóór ingebruikname op de nieuwe positie wordt de camera opnieuw getoetst aan doel, noodzaak en plaatsing en wordt zo nodig de bebording aangepast. De verplaatsing en de uitkomst van de toets worden vastgelegd in het cameraoverzicht	2	Doordat verplaatsing speciaal gereedschap vereist, is ad-hoc verplaatsing door onbevoegden feitelijk uitgesloten. Verplaatsen of anders richten kan alleen na een gezamenlijk besluit van de proceseigenaar en de systeemeigenaar, op advies van de privacy officer, en een nieuwe toets, en wordt vastgelegd in het cameraoverzicht. Daardoor beslist niemand alleen over een nieuwe positie, is

#	Risico kort		Maatregelen		Toelichting restrisico
					iedere nieuwe positie getoetst aan doelbinding en proportionaliteit en is dit controleerbaar
O-5	Transparantie	6	- Laag 1: Zorg ervoor dat er duidelijke bebording* is bij iedere camera waar betrokkenen zonder een barrière toegang hebben tot de locatie (bijvoorbeeld een vrij toegankelijk looppad langs de school), bij ieder toegangspunt in een hekwerk, op iedere buitendeur bij het naar binnen treden van de locatie (als er ook cameratoezicht binnen is) en bij iedere separaat in beeld gebrachte ruimte binnen het gebouw (kantine, aula, trappenhuis, nooduitgang, etc.) * cameraborden met cameralogo, cameratoezicht, tijdsperiode opname, identiteit verwerkingsverantwoordelijke, doel, bewaartermijn, privacygevoelige informatie, bijvoorbeeld: live monitoring, verstrekking aan derden en verwijzing naar tweede laag - zie bijlage 5 voor voorbeeld - Laag 2: De verwerking (beeldmateriaal t.b.v. bewakingsdoeleinden) is opgenomen in de privacyverklaring voor leerlingen/ouders en medewerkers en is eenvoudig vindbaar. Voor leerlingen en ouders minimaal op de school- en/of bestuurswebsite, met maximaal 1 keer doorklikken vanaf de hoofdpagina, en voor medewerkers daarnaast minimaal op de interne communicatieportal, met maximaal 1 keer doorklikken - Het "reglement cameratoezicht" van de organisatie is voor alle betrokkenen eenvoudig vindbaar. Voor alle betrokkenen minimaal op de school- en/of bestuurswebsite, met maximaal 1 keer doorklikken vanaf de hoofdpagina - Zorg bij aanvang van elk schooljaar voor leeftijdsadequate informatie over het cameratoezicht, afgestemd op de leeftijdsfase van leerlingen. Voor het PO in eenvoudige en waar mogelijk visuele vorm, voor het VO volledig inclusief uitleg over hun rechten. Documenteer de uitvoering hiervan	2	Door bebording op alle relevante punten en digitale vindbaarheid van de privacyverklaring en het reglement is aan de transparantieverplichting voldaan

#	Risico kort		Maatregelen		Toelichting restrisico
O-6	Privacy-rechten betrokkenen	4	• Stel een procedure op voor het afhandelen van privacyrechtverzoeken (inzage, verwijdering, beperking en bezwaar) • Leg vast hoe wordt omgegaan met een verzoek dat niet bij het juiste contactpunt binnenkomt: intern doorsturen naar het contactpunt of de betrokkene verwijzen naar het contactpunt • Wijs de proceseigenaar aan als verantwoordelijke voor tijdige afhandeling. Bij inzageverzoeken die betrekking hebben op beeldmateriaal reageert de proceseigenaar zo snel als redelijkerwijs mogelijk, gezien de korte bewaartermijnen en de kans dat het betreffende beeldmateriaal anders niet meer beschikbaar is • Informeer betrokkenen in de privacyverklaring over het bestaan van deze rechten en de wijze waarop zij een verzoek kunnen indienen • Bij inzageverzoeken mogen camerabeelden van de betrokkene de privacy van andere betrokkenen niet schaden (dus niet in beeld), neem dit op in de procedure	1	Met een gedocumenteerde procedure, heldere verantwoordelijkheid bij de proceseigenaar en informatieverstrekking aan betrokkenen is het risico op schending van privacyrechten tot een aanvaardbaar niveau teruggebracht
O-7	Datalek-respons en incident-afhandeling camera-systeem	4	• Verifieer dat het camerasysteem expliciet is opgenomen in het bestaande datalekresponsbeleid van het schoolbestuur. Voeg indien nodig een beknopte notitie toe die beschrijft hoe bij een incident met het camerasysteem wordt omgegaan met het veiligstellen van beeldmateriaal, gezien de korte bewaartermijnen en automatische overschrijving. Deze notitie hoeft geen zelfstandig document te zijn maar kan als aanvulling worden opgenomen in het bestaande beleid of het reglement cameratoezicht	1	Door expliciete verankering van het camerasysteem in het bestaande datalekresponsbeleid en een beknopte camera specifieke aanvulling is geborgd dat bij een incident tijdig kan worden beoordeeld welk beeldmateriaal is gecompromitteerd
<i>Toegang & gebruik</i>					
O-8	Autorisatie	6	• Stel bovenschools een autorisatiematrix vast die per rol vastlegt welke acties binnen het camerasysteem zijn toegestaan • Iedere gebruiker heeft een persoonlijk account, accounts worden niet gedeeld	2	Met een autorisatiematrix en persoonlijke accounts is toegang tot beelden controleerbaar en zijn misstanden aantoonbaar en herleidbaar
O-9	Hoe/wanneer	6	• Stel vast op welke manier beelden teruggekeken mogen worden (bijv. alleen	2	Door het vier-ogenprincipe, verplicht

#	Risico kort		Maatregelen		Toelichting restrisico
	beelden terugkijken		op de locatie, alleen via een door het schoolbestuur beheerd apparaat) - Het systeem is zo ingericht dat altijd opnieuw ingelogd moet worden voordat beelden teruggekeken kunnen worden, ook als er op dat moment al live beelden worden bekeken - Beelden worden door minimaal twee bevoegde collega's tegelijk bekeken. Stel vast welke combinaties van collega's dit mogen doen en neem dit op in de autorisatiematrix. Een medewerker van de onderhoudspartij telt niet mee voor dit vier-ogenprincipe en bekijkt beelden uitsluitend bij storingen of onderhoud. Alleen bij een calamiteit buiten Schooltijd mag individueel worden teruggekeken, volgens de richtlijnen voor calamiteiten, ook dan wordt het terugkijken vastgelegd in het logboek beeldgebruik - Het terugkijken van beelden wordt geregistreerd in het logboek beeldgebruik met minimaal: datum/tijdstip, tijdspad van de bekeken beelden, welke camera, reden en door wie of welke twee personen - Stel richtlijnen op voor calamiteiten buiten Schooltijd, waarbij individueel en zo nodig op afstand beelden teruggekeken mogen worden. Beperk dit tot calamiteiten (inbraak(poging), brandalarm, geweldsincident e.d.)		inloggen, logboekregistratie en vastgelegde uitzonderingen is ongecontroleerd terugkijken van beelden procedureel geborgd
O-10	Welke beelden terugkijken	4	Terugkijken van beelden is alleen toegestaan op momenten die voldoen aan de vastgestelde verwerkingsdoeleinden. Werk deze doeleinden uit in concrete, herkenbare voorbeeldsituaties	1	Door het terugkijken te beperken tot vastgestelde doeleinden, uitgewerkt in concrete situaties, is doelbeperking operationeel geborgd
O-11	Ongeautoriseerde eigen opnames van beelden	6	Neem een expliciete verbodsbepaling op in het reglement cameratoezicht: medewerkers mogen nimmer camerabeelden (ongeacht of daar betrokkenen op staan of niet) buiten het camerasysteem vastleggen (bijv. via mobiel het scherm filmen of exporteren naar een privéapparaat)	2	Met een expliciete verbodsbepaling in het reglement cameratoezicht is het risico verminderd. Het is technisch niet volledig te voorkomen dat iemand het scherm filmt met een privéapparaat. De kans is echter laag en de maatregel maakt de

#	Risico kort		Maatregelen		Toelichting restrisico
					handeling aantoonbaar onrechtmatig
O-12	Live beelden bekijken	6	- Stel richtlijnen op voor live kijken: alleen toegestaan in het kader van het voorkomen van en direct handelen bij incidenten. Dit moet in de praktijk ook daadwerkelijk plaatsvinden - Live beelden mogen alleen worden bekeken door medewerkers die in de autorisatiematrix zijn opgenomen - Beeldschermen waarop live beelden worden getoond, zijn zo opgesteld dat alleen medewerkers die in de autorisatiematrix zijn opgenomen de beelden kunnen zien en anderen niet kunnen meekijken, ook niet van buiten de ruimte, bijvoorbeeld door een raam	2	Door richtlijnen voor toegestaan gebruik, beperking tot bevoegde medewerkers en een opstelling van beeldschermen waarbij anderen niet kunnen meekijken, wordt willekeurig meekijken voorkomen
O-13	Beelden online terugkijken	9	- Toegang op afstand tot het camerasysteem is uitsluitend mogelijk voor accounteigenaren die daartoe in de autorisatiematrix zijn opgenomen, de systeemeigenaar implementeert dit technisch - Accounts voor toegang op afstand hebben uitsluitend kijkrechten: exporteren en downloaden zijn technisch uitgeschakeld en de app of webinterface slaat geen beelden op het apparaat op - Beelden mogen online alleen worden bekeken op door de organisatie beheerde apparaten, privéapparaten zijn niet toegestaan. Online toegang is beveiligd met MFA - Online toegang vergroot het aanvalsoppervlak: de infrastructuurbeveiliging is hierop afgestemd en de onderhoudsfrequentie van het camerasysteem is verhoogd	2	Door toegang op afstand te beperken tot calamiteiten buiten Schooltijd en tot bevoegde accounteigenaren met uitsluitend kijkrechten, en door online toegang te beveiligen met MFA en alleen toe te staan op beheerde apparaten waarop geen beelden worden opgeslagen, is het risico op ongeautoriseerde externe inzage, ook bij verlies of diefstal van een apparaat, tot een aanvaardbaar niveau teruggebracht
O-14	Bewaren van Beelden	4	- Stel richtlijnen op voor de situaties waarin beelden bewaard mogen worden - Iedere beslissing om beelden te bewaren of bewaard beeldmateriaal te verwijderen wordt geregistreerd in het logboek beeldgebruik met minimaal: datum/tijdstip, tijdspad van de beelden, welke camera, reden, door welke twee personen het besluit is genomen en wanneer verwijdering heeft plaatsgevonden. Het logboek beeldgebruik is als bijlage bij het reglement opgenomen	2	Door duidelijke richtlijnen, logboekregistratie van bewaar- en verwijderbeslissingen, een vastgestelde bewaartermijn en de periodieke controle van het logboek beeldgebruik (G-8) is de opslagbeperking

#	Risico kort		Maatregelen		Toelichting restrisico
			- Beelden worden bewaard binnen het camerasysteem zelf of op een extra beveiligde plek binnen de schoolbestuur kantoorautomatiseringsomgeving - Stel een bewaartermijn vast voor bewaard beeldmateriaal		voor incidentbeelden aantoonbaar geborgd
O-15	Inzage beelden door derden	6	- Stel richtlijnen op voor situaties waarin inzage aan derden (iedereen buiten de autorisatiematrix) is toegestaan - Iedere inzage aan derden wordt geregistreerd in het logboek beeldgebruik met minimaal: datum/tijdstip van inzage, tijdspad van de ingeziene beelden, welke camera, reden, door welke twee personen inzage is verleend, wie het besluit heeft genomen, aan wie inzage is verleend en hoe de ontvanger zich heeft geïdentificeerd	2	Door richtlijnen en verplichte logboekregistratie van iedere inzage is onrechtmatige toegang door derden aantoonbaar gemaakt en controleerbaar
O-16	Delen beelden met derden	6	- Stel richtlijnen op voor situaties waarin beelden met derden (iedereen buiten de autorisatiematrix) gedeeld mogen worden - Iedere deling wordt geregistreerd in het logboek beeldgebruik met minimaal: datum/tijdstip, tijdspad van de gedeelde beelden, welke camera, reden, door welke twee personen het delen is uitgevoerd, wie het besluit heeft genomen, met wie gedeeld is en hoe de ontvanger zich heeft geïdentificeerd - Stel richtlijnen op voor de technische wijze van delen: bij voorkeur via een vanuit het camerasysteem gegenereerde beveiligde link, waarbij is in te stellen of de ontvanger de beelden alleen kan bekijken of ook kan downloaden en hoe lang de link geldig is, anders via een versleutelde drager of een beveiligde uploadvoorziening van de ontvanger. Delen via e-mail of openbaar toegankelijke platforms is niet toegestaan - Stel een identificatieplicht vast voor de ontvanger van beelden	2	Door richtlijnen voor toegestane situaties, verplichte identificatie van de ontvanger, versleutelde overdracht en logboekregistratie is onrechtmatig delen van beelden aantoonbaar georganiseerd
Beheer					
O-17	Technisch Onderhoud	6	Onderhoudsafspraken (w.o. updates, upgrades, securitypatches) worden vastgelegd in een SLA met de onderhoudspartij en minimaal jaarlijks geëvalueerd door de proceseigenaar en systeemeigenaar OF	2	Door vastgelegde onderhoudsafspraken, opgenomen hersteltijden en compenserende maatregelen bij uitval en een geheimhoudingsclausul

#	Risico kort		Maatregelen		Toelichting restrisico
			De systeemeigenaar is zelf verantwoordelijk voor het onderhoud, hiervoor worden duidelijke interne afspraken gemaakt in een interne SLA - In de SLA of interne onderhoudsafspraken zijn hersteltijden (RTO) opgenomen voor het geval het camerasysteem uitvalt door een technisch of fysiek incident. De proceseigenaar is op de hoogte van de herstelprocedure en kan bij uitval adequate tijdelijke compenserende maatregelen treffen (bijv. tijdelijk verhoogd fysiek toezicht of beveiligingsronden) totdat het systeem is hersteld - In de SLA met een externe onderhoudspartij wordt een geheimhoudingsclausule opgenomen die het bekijken, opslaan en distribueren van camerabeelden verbiedt, tenzij strikt noodzakelijk op verzoek van de proceseigenaar/ systeemeigenaar		e voor onderhoud op afstand en op locatie is onbeheerd beheer van het camerasysteem voorkomen en is de continuïteit van de beveiliging geborgd
O-18	Externe onderhoudspartij	6	- Heeft de externe onderhoudspartij Structurele toegang tot het camerasysteem, sluit dan een verwerkersovereenkomst met deze partij - Verifieer dat de onderhoudspartij voldoende technische en organisatorische maatregelen heeft genomen	1	Met een getoetste verwerkersovereenkomst bij Structurele toegang is de juridische grondslag geborgd en heeft de verwerkingsverantwoordelijke voldoende grip op de verwerking. Zonder Structurele toegang beperkt de toegang van de onderhoudspartij zich tot lokaal onderhoud, waarvoor de geheimhoudingsafspraken in de SLA gelden
O-19	Fysieke beveiliging	6	- Technische componenten (recorder, switches) bevinden zich in een afgesloten technische ruimte. Als anderen dan de systeemeigenaar, proceseigenaar of geautoriseerde medewerkers toegang nodig hebben, bevinden de cameratoezicht componenten zich ook in een afgesloten patchkast die niet van de zijkant of achterkant te benaderen is - De technische ruimte is bij voorkeur beveiligd met een elektronisch slot. Is dit	2	Door fysieke afscherming van technische componenten en de kijkruimte via een afgesloten ruimte en toegangsregistratie wordt onbevoegde fysieke toegang aantoonbaar voorkomen

#	Risico kort		Maatregelen		Toelichting restrisico
			niet het geval, dan is er een sleutelregistratie en wordt iedere toegang tot de ruimte geregistreerd op een inschrijffijst De ruimte van waaruit live beelden of beelden teruggekeken kunnen worden is afgesloten en alleen toegankelijk voor medewerkers in de autorisatiematrix		
Governance					
<i>Inrichting & beheer</i>					
G-1	Eigenaarschap	9	- Er is een bestuursbrede proceseigenaar (rol) aangesteld voor het cameratoezicht - Er is een bestuursbrede systeemeigenaar (rol) aangesteld voor het cameratoezicht - Taken en verantwoordelijkheden van beide rollen zijn uitgewerkt in het reglement cameratoezicht en zijn bekend bij de rolhouders - Technisch beheer van het/de camerasyste(e)m(en) is centraal geborgd bij de systeemeigenaar op bestuursniveau - De proceseigenaar en de systeemeigenaar zijn, op advies van de privacy officer, gezamenlijk verantwoordelijk voor het beoordelen en goedkeuren van iedere aanschaf van camerasystemen	2	Door duidelijke toewijzing van eigenaarschap op bestuursniveau en documentatie van taken en verantwoordelijkheden zijn implementatie, beheer en controle geborgd
G-2	Inkoopproces	4	- Sluit aan bij het bestaande centrale inkoopproces van het schoolbestuur. Is een dergelijk proces er niet, dan verloopt de aanschaf van camerasystemen altijd via de proceseigenaar, die hiervoor zelf een proces inricht - De aanschaf is erop gericht dat binnen het schoolbestuur, zolang dit technisch mogelijk is, met één type camerasysteem wordt gewerkt, dat bij een nieuwe generatie kan worden geüpdatet in plaats van vervangen. Waar dit financieel verstandig is, wordt met één onderhoudspartij gewerkt, met aandacht voor het voorkomen van een te grote afhankelijkheid van één leverancier (beheerprincipe)	2	Door een centraal inkoopproces is geborgd dat nieuwe camerasystemen via één vaste route worden aangeschaft. Het beheerprincipe zorgt ervoor dat zoveel mogelijk met één type camerasysteem wordt gewerkt, wat versnippering voorkomt en uniform beheer en beveiliging mogelijk maakt
G-3	Inkoop-eisen	6	Stel als inkoop-eis dat het camerasysteem kan voldoen aan de in deze DPIA vastgestelde technische vereisten. Denk daarbij aan: het kunnen uitschakelen van niet-noodzakelijke opnamefuncties zoals geluid, AI-technieken en overige niet-	2	Door vooraf vastgestelde inkoop-eisen is geborgd dat nieuwe systemen kunnen voldoen aan de vastgestelde

#	Risico kort		Maatregelen		Toelichting restrisico
			noodzakelijke functies, softwarematige afscherming van delen van het beeld, netwerk- en toegangsbeveiliging (netwerksegmentatie, MFA, hernieuwd inloggen bij terugkijken, automatische sessievergrendeling), versleuteling van opgeslagen beelden en van het transport, een instelbare bewaartermijn met automatische overschrijving, bij voorkeur met de mogelijkheid om de verlengde termijn voor de zomervakantie vooraf in te plannen, zodat de terugval naar de reguliere termijn automatisch plaatsvindt, een per camera instelbaar tijdschema dat het camerasysteem zonder handmatige tussenkomst afdwingt, en logging/audittrail. Neem bij voorkeur ook privacy-by-design elementen mee, zoals ondersteuning bij het bijhouden van de logboeken (het uitvragen van de benodigde logboekinformatie bij terugkijken en bij het wijzigen van instellingen), rolgebaseerde toegangscontrole aansluitend op de autorisatiematrix en de mogelijkheid om beelden te vervagen of uit te snijden bij verstrekking aan betrokkenen. Werk deze inkoop Eisen uit in een concrete, schoolbestuur-eigen checklist		technische en organisatorische maatregelen
G-4	Reglement camera-toezicht	6	• Stel een reglement cameratoezicht op dat voldoet aan de AVG-minimumvereisten, alle elementen uit deze DPIA bevat en een revisiecyclus van twee jaar kent • Het reglement cameratoezicht is goedgekeurd door de (G)MR • De proceseigenaar zorgt dat het reglement bekend is bij alle stakeholders en controleert steekproefsgewijs het gebruik van het camerasysteem • Afwijkingen van het reglement zijn uitsluitend toegestaan na voorafgaande toestemming van het bestuur en worden vastgelegd in het logboek reglement afwijkingen • In het IBP-beleid wordt verwezen naar het cameratoezicht en het reglement cameratoezicht	1	Met een volledig, goedgekeurd en gepubliceerd reglement dat tweejaarlijks wordt herzien, is de organisatorische borging van cameratoezicht aantoonbaar
G-5	Account-beheer	9	• Wijs een formeel verantwoordelijke aan voor accountbeheer (proceseigenaar of systeemeigenaar)	2	Door gestructureerd accountbeheer met een aangewezen

#	Risico kort		Maatregelen		Toelichting restrisico
			- Stel een proces op voor het aanvragen, toewijzen en toekennen van rollen en rechten binnen het camerasysteem - Neem het verwijderen van accounts binnen camerasystemen op in het bestaande HR-proces "uit-dienst" en/of "wijziging van functie" - Bij de steekproefsgewijze controle van het gebruik van het camerasysteem gaat de proceseigenaar na of de accounts en de toegekende rechten nog overeenkomen met de autorisatiematrix		verantwoordelijke, koppeling aan het HR-proces en periodieke controle van accounts en rechten worden onbevoegde accounts tijdig verwijderd en is toegang aantoonbaar geregeld
<i>Borging & controle</i>					
G-6	Bewustwording medewerkers met toegang tot beelden	4	- Stel een bewustwordingsprogramma op specifiek voor medewerkers met toegang tot het camerasysteem, gericht op o.a.: de vastgestelde doeleinden en kaders, het vier-ogenprincipe, de verbodsbepaling op eigen opnames, de logboekplicht en de gevolgen van misbruik of onzorgvuldig gebruik - Medewerkers met toegang ontvangen bij het verkrijgen van hun autorisatie een briefing en bevestigen schriftelijk kennis te hebben genomen van het reglement cameratoezicht - Het bewustwordingsprogramma wordt jaarlijks herhaald, gekoppeld aan de jaarlijkse evaluatie van de rechtmatigheid van de camera's	1	Door gerichte bewustwording bij autorisatie, schriftelijke bevestiging en een jaarlijkse herhaling is de kans op onbewust misbruik door bevoegde medewerkers aanzienlijk verminderd
G-7	Logging	4	- Controleer of logging beschikbaar is, aanstaat en toegankelijk is voor de systeemeigenaar OF Als het camerasysteem geen of onvoldoende logging biedt: update naar een versie die dit wel ondersteunt en zet logging aan - Ondersteunt het camerasysteem ook na een update aantoonbaar geen of onvoldoende logging, dan wordt dit vastgelegd in de lokale DPIA en is logging een eis bij vervanging van het systeem	2	Met werkende en toegankelijke logging heeft de systeemeigenaar een audittrail om gebruik te monitoren en bij incidenten te reconstrueren. Ondersteunt een bestaand systeem geen logging, dan is het ontbreken ervan vastgelegd in de lokale DPIA, waarin het bestuur het restrisico afweegt en is logging een eis bij vervanging
G-8	Controle logging	6	Stel richtlijnen op voor zowel proactieve (periodiek, per kwartaal of halfjaar) als reactieve (incidentgestuurde) controle van	2	Door periodieke en incidentgestuurde controle van de logging

#	Risico kort		Maatregelen		Toelichting restrisico
			de logging en de logboeken door de systeemeigenaar. De systeemeigenaar rapporteert de uitkomsten aan de proceseigenaar		en de logboeken, met rapportage aan de proceseigenaar, is toezicht op gebruik geborgd en kunnen afwijkingen tijdig worden gesignaleerd
G-9	Verder gebruik locatie door huurders	6	- In de huurovereenkomst wordt vastgelegd dat op de locatie cameratoezicht plaatsvindt en dat de huurder zijn gebruikers namens het schoolbestuur hierover informeert. Het schoolbestuur stelt de huurder daarvoor de benodigde informatie ter beschikking. Het reglement cameratoezicht maakt als bijlage onderdeel uit van de overeenkomst - Degene die de huurovereenkomst namens het schoolbestuur aangaat, geeft de tijden van verhuur voorafgaand aan de verhuur door aan de systeemeigenaar, zodat het tijdschema van de camera's daarop wordt afgestemd	1	Door de contractuele afspraak en het ter beschikking stellen van de informatie bereikt de informatie over het cameratoezicht ook de gebruikers van de huurder. Daarnaast informeert de bebording bij de toegangen alle betrokkenen, ook de gebruikers van de huurder
<i>Nieuwbouw en verbouwing</i>					
G-10	Gebouw ontwerp	4	- Betrek bij elk ontwerp- of verbouwtraject van een schoolgebouw de proces- en/of systeemeigenaar cameratoezicht, zodat de bouwkundige indeling vooraf wordt beoordeeld op de noodzaak voor aanvullend cameratoezicht - Neem als ontwerpeis op dat een overvloed aan nissen, hoeken of anderszins onoverzichtelijke ruimtes wordt vermeden waar dit redelijkerwijs mogelijk is. Is dit niet mogelijk (bijvoorbeeld bij monumentale of bestaande bouw), dan wordt dit vooraf gemeld bij de proceseigenaar, zodat de noodzaak voor aanvullend cameratoezicht bewust wordt afgewogen in plaats van pas achteraf te blijken	2	Door de proces-/systeemeigenaar vooraf te betrekken en onoverzichtelijke ruimtes als ontwerpeis te benoemen, wordt de noodzaak voor aanvullend cameratoezicht een bewuste afweging in plaats van een onbedoeld gevolg. Bij bestaande of monumentale bouw blijft dit niet altijd volledig te voorkomen
G-11	Camera-toezicht via het bestek bij nieuwbouw	6	- Neem camera's en recorder niet op in het bestek van de bouwaanbesteding - Het schoolbestuur schaft het camerasysteem zelf aan, volgens de inkoop Eisen en het beheerprincipe - Alleen bij een één-op-één vervanging van een schoolgebouw op dezelfde locatie, waar eerder rechtmatig cameratoezicht plaatsvond, mag het cameratoezicht direct bij oplevering worden ingericht. De	2	Doordat het camerasysteem buiten het bestek om door het schoolbestuur zelf wordt aangeschaft en de rechtmatigheid, inclusief instemming van de (G)MR, vooraf wordt getoetst, behoudt het

#	Risico kort		Maatregelen		Toelichting restrisico
			ervaringen op de bestaande locatie kunnen worden gebruikt om cameraposities al in het ontwerp mee te nemen en voorbereidende voorzieningen, zoals bekabeling, kunnen in het bestek worden opgenomen. Actualiseer in dat geval vóór ingebruikname het cameraoverzicht, toets per camera opnieuw aan doel, noodzaak en plaatsing en vraag instemming van de (G)MR. Bij andere nieuwbouw wordt het cameratoezicht niet direct bij oplevering ingericht, maar pas wanneer op de nieuwe locatie een aanleiding is vastgesteld (incidenthistorie of aantoonbaar dreigend gevaar)		schoolbestuur de regie over de keuze van het systeem, het beheer en de rechtmatigheid van het cameratoezicht

9. Deel E: MODEL lokale DPIA

Dit hoofdstuk is het model waarmee het schoolbestuur de lokale DPIA uitvoert op basis van de centrale DPIA in hoofdstuk 5 tot en met 8. Het schoolbestuur controleert de uitkomsten van de centrale DPIA voor de eigen situatie, vult aanvullende risico's en maatregelen in en legt het advies van de FG, de raadpleging van betrokkenen, de conclusie en het besluit van het bestuur vast. De invulling gebeurt met behulp van het instructieblad (Bijlage 2).

! Volg instructie: 1. Model lokale DPIA op instructieblad

Lokale Management Samenvatting

! Volg instructie: 2. Lokale Managementsamenvatting op instructieblad

[Naam schoolbestuur] heeft in de periode [maand-jaar tot maand-jaar] een lokale DPIA uitgevoerd op het cameratoezicht op [aantal] [locatie/locaties]. De lokale DPIA bouwt voort op de centrale DPIA van SIVON (hoofdstuk 5 tot en met 8).

Conclusie centrale DPIA

Zonder maatregelen houdt cameratoezicht een hoog risico in voor de rechten en vrijheden van betrokkenen. Als alle maatregelen uit de centrale DPIA zijn doorgevoerd en geborgd, is het restrisico voor alle geïdentificeerde risico's laag of zeer laag. De risicogebieden zijn samengevat in hoofdstuk 2 van de centrale DPIA.

Lokale afwijkingen

De lokale situatie wijkt [niet/op de volgende onderdelen] af van de centrale DPIA: [onderdeel en korte toelichting WAT afwijkt en WAAROM]. Daarnaast [zijn geen/zijn de volgende] aanvullende lokale risico's vastgesteld: [L-1 ..., L-2 ...].

Technische beperkingen van het camerasysteem

Het camerasysteem voldoet [aan alle technische eisen uit deze DPIA/ niet aan de volgende technische eisen]:

- [eis] – [hoe het schoolbestuur hiermee omgaat, bijvoorbeeld de functie of camera niet gebruiken of het camerasysteem vervangen, met planning]
- [kopieer bovenstaande bij meerdere eisen waar niet aan voldaan kan worden]

Stand van de maatregelen

Van de [X] maatregelen uit de centrale en lokale DPIA zijn er [X] reeds uitgevoerd en staan er [X] nog open. De belangrijkste openstaande maatregelen zijn:

- [maatregel – termijn]

De volledige lijst staat in het verbeterplan (D.1 en L.3).

Advies FG en raadpleging betrokkenen

De FG adviseert [kern van het advies]. De betrokkenen zijn [geraadpleegd/ geïnformeerd] via [de (G)MR/ de leerlingenraad/ ...].

Uitkomst

Er is [wel/ geen] voorafgaande raadpleging van de Autoriteit Persoonsgegevens nodig.

A. Uitvoering lokale DPIA

! Volg instructie: 3. Uitvoering lokale DPIA op instructieblad

Binnen [naam schoolbestuur] is op basis van de door SIVON uitgevoerde centrale DPIA op cameratoezicht een lokale DPIA uitgevoerd in de periode [maand(-jaar) tot maand-jaar].

Hierbij [is/zijn] de volgende [locatie/locaties] in de beoordeling meegenomen:

- [Locatie A]
- [Locatie]

Bij de beoordeling in deze lokale DPIA zijn betrokken:

- [naam – (privacy officer)]
- [naam – (proceseigenaar)]
- [naam – (systeemeigenaar)]
- [naam – (lokale kerngebruiker)]
- [naam – (locatiedirecteur)]
- [naam – (FG)]
- [naam – (leverancier/externe onderhoudspartij)]
- [naam – (vertegenwoordiging betrokkenen)]
- [naam – (overig)]

B. Overwegingen centrale DPIA, lokaal maken

! Volg instructie: 4. Overwegingen centrale DPIA op instructieblad

Bij de uitvoering van de lokale DPIA, zijn de volgende onderdelen van de centrale DPIA overwogen en in de lokale DPIA bevestigd, aangevuld en/of onderbouwd tegengesproken.

Deel A: Gegevensverwerkingsanalyse

! Volg instructie: 5. Gegevensverwerkingsanalyse op instructieblad

1. Beschrijving gegevensverwerkende proces**1. Vastlegging**

Per locatie zijn de volgende systemen in gebruik:

#	Locatie	Installateur	Merk & type camera	Merk en type recorder	Opnamemodus (meerdere opties mogelijk)
1	[A]	[B]	[C – D]	[E – F]	[Continu/ Beweging/ Volgens tijdschema]

2					
3					

2. Opslag

Per locatie is de wijze van opslag:

#	Locatie	Opslag	Online bereikbaar	MFA ingesteld	Gescheiden netwerk
1	[A]	[Lokaal/ Cloud]	[Ja/ Nee]	[Ja/ Nee/ Niet mogelijk]	[Fysiek/ Logisch/ Nee]
2					
3					

De technische ruimte(s) waarin de componenten van het camerasysteem (recorder, switches e.d.) zich bevinden zijn toegankelijk voor de:

- [systeemeigenaar]
- [overige bevoegde medewerkers....]

3. Toegang en raadpleging

Per locatie is de wijze van toegang en raadplegen:

#	Locatie	Raadpleging mogelijk via	Live meekijken mogelijk	Monitor zichtbaar voor derden	Recorder & Monitor in afgesloten ruimte
1	[A]	[Recorder/ Netwerk/ Laptop/ (mobiele) App]	[Ja/ Nee]	[Ja/ Nee/ N.v.t.]	[Ja/ Nee]
2					
3					

5. Verwijdering en bewaartermijnen

Beelden die in het kader van een incident worden bewaard, blijven bewaard totdat het incident is afgehandeld of de beelden zijn overgedragen aan politie of justitie, waarna zij zo spoedig mogelijk en uiterlijk binnen drie weken worden verwijderd door [Rol X]. Beelden die buiten het camerasysteem zijn opgeslagen, worden na afhandeling van het incident eveneens zo spoedig mogelijk en uiterlijk binnen drie weken verwijderd door [Rol Y].

6. Beheer en onderhoud

Het camerasysteem wordt [gezamenlijk] beheerd door [de systeemeigenaar/ externe onderhoudspartij], die ook verantwoordelijk is voor het doorvoeren van updates, upgrades en beveiligingspatches. Beveiligingsupdates worden [automatisch door het systeem toegepast/ minimaal eens per kwartaal handmatig gecontroleerd en toegepast door [de systeemeigenaar/ externe onderhoudspartij]].

De afspraken rondom de werkzaamheden die uitgevoerd worden door de onderhoudsverantwoordelijke en de frequentie ervan zijn [wel/niet] vastgelegd in een [Service Level Agreement (SLA)/ onderhoudscontract].

[In deze afspraken is [wel/geen] geheimhoudingsclausule opgenomen die de externe onderhoudspartij verbiedt beelden te bekijken, op te slaan of te delen, tenzij strikt noodzakelijk op verzoek van de proces- of systeemeigenaar.]

2. Persoonsgegevens

! Volg instructie: 6. Persoonsgegevens op instructieblad

De categorieën van betrokkenen en persoonsgegevens uit de centrale DPIA komen [wel/niet] volledig overeen met de lokale situatie.

[In onze lokale situatie wijkt de tabel op de volgende wijze af: [toelichting WAT afwijkt en WAAROM]]

3. Gegevensverwerkingen

! Volg instructie: 7. Gegevensverwerkingen op instructieblad

De gehanteerde levenscyclus van de verwerking is [Scenario A: lokale opslag/ Scenario B: cloudopslag/ een combinatie van beide, afhankelijk van locatie].

[Als een combinatie: geef per locatie aan welk scenario van toepassing is.]

4. Verwerkingsdoeleinden

! Volg instructie: 8. Verwerkingsdoeleinden op instructieblad

De doeleinden voor het gebruik van cameratoezicht uit de centrale DPIA komen [wel/niet] volledig overeen met de lokale situatie.

[In onze lokale situatie wijkt de tabel op de volgende wijze af: [toelichting WAT afwijkt en WAAROM]]

5. Betrokken partijen

! Volg instructie: 9. Betrokken partijen op instructieblad

De volgende partijen zijn betrokken bij de verwerking:

Naam partij	AVG-rol	Functie/taak	Betrokken persoonsgegevens	Verstrekker of ontvanger	De volgende personen hebben directe toegang tot deze persoonsgegevens
[Schoolbestuur]	Verwerkings verantwoordelijke	Beveiliging van personen en middelen	Beeldmateriaal, metadata/ logging, logboek-gegevens	Verstrekker	Medewerkers die zijn opgenomen in de autorisatiematrix

[Externe onderhoudspartij]	Verwerker, uitsluitend bij Structurele toegang	Onderhoud van het camera-systeem	Beeldmateriaal, metadata/ logging	Ontvanger	Door de installateur aangewezen technisch medewerkers die betrokken zijn bij onderhoud
[Cloudopslag leverancier]	Verwerker	Verzorgt de opslag van beeldmateriaal op een extern platform	Beeldmateriaal, metadata/ logging	Ontvanger	Technisch beheerders van de cloudleverancier, uitsluitend voor zover noodzakelijk voor de uitvoering van de overeenkomst

6. Belangen bij de gegevensverwerking

! Volg instructie: 10. Belangen bij de gegevensverwerking op instructieblad

De belangen van de gegevensverwerking uit de centrale DPIA komen [wel/niet] volledig overeen met de lokale situatie.

[In onze lokale situatie wijkt de tabel op de volgende wijze af: [toelichting WAT afwijkt en WAAROM]]

7. Verwerkingslocaties

! Volg instructie: 11. Verwerkingslocaties op instructieblad

De volgende verwerkingslocaties zijn van toepassing bij de verwerking:

Naam partij	Statutaire vestigingsplaats en land	Beknpte omschrijving taak/dienst waaruit blijkt welke informatie wordt verwerkt	Plaats/land van opslag en verwerking persoonsgegevens en doorgifte mechanisme indien buiten de EER
[Schoolbestuur]	[Stad – Land]	Lokale opslag en beheer van het cameratoezicht	[Land - Doorgiftemechanisme]
[Cloudopslag leverancier]	[Stad – Land]	Opslag van beeldmateriaal op een extern platform	[Land - Doorgiftemechanisme]

8. DTIA

! Volg instructie: 12. DTIA op instructieblad

De opslag vindt [wel/niet] plaats binnen de EER.

[Omdat de opslag plaatsvindt binnen de EER, hoeft er geen DTIA te worden uitgevoerd.

OF

Omdat de opslag plaatsvindt in een land met een adequaatheidsbesluit, hoeft er geen DTIA te worden uitgevoerd.

OF

Omdat de opslag plaatsvindt in een land buiten de EER zonder adequaatheidsbesluit en de doorgifte is afgedekt met SCC's, moet er los van deze DPIA een DTIA worden uitgevoerd. Deze DTIA is geen onderdeel van deze DPIA maar een zelfstandig document met de naam: "DTIA".]

11. Bewaartermijnen

! Volg instructie: 13. Bewaartermijnen op instructieblad

De reguliere bewaartermijn van ons camerasysteem is [drie/ vier] weken en deze is technisch ingesteld in het systeem.

[Bij vier weken: de verlenging van drie naar vier weken is noodzakelijk om de volgende reden: motivering]

Tijdens de zomervakantie hanteren wij een bewaartermijn van [X] weken (maximaal zes weken) en deze is technisch ingesteld in het systeem.

Na de zomervakantie valt de bewaartermijn terug naar de reguliere bewaartermijn: [automatisch door het camerasysteem/ handmatig door de systeemeigenaar na de eerste schooldag en uiterlijk op de tweede schooldag, vastgelegd in het logboek wijzigingen camera-instellingen].

Deel B: Beoordeling rechtmatigheid gegevensverwerkingen**12. Rechtsgrond**

! Volg instructie: 14. Rechtsgrond op instructieblad

De gebruikte rechtsgronden voor het cameratoezicht zijn:

- Algemeen belang (art. 6 lid 1 sub e AVG): voor de doeleinden 1 tot en met 5 en voor verstrekking van incidentgegevens op eigen besluit (doeleinde 7), ter uitvoering van de zorgplicht voor de veiligheid op school (art. 4c WPO / art. 3.40 WVO 2020).
- Wettelijke verplichting (art. 6 lid 1 sub c AVG): voor de zorg voor de veiligheid en gezondheid van medewerkers (doeleinden 1 en 5, art. 3 Arbowet), voor de beveiliging, controle en verantwoording van de verwerking (doeleinde 6, art. 5 lid 2, 24 en 32 AVG) en voor verstrekking op een vordering van politie of justitie (doeleinde 7, art. 126nd en 126nda Sv).

14. Doelbinding

! Volg instructie: 15. Doelbinding op instructieblad

De doelbinding uit de centrale DPIA komt [wel/niet] volledig overeen met de lokale situatie.

[In onze lokale situatie wijkt de doelbinding op de volgende wijze af: [toelichting WAT afwijkt en WAAROM]]

16. Noodzakelijkheid

! Volg instructie: 16. Noodzakelijkheid op instructieblad

De noodzakelijkheid uit de centrale DPIA komt [wel/niet] volledig overeen met de lokale situatie.

[In onze lokale situatie wijkt de noodzakelijkheid op de volgende wijze af: [toelichting WAT afwijkt en WAAROM]]

17. Proportionaliteit en subsidiariteit

! Volg instructie: 17. Proportionaliteit en subsidiariteit op instructieblad

Het cameratoezicht [is/wordt] ingericht volgens de randvoorwaarden die in deze DPIA zijn vastgesteld.

Het cameratoezicht is [wel/niet] een op zichzelf staande maatregel voor de realisatie van de vastgestelde doeleinden. De volgende aanvullende maatregelen zijn nog altijd actief en [zijn/worden] vastgelegd in het cameraoverzicht en het reglement cameratoezicht:

- [Surveillance door personeel of beveiligingspersoneel op het schoolterrein.
- Een operationeel alarmsysteem voor inbraak- en branddetectie.
- Het afsluiten van gebieden of terreinen buiten Schooltijd.
- Bebording en posters als preventieve communicatie richting bezoekers en leerlingen.
- Bewustwordingsacties en gesprekken met leerlingen over veiligheid en gedrag.
- Aansluiting bij een wijkapp ter ondersteuning van buurttoezicht. *Let op: de privacyaspecten van de gebruikte wijkapp zijn niet in deze DPIA getoetst, het schoolbestuur dient hiervoor een separate beoordeling uit te voeren.*
- Buurtpreventie in samenwerking met omwonenden.
- Overleg met gemeente, politie en/of wijkagent over veiligheid en toezicht rondom de schoollocatie.
- Bij nieuwbouw: aandacht voor het ontwerp zodat onoverzichtelijke hoeken worden vermeden.]

Per camera [is/wordt] beoordeeld, mede op basis van het effect van de getroffen maatregelen, of het doeleinde zonder cameratoezicht kan worden bereikt. De uitkomst [is/wordt] vastgelegd in het cameraoverzicht.

18. Rechten van de betrokkenen

! Volg instructie: 18. Rechten van betrokkenen op instructieblad

De afhandeling en technische mogelijkheden voor de rechten van de betrokkenen uit de centrale DPIA komen [wel/niet] volledig overeen met de lokale situatie.

[In onze lokale situatie wijkt dit op de volgende wijze af: [toelichting WAT afwijkt en WAAROM]]

19. Beoordeling verwerkersovereenkomst

! Volg instructie: 19. Beoordeling verwerkersovereenkomst op instructieblad

Er is [wel/geen] sprake van cloudopslag van de camerabeelden.

[Er is [nog geen/een] verwerkersovereenkomst met deze cloudopslag leverancier afgesloten.]

Er is [wel/geen] sprake van online beheer- of viewsoftware (niet lokaal geïnstalleerd).

[Er is [nog geen/een] verwerkersovereenkomst met deze leverancier afgesloten.]

Er is [wel/geen] sprake van Structurele toegang tot het camerasysteem door de externe onderhoudspartij.

[Er is [nog geen/een] verwerkersovereenkomst met deze externe onderhoudspartij afgesloten, inclusief geheimhoudingsclausule.]

Deel C: Beschrijving en beoordeling risico's voor de betrokkenen

20. Risico's

! Volg instructie: 20. Risico's op instructieblad

Alle in de DPIA beschreven risico's zijn van toepassing op de lokale situatie. [, behalve:

- Risico A, omdat X
- Risico B, omdat Y
- Risico C, omdat Z.....]

Deel D: Beschrijving voorgenomen maatregelen

21. Maatregelen

! Volg instructie: 21. Maatregelen op instructieblad

Na uitgebreide analyse van ons camerasysteem en de processen daaromheen, door middel van het beantwoorden van de "Vragenlijst DPIA Cameratoezicht" (ook ingevuld als **bijlage 3** opgenomen in deze DPIA), is in onderstaande tabel opgenomen welke maatregelen al zijn genomen en welke maatregelen nog genomen dienen te worden. Als er nog maatregelen genomen dienen te worden dan wordt hier ook de actiehouders, actiedatum en eventuele opmerking over de status/nog te nemen stappen opgenomen. Deze tabel is daarmee naast een momentopname tijdens de uitvoer van de DPIA ook direct ons interne verbeterplan voor het doorvoeren van alle nog te nemen beheersmaatregelen.

Alle in het verbeterplan opgenomen maatregelen worden beleidsmatig in het reglement cameratoezicht opgenomen.

D.1 Verbeterplan centraal

Risico	Status	Maatregel	Actiehouders ¹⁹	Actie datum	Opmerking
Technisch					
Opname					

¹⁹ EV = Eindverantwoordelijke
UV = Uitvoerende

Risico	Status	Maatregel	Actiehouder ¹⁹	Actie datum	Opmerking
T-1.1	☐	Vaste camera's gericht op de openbare ruimte buiten de eigendomsgrens worden bijgesteld of softwarematig (zwart/wazig) afgeschermd. Alleen de systeemeigenaar kan deze instelling aanpassen. Wijzigingen worden gelogd en vastgelegd in het logboek wijzigingen camera-instellingen	EV: - UV: -		
T-1.2	☐	Beweegbare camera's worden softwarematig vastgezet zodat de openbare ruimte buiten de eigendomsgrens niet in beeld kan komen. Alleen de systeemeigenaar kan deze instelling aanpassen. Wijzigingen worden gelogd en vastgelegd in het logboek wijzigingen camera-instellingen	EV: - UV: -		
T-2	☐	Geluidsopname wordt uitgeschakeld in het camerasysteem. Alleen de systeemeigenaar kan deze instelling aanpassen. Wijzigingen worden gelogd en vastgelegd in het logboek wijzigingen camera-instellingen	EV: - UV: -		
T-3	☐	AI-technieken bij opname (zoals gezichtsherkenning of gedragsanalyse) worden uitgeschakeld. Alleen de systeemeigenaar kan deze instelling aanpassen. Wijzigingen worden gelogd en vastgelegd in het logboek wijzigingen camera-instellingen <i>Opmerking: deze maatregel betreft geen beoordeling van AI-camerasystemen als zodanig - die vallen buiten de scope van deze DPIA - maar een controlemaatregel voor het geval een regulier camerasysteem ongevraagd over AI-gestuurde opnametechnieken beschikt</i>	EV: - UV: -		
T-4	☐	Bij de aanschaf, installatie en configuratie van het camerasysteem worden uitsluitend de functies ingeschakeld die strikt noodzakelijk zijn voor de vastgestelde verwerkingsdoeleinden per camera (privacy by default, art. 25 lid 2 AVG). Aanwezige maar niet-noodzakelijke functies, zoals onbeperkte PTZ-beweging, optische zoom, geluidsopname, analytische functies en draadloze verzending, worden technisch uitgeschakeld of geblokkeerd. Alleen de systeemeigenaar kan dergelijke functies activeren. Elke activering wordt gelogd, vastgelegd in het logboek wijzigingen camera-instellingen en vereist een	EV: - UV: -		

Risico	Status	Maatregel	Actiehouder ¹⁹	Actie datum	Opmerking
		aantoonbare relatie met een vastgesteld verwerkingsdoel			
<i>Opslag & beveiliging</i>					
T-5	☐	Sluit een verwerkersovereenkomst met de cloudopslag leverancier en met de leverancier van online beheer- of viewsoftware. Verifieer dat de leverancier voldoende technische en organisatorische maatregelen heeft genomen en opslaat of verwerkt binnen de EER, een land met adequaatheidsbesluit, dan wel beschikt over een passende doorgifte-waARBorg (bijv. SCC) inclusief DTIA OF Stap over op goed ingerichte lokale opslag met lokaal geïnstalleerde beheer- en viewsoftware. Het schoolbestuur verwerkt de beelden dan volledig binnen de eigen organisatie en een verwerkersovereenkomst is dan niet vereist	EV: - UV: -		
T-6.1	☐	Het camerasysteem is aangesloten op een compleet fysiek of logisch gescheiden netwerk. Bij een logisch gescheiden netwerk (VLAN) is een firewall actief tussen het camerasegment en de overige netwerksegmenten, zodat alleen strikt noodzakelijk verkeer is toegestaan. Bij een volledig fysiek gescheiden netwerk zonder internetverbinding is deze maatregel niet van toepassing	EV: - UV: -		
T-6.2	☐	Waar het camerasysteem online bereikbaar is, is altijd een firewall aanwezig die inkomend en uitgaand verkeer beperkt tot wat strikt noodzakelijk is voor het beoogde gebruik. Waar het camerasysteem is verbonden met bredere IT-infrastructuur of online bereikbaar is, zijn aanvullende beveiligingsmaatregelen getroffen, zoals netwerkinbraakdetectie (IDS/IPS) of gelijkwaardige monitoring. Bij een volledig fysiek gescheiden netwerk zonder internetverbinding is deze maatregel niet van toepassing	EV: - UV: -		
T-6.3	☐	Bij online of remote toegang tot het camerasysteem is MFA verplicht ingesteld. Bij uitsluitend lokale toegang is MFA ingesteld waar het systeem dit ondersteunt.	EV: - UV: -		

Risico	Status	Maatregel	Actiehouder ¹⁹	Actie datum	Opmerking
		Is dat niet het geval, dan worden wachtwoorden of wachzinnen van minimaal 15 tekens gebruikt. Standaardwachtwoorden van de fabrikant zijn bij ingebruikname gewijzigd. Er gelden geen verplichte samenstellingsregels en geen periodieke wijziging, een wachtwoord wordt direct gewijzigd bij (vermoeden van) compromittering. Veelgebruikte of eerder gelekte wachtwoorden en hergebruik van wachtwoorden zijn niet toegestaan			
T-6.4	☐	Een sessie waarin live wordt meegekeken, beelden worden teruggekeken of camera-instellingen worden gewijzigd, vergrendelt automatisch na maximaal vijf minuten inactiviteit, waarna opnieuw inloggen vereist is. Bij live kijken blijven de beelden daarna wel zichtbaar			
T-6.5	☐	Opgeslagen beeldmateriaal is versleuteld (versleuteling in rust). Ondersteunt een bestaande recorder dit aantoonbaar niet, dan staat de recorder in een afgesloten ruimte, wordt dit vastgelegd in de lokale DPIA en is versleuteling in rust een eis bij vervanging van het systeem	EV: - UV: -		
T-6.6	☐	Beelden worden versleuteld getransporteerd bij overdracht via een logisch gescheiden netwerk (VLAN), een cloudverbinding of een internetverbinding. Bij een volledig fysiek gescheiden netwerk zonder internetverbinding is deze maatregel niet van toepassing	EV: - UV: -		
T-6.7	☐	Het systeem past securityupdates automatisch toe OF Securityupdates worden minimaal eens per kwartaal handmatig gecontroleerd en toegepast	EV: - UV: -		
Organisatorisch					
Beleid & rechten					
O-1.1	☐	Stel duidelijke doeleinden vast voor het gebruik van cameratoezicht. De doeleinden (1) tot en met (4) worden per camera vastgesteld in het cameraoverzicht, de doeleinden (5) tot en met (7) gelden voor het cameratoezicht als geheel:	EV: - UV: -		

Risico	Status	Maatregel	Actiehouder ¹⁹	Actie datum	Opmerking
		(1) De bescherming van de veiligheid en gezondheid van leerlingen, medewerkers en bezoekers. (2) De beveiliging van de toegang tot gebouwen en terreinen, waaronder mede begrepen het weren van onbevoegden. (3) Het voorkomen en registreren van overlast en strafbare feiten zoals vandalisme, diefstal en inbraak. (4) De bewaking van zaken die zich in de gebouwen of op de terreinen bevinden. (5) Het vastleggen van incidenten ten aanzien van de onder (1) tot en met (4) genoemde doeleinden. (6) Beveiliging, controle en ook verantwoording van de verwerking door middel van systeemlogging (audittrail) en logboeken (logboek wijzigingen camera-instellingen, logboek reglement afwijkingen en logboek beeldgebruik). (7) Verstrekking van incidentgegevens aan derden, op eigen besluit of op vordering (bijvoorbeeld aan politie of justitie)			
O-1.2	☐	Ieder jaar worden de doeleinden van alle camera's in het cameraoverzicht opnieuw getoetst, inclusief de actualiteit van de voor iedere camera vastgelegde aanleiding	EV: - UV: -		
O-1.3	☐	Kan er geen toelaatbaar doel (meer) worden vastgesteld voor een camera, dan wordt die camera verwijderd of buiten gebruik gesteld	EV: - UV: -		
O-2	☐	Het camerasysteem is ingesteld op een automatische bewaartermijn van standaard drie weken, die met een gemotiveerde reden kan worden verlengd tot maximaal vier weken. Tijdens de zomervakantie geldt een maximale bewaartermijn van zes weken. Na de zomervakantie valt de bewaartermijn terug naar de reguliere bewaartermijn. Ondersteunt het camerasysteem dit, dan gebeurt dit automatisch. Is dat niet het geval, dan zet de systeemeigenaar de bewaartermijn na de eerste schooldag en uiterlijk op de tweede schooldag handmatig terug en legt deze wijziging vast in het logboek wijzigingen camera-instellingen. Beelden worden na	EV: - UV: -		

Risico	Status	Maatregel	Actiehouder ¹⁹	Actie datum	Opmerking
		afloop van de ingestelde termijn automatisch overschreven			
O-3.1	☐	Voor iedere camera is in het cameraoverzicht een aanleiding vastgelegd. Hoe zwaar die aanleiding moet zijn, hangt af van het moment waarop de camera opneemt. Camera's die uitsluitend zijn ingezet voor de doeleinden 3 en/of 4 nemen alleen buiten de Gebruikstijden van de locatie op, dus niet tijdens Schooltijd en niet tijdens verhuur. Buiten de Gebruikstijden zijn er op het eigen terrein geen personen aanwezig die daar mogen zijn, zoals leerlingen, medewerkers of gebruikers van huurders. De inbreuk is daardoor beperkt en als aanleiding volstaan incidenten op of rond de locatie, of een aantoonbaar dreigend gevaar, zoals de aanwezigheid van kostbare apparatuur. Camera's die (mede) zijn ingezet voor doeleinde 1 en/of 2 mogen ook tijdens de Gebruikstijden opnemen. Omdat leerlingen, medewerkers en bezoekers dan in beeld komen, geldt voor deze camera's een zwaardere eis: het doeleinde is per camera onderbouwd met daadwerkelijke voorvallen of een aantoonbaar dreigend gevaar op die plek. Een voorval op één plek rechtvaardigt alleen een camera op die plek	EV: - UV: -		
O-3.2	☐	In leslokalen en gymzalen wordt nooit gefilmd terwijl de ruimte in gebruik is door personen die daar mogen zijn, zoals leerlingen, medewerkers en gebruikers van huurders. Buiten de Gebruikstijden is cameratoezicht daar uitsluitend toegestaan in praktijklokalen met kostbare apparatuur en in gymzalen, ter beveiliging van de ruimte en de daarin aanwezige eigendommen			
O-3.3	☐	Leg per camera het tijdschema vast in het cameraoverzicht, rekening houdend met de Gebruikstijden van de locatie. Het camerasysteem dwingt dit tijdschema per camera technisch af. Handmatig aan- en uitzetten is geen toegestaan alternatief. Kan het tijdschema niet technisch worden ingericht, dan is cameratoezicht niet toegestaan met een camera die uitsluitend is ingezet voor de doeleinden 3 en/of 4. Wijzigingen in het tijdschema worden vastgelegd in het logboek wijzigingen camera-instellingen			

Risico	Status	Maatregel	Actiehouder ¹⁹	Actie datum	Opmerking
O-3.4	☐	Cameratoezicht in toiletten, kleedkamers of andere ruimtes met een fundamenteel privacykarakter is, ongeacht het doel, nooit aanvaardbaar	EV: - UV: -		
O-3.5	☐	Cameratoezicht om leerlingen en/of medewerkers te beoordelen is niet toegestaan. Bij constatering hiervan worden camera's per direct buiten gebruik gesteld of verwijderd	EV: - UV: -		
O-3.6	☐	Stel per camera een overzicht op van andere preventieve maatregelen die de organisatie heeft getroffen om hetzelfde doel te bereiken. Beoordeel per camera, mede op basis van het effect dat deze maatregelen hebben gehad, of het doel zonder cameratoezicht kan worden bereikt. Leg het overzicht en de uitkomst van de beoordeling vast in het cameraoverzicht en herhaal de beoordeling bij de jaarlijkse toets van de doeleinden	EV: - UV: -		
O-3.7	☐	Ontbreken andere preventieve maatregelen volledig, dan worden deze opnieuw vastgesteld en ingevoerd voordat het cameratoezicht wordt voortgezet	EV: - UV: -		
O-3.8	☐	Laat bij de initiële plaatsing van camera's of aanvullende cameraplaatsing deze beoordelen door de betrokkenen (m.n. de leerlingen) op o.a. een onaanvaardbaar chilling effect bij leerlingen (PO via de oudergeleding van de MR, VO via de leerlingenraad). Leg de uitkomst vast in het cameraoverzicht	EV: - UV: -		
O-3.9	☐	Raadpleeg leerlingen bij de vaststelling of wijziging van het reglement cameratoezicht, voor het PO via de oudergeleding van de MR en voor het VO via de leerlingenraad. Leg de uitkomst van de consultatie schriftelijk vast	EV: - UV: -		
O-4.1	☐	Zorg ervoor dat camera's fysiek zijn bevestigd op een vaste locatie, zodanig dat verplaatsing niet mogelijk is zonder (speciaal) gereedschap	EV: - UV: -		
O-4.2	☐	Een camera wordt alleen verplaatst of anders gericht na een gezamenlijk besluit van de proceseigenaar en de systeemeigenaar, op advies van de privacy officer. Vóór ingebruikname op de nieuwe positie wordt de camera opnieuw getoetst aan doel, noodzaak en plaatsing en wordt zo	EV: - UV: -		

Risico	Status	Maatregel	Actiehouder ¹⁹	Actie datum	Opmerking
		nodig de bebording aangepast. De verplaatsing en de uitkomst van de toets worden vastgelegd in het cameraoverzicht			
O-5.1	☐	Laag 1: Zorg ervoor dat er duidelijke bebording* is bij iedere camera waar betrokkenen zonder een barrière toegang hebben tot de locatie (bijvoorbeeld een vrij toegankelijk looppad langs de school), bij ieder toegangspunt in een hekwerk, op iedere buitendeur bij het naar binnen treden van de locatie (als er ook cameratoezicht binnen is) en bij iedere separaat in beeld gebrachte ruimte binnen het gebouw (kantine, aula, trappenhuis, nooduitgang, etc.) * cameraborden met cameralogo, cameratoezicht, tijdsperiode opname, identiteit verwerkingsverantwoordelijke, doel, bewaartermijn, privacygevoelige informatie, bijvoorbeeld: live monitoring, verstrekking aan derden en verwijzing naar tweede laag - zie bijlage 5 voor voorbeeld	EV: - UV: -		
O-5.2	☐	Laag 2: De verwerking (beeldmateriaal t.b.v. bewakingsdoeleinden) is opgenomen in de privacyverklaring voor leerlingen/ouders en medewerkers en is eenvoudig vindbaar. Voor leerlingen en ouders minimaal op de school- en/of bestuurswebsite, met maximaal 1 keer doorklikken vanaf de hoofdpagina, en voor medewerkers daarnaast minimaal op de interne communicatieportal, met maximaal 1 keer doorklikken	EV: - UV: -		
O-5.3	☐	Het "reglement cameratoezicht" van de organisatie is voor alle betrokkenen eenvoudig vindbaar. Voor alle betrokkenen minimaal op de school- en/of bestuurswebsite, met maximaal 1 keer doorklikken vanaf de hoofdpagina	EV: - UV: -		
O-5.4	☐	Zorg bij aanvang van elk schooljaar voor leeftijdsadequate informatie over het cameratoezicht, afgestemd op de leeftijdsfase van leerlingen. Voor het PO in eenvoudige en waar mogelijk visuele vorm, voor het VO volledig inclusief uitleg over hun rechten. Documenteer de uitvoering hiervan	EV: - UV: -		
O-6.1	☐	Stel een procedure op voor het afhandelen van privacyrechtverzoeken (inzage, verwijdering, beperking en bezwaar)	EV: - UV:		

Risico	Status	Maatregel	Actiehouder ¹⁹	Actie datum	Opmerking
			-		
O-6.2	☐	Leg vast hoe wordt omgegaan met een verzoek dat niet bij het juiste contactpunt binnenkomt: intern doorsturen naar het contactpunt of de betrokkene verwijzen naar het contactpunt	EV: - UV: -		
O-6.3	☐	Wijs de proceseigenaar aan als verantwoordelijke voor tijdige afhandeling. Bij inzageverzoeken die betrekking hebben op beeldmateriaal reageert de proceseigenaar zo snel als redelijkerwijs mogelijk, gezien de korte bewaartermijnen en de kans dat het betreffende beeldmateriaal anders niet meer beschikbaar is	EV: - UV: -		
O-6.4	☐	Informeer betrokkenen in de privacyverklaring over het bestaan van deze rechten en de wijze waarop zij een verzoek kunnen indienen	EV: - UV: -		
O-6.5	☐	Bij inzageverzoeken mogen camerabeelden van de betrokkene de privacy van andere betrokkenen niet schaden (dus niet in beeld), neem dit op in de procedure	EV: - UV: -		
O-7	☐	Verifieer dat het camerasysteem expliciet is opgenomen in het bestaande datalekresponsbeleid van het schoolbestuur. Voeg indien nodig een beknopte notitie toe die beschrijft hoe bij een incident met het camerasysteem wordt omgegaan met het veiligstellen van beeldmateriaal, gezien de korte bewaartermijnen en automatische overschrijving. Deze notitie hoeft geen zelfstandig document te zijn maar kan als aanvulling worden opgenomen in het bestaande beleid of het reglement cameratoezicht	EV: - UV: -		
Toegang & gebruik					
O-8.1	☐	Stel bovenschools een autorisatiematrix vast die per rol vastlegt welke acties binnen het camerasysteem zijn toegestaan	EV: - UV: -		
O-8.2	☐	Iedere gebruiker heeft een persoonlijk account, accounts worden niet gedeeld	EV: - UV: -		

Risico	Status	Maatregel	Actiehouder ¹⁹	Actie datum	Opmerking
O-9.1	☐	Stel vast op welke manier beelden teruggekeken mogen worden (bijv. alleen op de locatie, alleen via een door het schoolbestuur beheerd apparaat)	EV: - UV: -		
O-9.2	☐	Het systeem is zo ingericht dat altijd opnieuw ingelogd moet worden voordat beelden teruggekeken kunnen worden, ook als er op dat moment al live beelden worden bekeken	EV: - UV: -		
O-9.3	☐	Beelden worden door minimaal twee bevoegde collega's tegelijk bekeken. Stel vast welke combinaties van collega's dit mogen doen en neem dit op in de autorisatiematrix. Een medewerker van de onderhoudspartij telt niet mee voor dit vier-ogenprincipe en bekijkt beelden uitsluitend bij storingen of onderhoud. Alleen bij een calamiteit buiten Schooltijd mag individueel worden teruggekeken, volgens de richtlijnen voor calamiteiten, ook dan wordt het terugkijken vastgelegd in het logboek beeldgebruik	EV: - UV: -		
O-9.4	☐	Het terugkijken van beelden wordt geregistreerd in het logboek beeldgebruik met minimaal: datum/tijdstip, tijdspad van de bekeken beelden, welke camera, reden en door wie of welke twee personen	EV: - UV: -		
O-9.5	☐	Stel richtlijnen op voor calamiteiten buiten Schooltijd, waarbij individueel en zo nodig op afstand beelden teruggekeken mogen worden. Beperk dit tot calamiteiten (inbraak(poging), brandalarm, geweldsincident e.d.)	EV: - UV: -		
O-10	☐	Terugkijken van beelden is alleen toegestaan op momenten die voldoen aan de vastgestelde verwerkingsdoeleinden. Werk deze doeleinden uit in concrete, herkenbare voorbeeldsituaties	EV: - UV: -		
O-11	☐	Neem een expliciete verbodsbepaling op in het reglement cameratoezicht: medewerkers mogen nimmer camerabeelden (ongeacht of daar betrokkenen op staan of niet) buiten het camerasysteem vastleggen (bijv. via mobiel het scherm filmen of exporteren naar een privéapparaat)	EV: - UV: -		
O-12.1	☐	Stel richtlijnen op voor live kijken: alleen toegestaan in het kader van het voorkomen	EV: -		

Risico	Status	Maatregel	Actiehouder ¹⁹	Actie datum	Opmerking
		van en direct handelen bij incidenten. Dit moet in de praktijk ook daadwerkelijk plaatsvinden	UV: -		
O-12.2	☐	Live beelden mogen alleen worden bekeken door medewerkers die in de autorisatiematrix zijn opgenomen	EV: - UV: -		
O-12.3	☐	Beeldschermen waarop live beelden worden getoond, zijn zo opgesteld dat alleen medewerkers die in de autorisatiematrix zijn opgenomen de beelden kunnen zien en anderen niet kunnen meekijken, ook niet van buiten de ruimte, bijvoorbeeld door een raam	EV: - UV: -		
O-13.1	☐	Toegang op afstand tot het camerasysteem is uitsluitend mogelijk voor accounteigenaren die daartoe in de autorisatiematrix zijn opgenomen, de systeemeigenaar implementeert dit technisch	EV: - UV: -		
O-13.2	☐	Accounts voor toegang op afstand hebben uitsluitend kijkrechten: exporteren en downloaden zijn technisch uitgeschakeld en de app of webinterface slaat geen beelden op het apparaat op	EV: - UV: -		
O-13.3	☐	Beelden mogen online alleen worden bekeken op door de organisatie beheerde apparaten, privéapparaten zijn niet toegestaan. Online toegang is beveiligd met MFA	EV: - UV: -		
O-13.4	☐	Online toegang vergroot het aanvalsoppervlak: de infrastructuurbeveiliging is hierop afgestemd en de onderhoudsfrequentie van het camerasysteem is verhoogd	EV: - UV: -		
O-14.1	☐	Stel richtlijnen op voor de situaties waarin beelden bewaard mogen worden	EV: - UV: -		
O-14.2	☐	Iedere beslissing om beelden te bewaren of bewaard beeldmateriaal te verwijderen wordt geregistreerd in het logboek beeldgebruik met minimaal: datum/tijdstip, tijdspad van de beelden, welke camera, reden, door welke twee personen het besluit is genomen en wanneer verwijdering heeft plaatsgevonden. Het logboek	EV: - UV: -		

Risico	Status	Maatregel	Actiehouder ¹⁹	Actie datum	Opmerking
		beeldgebruik is als bijlage bij het reglement opgenomen			
O-14.3	☐	Beelden worden bewaard binnen het camerasysteem zelf of op een extra beveiligde plek binnen de schoolbestuur kantoorautomatiseringsomgeving	EV: - UV: -		
O-14.4	☐	Stel een bewaartermijn vast voor bewaard beeldmateriaal	EV: - UV: -		
O-15.1	☐	Stel richtlijnen op voor situaties waarin inzage aan derden (iedereen buiten de autorisatiematrix) is toegestaan	EV: - UV: -		
O-15.2	☐	Iedere inzage aan derden wordt geregistreerd in het logboek beeldgebruik met minimaal: datum/tijdstip van inzage, tijdspad van de ingeziene beelden, welke camera, reden, door welke twee personen inzage is verleend, wie het besluit heeft genomen, aan wie inzage is verleend en hoe de ontvanger zich heeft geïdentificeerd	EV: - UV: -		
O-16.1	☐	Stel richtlijnen op voor situaties waarin beelden met derden (iedereen buiten de autorisatiematrix) gedeeld mogen worden	EV: - UV: -		
O-16.2	☐	Iedere deling wordt geregistreerd in het logboek beeldgebruik met minimaal: datum/tijdstip, tijdspad van de gedeelde beelden, welke camera, reden, door welke twee personen het delen is uitgevoerd, wie het besluit heeft genomen, met wie gedeeld is en hoe de ontvanger zich heeft geïdentificeerd	EV: - UV: -		
O-16.3	☐	Stel richtlijnen op voor de technische wijze van delen: bij voorkeur via een vanuit het camerasysteem gegenereerde beveiligde link, waarbij is in te stellen of de ontvanger de beelden alleen kan bekijken of ook kan downloaden en hoe lang de link geldig is, anders via een versleutelde drager of een beveiligde uploadvoorziening van de ontvanger. Delen via e-mail of openbaar toegankelijke platforms is niet toegestaan	EV: - UV: -		
O-16.4	☐	Stel een identificatieplicht vast voor de ontvanger van beelden	EV: - UV:		

Risico	Status	Maatregel	Actiehouder ¹⁹	Actie datum	Opmerking
			-		
<i>Beheer</i>					
O-17.1	☐	Onderhoudsafspraken (w.o. updates, upgrades, securitypatches) worden vastgelegd in een SLA met de onderhoudspartij en minimaal jaarlijks geëvalueerd door de proceseigenaar en systeemeigenaar OF De systeemeigenaar is zelf verantwoordelijk voor het onderhoud, hiervoor worden duidelijke interne afspraken gemaakt in een interne SLA	EV: - UV: -		
O-17.2	☐	In de SLA of interne onderhoudsafspraken zijn hersteltijden (RTO) opgenomen voor het geval het camerasysteem uitvalt door een technisch of fysiek incident. De proceseigenaar is op de hoogte van de herstelprocedure en kan bij uitval adequate tijdelijke compenserende maatregelen treffen (bijv. tijdelijk verhoogd fysiek toezicht of beveiligingsronden) totdat het systeem is hersteld	EV: - UV: -		
O-17.3	☐	In de SLA met een externe onderhoudspartij wordt een geheimhoudingsclausule opgenomen die het bekijken, opslaan en distribueren van camerabeelden verbiedt, tenzij strikt noodzakelijk op verzoek van de proceseigenaar/ systeemeigenaar	EV: - UV: -		
O-18.1	☐	Heeft de externe onderhoudspartij Structurele toegang tot het camerasysteem, sluit dan een verwerkersovereenkomst met deze partij	EV: - UV: -		
O-18.2	☐	Verifieer dat de onderhoudspartij voldoende technische en organisatorische maatregelen heeft genomen	EV: - UV: -		
O-19.1	☐	Technische componenten (recorder, switches) bevinden zich in een afgesloten technische ruimte. Als anderen dan de systeemeigenaar, proceseigenaar of geautoriseerde medewerkers toegang nodig hebben, bevinden de cameratoezicht componenten zich ook in een afgesloten patchkast die niet van de zijkant of achterkant te benaderen is	EV: - UV: -		

Risico	Status	Maatregel	Actiehouder ¹⁹	Actie datum	Opmerking
O-19.2	☐	De technische ruimte is bij voorkeur beveiligd met een elektronisch slot. Is dit niet het geval, dan is er een sleutelregistratie en wordt iedere toegang tot de ruimte geregistreerd op een inschrijflijs	EV: - UV: -		
O-19.3	☐	De ruimte van waaruit live beelden of beelden teruggekeken kunnen worden is afgesloten en alleen toegankelijk voor medewerkers in de autorisatiematrix	EV: - UV: -		
Governance					
<i>Inrichting & beheer</i>					
G-1.1	☐	Er is een bestuursbrede proceseigenaar (rol) aangesteld voor het cameratoezicht	EV: - UV: -		
G-1.2	☐	Er is een bestuursbrede systeemeigenaar (rol) aangesteld voor het cameratoezicht	EV: - UV: -		
G-1.3	☐	Taken en verantwoordelijkheden van beide rollen zijn uitgewerkt in het reglement cameratoezicht en zijn bekend bij de rolhouders	EV: - UV: -		
G-1.4	☐	Technisch beheer van het/de camerasyste(e)m(en) is centraal geborgd bij de systeemeigenaar op bestuursniveau	EV: - UV: -		
G-1.5	☐	De proceseigenaar en de systeemeigenaar zijn, op advies van de privacy officer, gezamenlijk verantwoordelijk voor het beoordelen en goedkeuren van iedere aanschaf van camerasystemen	EV: - UV: -		
G-2.1	☐	Sluit aan bij het bestaande centrale inkoopproces van het schoolbestuur. Is een dergelijk proces er niet, dan verloopt de aanschaf van camerasystemen altijd via de proceseigenaar, die hiervoor zelf een proces inricht	EV: - UV: -		
G-2.2	☐	De aanschaf is erop gericht dat binnen het schoolbestuur, zolang dit technisch mogelijk is, met één type camerasysteem wordt gewerkt, dat bij een nieuwe generatie kan worden geüpdatet in plaats van vervangen. Waar dit financieel verstandig is, wordt met één onderhoudspartij gewerkt, met	EV: - UV: -		

Risico	Status	Maatregel	Actiehouder ¹⁹	Actie datum	Opmerking
		aandacht voor het voorkomen van een te grote afhankelijkheid van één leverancier (beheerprincipe)			
G-3	☐	Stel als inkoop eis dat het camerasysteem kan voldoen aan de in deze DPIA vastgestelde technische vereisten. Denk daarbij aan: het kunnen uitschakelen van niet-noodzakelijke opnamefuncties zoals geluid, AI-technieken en overige niet-noodzakelijke functies, softwarematige afscherming van delen van het beeld, netwerk- en toegangsbeveiliging (netwerksegmentatie, MFA, hernieuwd inloggen bij terugkijken, automatische sessievergrendeling), versleuteling van opgeslagen beelden en van het transport, een instelbare bewaartermijn met automatische overschrijving, bij voorkeur met de mogelijkheid om de verlengde termijn voor de zomervakantie vooraf in te plannen, zodat de terugval naar de reguliere termijn automatisch plaatsvindt, een per camera instelbaar tijdschema dat het camerasysteem zonder handmatige tussenkomst afdwingt, en logging/audittrail. Neem bij voorkeur ook privacy-by-design elementen mee, zoals ondersteuning bij het bijhouden van de logboeken (het uitvragen van de benodigde logboek informatie bij terugkijken en bij het wijzigen van instellingen), rolgebaseerde toegangscontrole aansluitend op de autorisatiematrix en de mogelijkheid om beelden te vervagen of uit te snijden bij verstrekking aan betrokkenen. Werk deze inkoop eisen uit in een concrete, schoolbestuur-eigen checklist	EV: - UV: -		
G-4.1	☐	Stel een reglement cameratoezicht op dat voldoet aan de AVG-minimumvereisten, alle elementen uit deze DPIA bevat en een revisiecyclus van twee jaar kent	EV: - UV: -		
G-4.2	☐	Het reglement cameratoezicht is goedgekeurd door de (G)MR	EV: - UV: -		
G-4.3	☐	De proceseigenaar zorgt dat het reglement bekend is bij alle stakeholders en controleert steekproefsgewijs het gebruik van het camerasysteem	EV: - UV: -		

Risico	Status	Maatregel	Actiehouder ¹⁹	Actie datum	Opmerking
G-4.4	☐	Afwijkingen van het reglement zijn uitsluitend toegestaan na voorafgaande toestemming van het bestuur en worden vastgelegd in het logboek reglement afwijkingen	EV: - UV: -		
G-4.5	☐	In het IBP-beleid wordt verwezen naar het cameratoezicht en het reglement cameratoezicht	EV: - UV: -		
G-5.1	☐	Wijs een formeel verantwoordelijke aan voor accountbeheer (proceseigenaar of systeemeigenaar)	EV: - UV: -		
G-5.2	☐	Stel een proces op voor het aanvragen, toewijzen en toekennen van rollen en rechten binnen het camerasysteem	EV: - UV: -		
G-5.3	☐	Neem het verwijderen van accounts binnen camerasystemen op in het bestaande HR-proces "uit-dienst" en/of "wijziging van functie"	EV: - UV: -		
G-5.4	☐	Bij de steekproefsgewijze controle van het gebruik van het camerasysteem gaat de proceseigenaar na of de accounts en de toegekende rechten nog overeenkomen met de autorisatiematrix	EV: - UV: -		
Borging & controle					
G-6.1	☐	Stel een bewustwordingsprogramma op specifiek voor medewerkers met toegang tot het camerasysteem, gericht op o.a.: de vastgestelde doeleinden en kaders, het vier-ogenprincipe, de verbodsbepaling op eigen opnames, de logboekplicht en de gevolgen van misbruik of onzorgvuldig gebruik	EV: - UV: -		
G-6.2	☐	Medewerkers met toegang ontvangen bij het verkrijgen van hun autorisatie een briefing en bevestigen schriftelijk kennis te hebben genomen van het reglement cameratoezicht	EV: - UV: -		
G-6.3	☐	Het bewustwordingsprogramma wordt jaarlijks herhaald, gekoppeld aan de jaarlijkse evaluatie van de rechtmatigheid van de camera's	EV: - UV: -		
G-7.1	☐	Controleer of logging beschikbaar is, aanstaat en toegankelijk is voor de systeemeigenaar	EV: - UV:		

Risico	Status	Maatregel	Actiehouder ¹⁹	Actie datum	Opmerking
		OF Als het camerasysteem geen of onvoldoende logging biedt: update naar een versie die dit wel ondersteunt en zet logging aan	-		
G-7.2	☐	Ondersteunt het camerasysteem ook na een update aantoonbaar geen of onvoldoende logging, dan wordt dit vastgelegd in de lokale DPIA en is logging een eis bij vervanging van het systeem			
G-8	☐	Stel richtlijnen op voor zowel proactieve (periodiek, per kwartaal of halfjaar) als reactieve (incidentgestuurde) controle van de logging en de logboeken door de systeemeigenaar. De systeemeigenaar rapporteert de uitkomsten aan de proceseigenaar	EV: - UV: -		
G-9.1	☐	In de huurovereenkomst wordt vastgelegd dat op de locatie cameratoezicht plaatsvindt en dat de huurder zijn gebruikers namens het schoolbestuur hierover informeert. Het schoolbestuur stelt de huurder daarvoor de benodigde informatie ter beschikking. Het reglement cameratoezicht maakt als bijlage onderdeel uit van de overeenkomst	EV: - UV: -		
G-9.2	☐	Degene die de huurovereenkomst namens het schoolbestuur aangaat, geeft de tijden van verhuur voorafgaand aan de verhuur door aan de systeemeigenaar, zodat het tijdschema van de camera's daarop wordt afgestemd	EV: - UV: -		
Nieuwbouw & verbouwing					
G-10.1	☐	Betrek bij elk ontwerp- of verbouwtraject van een schoolgebouw de proces- en/of systeemeigenaar cameratoezicht, zodat de bouwkundige indeling vooraf wordt beoordeeld op de noodzaak voor aanvullend cameratoezicht	EV: - UV: -		
G-10.2	☐	Neem als ontwerpeis op dat een overvloed aan nissen, hoeken of anderszins onoverzichtelijke ruimtes wordt vermeden waar dit redelijkerwijs mogelijk is. Is dit niet mogelijk (bijvoorbeeld bij monumentale of bestaande bouw), dan wordt dit vooraf gemeld bij de proceseigenaar, zodat de noodzaak voor aanvullend cameratoezicht bewust wordt afgewogen in plaats van pas achteraf te blijken	EV: - UV: -		

Risico	Status	Maatregel	Actiehouder ¹⁹	Actie datum	Opmerking
G-11.1	☐	Neem camera's en recorder niet op in het bestek van de bouwaanbesteding	EV: - UV: -		
G-11.2	☐	Het schoolbestuur schaft het camerasysteem zelf aan, volgens de inkoop Eisen en het beheerprincipe	EV: - UV: -		
G-11.3	☐	Alleen bij een één-op-één vervanging van een schoolgebouw op dezelfde locatie, waar eerder rechtmatig cameratoezicht plaatsvond, mag het cameratoezicht direct bij oplevering worden ingericht. De ervaringen op de bestaande locatie kunnen worden gebruikt om cameraposities al in het ontwerp mee te nemen en voorbereidende voorzieningen, zoals bekabeling, kunnen in het bestek worden opgenomen. Actualiseer in dat geval vóór ingebruikname het cameraoverzicht, toets per camera opnieuw aan doel, noodzaak en plaatsing en vraag instemming van de (G)MR. Bij andere nieuwbouw wordt het cameratoezicht niet direct bij oplevering ingericht, maar pas wanneer op de nieuwe locatie een aanleiding is vastgesteld (incidenthistorie of aantoonbaar dreigend gevaar)	EV: - UV: -		

C. Overwegingen lokale DPIA, aanvullende risico's en maatregelen

! Volg instructie: 22. Lokale risico's en maatregelen op instructieblad

In aanvulling op de in de centrale DPIA gevonden risico's en maatregelen, zijn tijdens de uitvoer van deze lokale DPIA [geen/de volgende] lokale risico's en maatregelen vastgesteld.

[



= Kans



= Impact



= Risico

L.1 Risicotabel lokaal

#	Risico	Gevolgen			
Lokale DPIA					
L-1	...	...	-	-	!
L-2	...	...	-	-	!



= Risico



= Restrisko

L.2 Maatregelentabel lokaal

#	Risico kort		Maatregelen		Toelichting restrisko
Lokale DPIA					
L-1	...		...		...
L-2	...		...		...

L.3 Verbeterplan lokaal

Risico	Status	Maatregel	Actiehouder	Actiedatum	Opmerking
Lokaal					
L-1					
L-2					

D. Verklaring en advies functionaris voor gegevensbescherming (FG)

Volg instructie: 23. Verklaring en advies functionaris voor gegevensbescherming (FG) op instructieblad

De FG heeft kennis genomen van de door SIVON uitgevoerde centrale DPIA, de daarin geconstateerde risico's en aanbevolen maatregelen, en ook van de door het schoolbestuur zelf uitgevoerde lokale toetsing en de eventueel daaruit voortgekomen aanvullende risico's en maatregelen.

De FG is [wel/niet] betrokken geweest bij uitvoering en opstellen van de lokale DPIA voor [naam schoolbestuur]. [beschrijving rol FG schoolbestuur bij deze DPIA]
Het advies van de FG is [...].

E. Raadplegen betrokkenen

Volg instructie: 24. Raadplegen betrokkenen op instructieblad

In het kader van deze DPIA zijn de betrokkenen, te weten [leerlingen/, hun ouders/, medewerkers] [geraadpleegd/geïnformeerd] over de uitkomst.
[Zijn de betrokkenen, op wie de verwerking betrekking heeft, geraadpleegd over deze DPIA en wat is hun mening over de verwerking? Zo nee, waarom niet?]

F. Conclusie

! Volg instructie: 25. Conclusie op instructieblad

De centrale en lokale DPIA laten zien dat de gevolgen van de verwerking van persoonsgegevens binnen cameratoezicht - van leerlingen, [opvangkinderen,] ouders/verzorgers, (oud)medewerkers, bezoekers, leveranciers [en huurders] - voor de rechten en vrijheden van deze betrokkenen, na toepassing van risico-mitigerende maatregelen, in [onvoldoende/voldoende/goede] mate beheerst zijn.

Deze conclusie verandert, als de in deze DPIA genoemde maatregelen door het schoolbestuur niet of onvoldoende worden uitgevoerd.

De genomen en te nemen maatregelen, waarborgen, veiligheidsmaatregelen en mechanismen die binnen cameratoezicht de bescherming van persoonsgegevens garanderen, zijn [onvoldoende/voldoende/goed] gericht op het beperken van de risico's voor de rechten en vrijheden van betrokkenen.

Er is [wel/niet] gebleken van hoge risico's voor de rechten en vrijheden van betrokkenen die moeten leiden tot een 'voorafgaande raadpleging' zoals omschreven in artikel 36 AVG.

G. Risico-mitigerende maatregelen schoolbestuur

! Volg instructie: 26. Risico-mitigerende maatregelen schoolbestuur op instructieblad

Tijdens de uitvoer van de centrale en lokale DPIA zijn een aantal risico's geïdentificeerd. In de lokale DPIA is uitgewerkt welke maatregelen al zijn uitgevoerd en welke niet. De volledige lijst met openstaande maatregelen, inclusief eigenaar en streefdatum, is onderdeel van de lokale DPIA, onderdeel B. Overwegingen centrale DPIA, 21. Maatregelen (*D.1 Verbeterplan centraal*) en onderdeel C. Overwegingen lokale DPIA (*L.3 Verbeterplan lokaal*).

De genoemde punten worden uitgevoerd op een termijn van:

- [X-MAANDEN] voor de maatregelen bij hoge risico's (score 6-9)
- [X-MAANDEN] voor de maatregelen bij middel risico's (score 4)
- [X-MAANDEN] voor de maatregelen [noem maatregelnummers] die een aanzienlijke financiële investering vragen

H. Verklaring schoolbestuur

! Volg instructie: 27. Verklaring schoolbestuur op instructieblad

Het schoolbestuur, aangemerkt als vertegenwoordiging van verwerkingsverantwoordelijke [naam schoolbestuur], overwegende de conclusies, risico-mitigerende maatregelen en de aanbevelingen, verklaart hierbij:

- I. Kennis te hebben genomen van inhoud en uitkomsten van deze centrale en lokale DPIA.
- II. Kennis te hebben genomen van het advies van de FG en dit [in zijn geheel/gedeeltelijk/niet] over te nemen.

- III. In te stemmen met de in de rapportage genoemde beheersmaatregelen.
- IV. Opdracht te geven voor het uitvoeren van de beheersmaatregelen binnen de daarbij genoemde termijnen.
- V. De - in dit rapport - vermelde resterende risico's te aanvaarden.
- VI. Een jaarlijkse evaluatie van de rechtmatigheid van de camera's uit te voeren.
- VII. Jaarlijks aan de (G)MR te rapporteren over het cameratoezicht, waaronder de controle op het gebruik, datalekken en een samenvatting van de logboeken.
- VIII. Elke twee jaar het reglement cameratoezicht te evalueren en opnieuw vast te stellen.
- IX. Deze DPIA binnen een periode van 3 jaar te laten herzien, of eerder indien nodig*.
- X. [Een/Geen] voorafgaande raadpleging bij de Autoriteit Persoonsgegevens in te dienen.
- XI. Het DPIA-team decharge te verlenen.

* het cameratoezicht wezenlijk wijzigt (nieuwe hardware, nieuwe software, uitbreiding, etc.), nieuwe risico's ontstaan (bijvoorbeeld toepassen van nieuwe technieken, cloudopslag, etc.), technische of organisatorische wijzigingen plaatsvinden (het beheer aangepast wordt, andere netwerkinrichting, etc.) of wanneer incidenten daartoe aanleiding geven.

EN BESLUIT [NA (HER)OVERWEGING] HET GEBRUIK VAN CAMERATOEZICHT [WEL/NIET] TE [GEBRUIKEN/CONTINUEREN].

Naam bestuurder(s):

Plaats:

Datum:

Ondertekening:

10. Bijlagen

Bijlage 1: Gebruikte termen en definities

Alle type gegevens worden beschouwd als persoonsgegevens als ze direct of indirect tot een persoon te herleiden zijn. Deze definitiebepalingen hebben tot doel om consistentie te bieden bij het begrijpen van verschillende (wettelijke) termen en concepten die worden gebruikt bij de naleving van de AVG.

Begrippen die specifiek voor deze DPIA zijn gedefinieerd, zijn in deze bijlage gemarkeerd met een * en worden in de tekst met een hoofdletter geschreven. De overige begrippen zijn algemene termen uit de AVG en de privacypraktijk. Zij zijn ter uitleg opgenomen en worden in de tekst met een kleine letter geschreven. Rollen en logboeken worden in deze DPIA niet gedefinieerd en daarom met een kleine letter geschreven. In het reglement cameratoezicht zijn begrippen formeel gedefinieerd en worden zij met een hoofdletter geschreven.

Betrokkenen zijn personen waarop de gegevens betrekking hebben. Betrokkenen zijn alle geïdentificeerde of identificeerbare natuurlijke personen binnen de gegevensverwerkingen, oftewel de personen over wie de persoonsgegevens worden verwerkt. Denk hierbij aan: leerlingen, medewerkers, cliënten, zakelijke contacten, gebruikers en bezoekers.

Bijzondere persoonsgegevens mogen alleen verwerkt worden als je een beroep kunt doen op een uitzondering. Voor het onderwijs geldt bijvoorbeeld dat gezondheidsgegevens alleen gebruikt mogen worden als dat noodzakelijk is voor het geven van onderwijs en het begeleiden van een leerling. Ze zijn bijzonder omdat het gebruik van deze gegevens iemands privacy ernstig kan beïnvloeden. Voorbeelden zijn gezondheidsgegevens, levensovertuiging, lidmaatschap van de vakbond, ras of etnische afkomst.

Metadata is een categorie gegevens die over gebruik gaan, zoals de locatie van gebruik, tijdstip en device type.

***Gebruikstijden** zijn de tijden waarop een locatie in gebruik is: de Schooltijd en de tijden waarop (een deel van) de locatie wordt verhuurd. Het begrip wordt gebruikt voor de opnametijden van camera's die uitsluitend zijn ingezet voor de doeleinden 3 en/of 4 en voor cameratoezicht in praktijklokalen en gymzalen: deze camera's nemen alleen buiten de Gebruikstijden op.

Gevoelige persoonsgegevens gaan over gegevens die volgens de Autoriteit Persoonsgegevens (AP) snel inbreuk (kunnen) maken op de persoonlijke levenssfeer. Het gaat bijvoorbeeld om leerresultaten van kinderen, omdat daar conclusies aan kunnen worden verbonden met gevolgen voor het latere maatschappelijke leven. Of het gaat om grote verzamelingen van informatie van (zeer) jonge kinderen, gegevens over (problematische) gezinssituatie of²⁰ zwaardere eisen gesteld aan de beveiliging van de gegevens.

Kwetsbare groepen de categorieën van betrokkenen kunnen invloed hebben op de effecten van het voorstel. Bepaalde betrokkenen zijn kwetsbaarder dan anderen. Met kwetsbaar wordt bedoeld dat de negatieve effecten van een (onrechtmatige) gegevensverwerking groter kunnen zijn voor bepaalde betrokkenen dan voor andere betrokkenen. Denk hierbij aan minderjarigen en etnische minderheden. De AVG biedt specifieke bescherming aan kinderen, omdat zij zich minder bewust zullen zijn van de effecten van de gegevensverwerking en van hun rechten in dat kader.

Persoonsgegevens Onder persoonsgegeven wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. De term 'natuurlijke personen' betekent hier levende mensen. Informatie over overleden personen, rechtspersonen, dieren, zaken en objecten zijn in principe geen persoonsgegevens. Om te bepalen of een natuurlijke persoon identificeerbaar is, moet rekening worden

²⁰ https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013_snappet.pdf

gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken.

Hieronder staan voorbeelden van categorieën persoonsgegevens en type persoonsgegevens die binnen die categorie vallen:

- Naam (voornaam, achternaam, voorvoegsel, initialen)
- Contactgegevens (huisadres, telefoonnummer, e-mailadres)
- Demografische gegevens (leeftijd, geboortedatum en -plaats, geslacht, nationaliteit, opleiding, IQ)
- Apparaat- en internetgegevens (IP-adres, MAC-adres, metadata, locatie-informatie en geografische informatie)
- Financiële gegevens (bankrekeningnummer en -saldo, inkomens- en vermogensgegevens, loonschaal, kredietwaardigheid, winst eenmanszaak)
- Werk gerelateerde gegevens (KvK-nummer, verslag van een functioneringsgesprek, documentatie over negatief gedrag op de werkvloer)
- Overige persoonsgegevens (voertuigidentificatienummer, persoonlijke voorkeuren)

Ook metadata zijn persoonsgegevens als hieruit de identiteit van de betrokkene kan worden herleid. Over het algemeen is een type metadata op zichzelf niet voldoende identificerend, maar meestal worden meerdere type metadata verzameld van gebruikers. Al deze gegevens gecombineerd met elkaar kan leiden tot identificeerbaarheid van een individu.

***Schooltijd** is de tijd waarop een locatie in gebruik is voor het onderwijs en de overige activiteiten van de school zelf.

Strafrechtelijke persoonsgegevens zijn persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (artikel 10 AVG). Daaronder vallen ook gegevens over een verdenking, zoals het gegeven dat iemand als verdachte is aangemerkt. Deze gegevens genieten een verhoogde bescherming en mogen alleen worden verwerkt onder toezicht van de overheid, of wanneer de wet dit toestaat met passende waarborgen voor de rechten van betrokkenen. In Nederland is dit uitgewerkt in de artikelen 31 tot en met 33 UAVG.

***Structurele toegang** is de mogelijkheid voor een leverancier of onderhoudspartij om zich op elk moment, zonder voorafgaand akkoord van het schoolbestuur, met een eigen account op afstand toegang te verschaffen tot het camerasysteem, al dan niet in combinatie met toegang op de locatie. Toegang op de locatie met een account dat alleen lokaal werkt, zoals bij periodiek fysiek onderhoud, is geen Structurele toegang.

Verwerkingsverantwoordelijke is de partij die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Dit is degene die bepaalt waaróm en hóe persoonsgegevens worden verwerkt en is daarmee verantwoordelijk voor de naleving van de AVG.

Verwerker is een partij die ten behoeve van en in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder daarbij een eigen doel na te streven. Een verwerker verwerkt de gegevens dus niet voor eigen doeleinden, maar uitsluitend volgens de instructies van de verwerkingsverantwoordelijke. Deze afspraken worden vastgelegd in een verwerkersovereenkomst.

Bijlage 2: Instructies voor het uitvoeren van de lokale DPIA

De instructies voor het uitvoeren van de lokale DPIA is opgenomen in een apart document:

- DPIA Rapport Cameratoezicht instructies v1.0.pdf

Bijlage 3: Vragenlijst vaststellen risico's en getroffen maatregelen

! Volg instructie: 28. Bijlage 3 op instructieblad

De vragenlijst is opgenomen in een apart document:

- Vragenlijst DPIA Cameratoezicht v1.0.docx

Bijlage 4: Cameraoverzicht

! Volg instructie: 29. Bijlage 4 op instructieblad

Het cameraoverzicht is opgenomen in een apart document:

- Cameraoverzicht v1.0.xlsx

Bijlage 5: Voorbeeldborden cameratoezicht die aan de eisen van de EDPB voldoen

! Volg instructie: 30. Bijlage 5 op instructieblad

De bebording is opgenomen in een apart document:

- Cameratoezicht bebording v1.0.docx