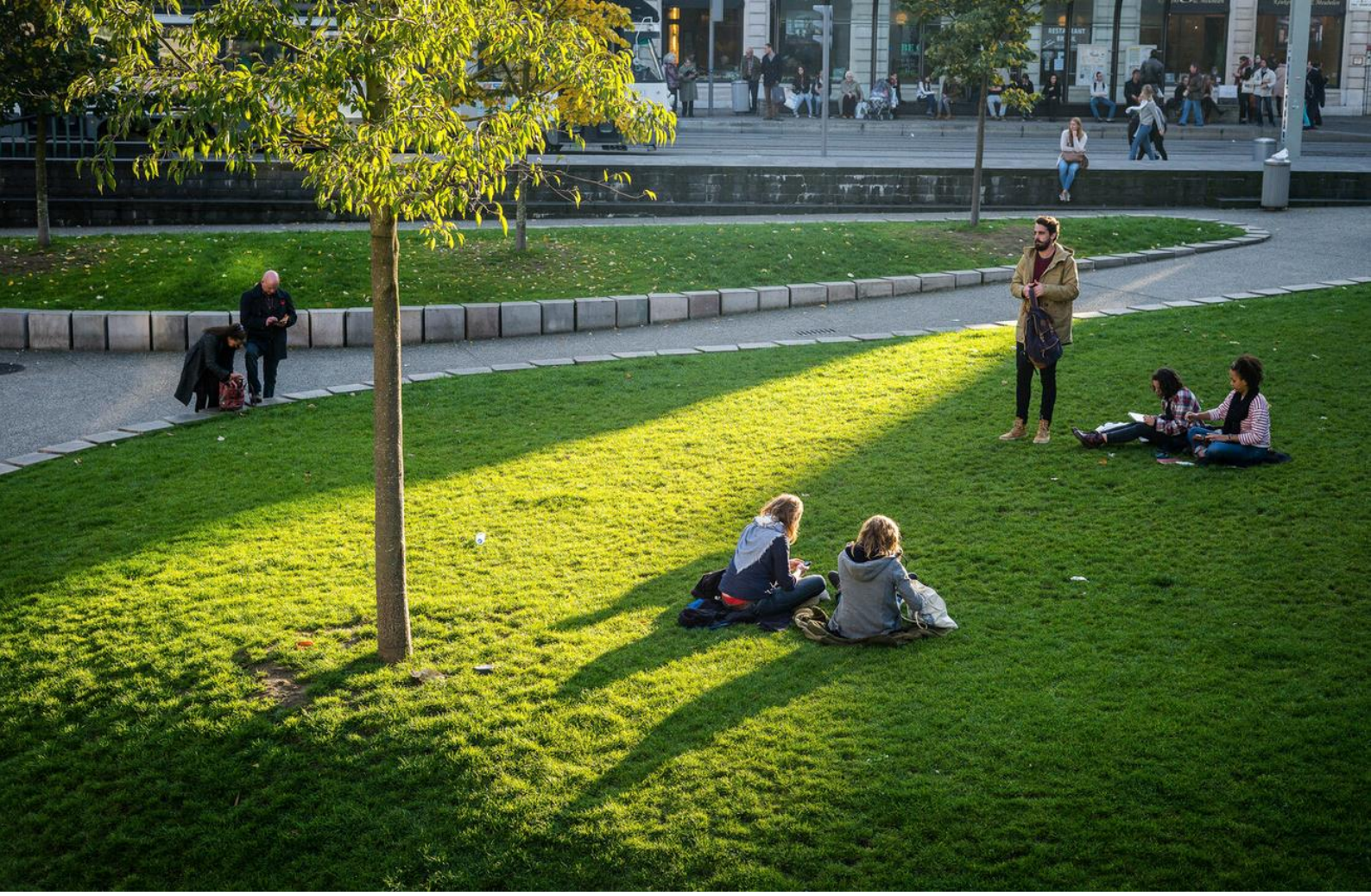
Cybersecurity

Beveiligingsrichtlijnen voor camerasystemen

Implementatie

vvsg



Voorwoord

In 2022 steeg de aandacht omtrent de cyberbeveiliging van (beveiligings)camera's en camerasystemen bij lokale besturen als gevolg van verschillende nieuwsartikels. Enkele veelgebruikte camera's of camerasystemen van bepaalde fabrikanten zouden veiligheidsrisico's onvoldoende afdekken, waardoor o.a. spionage mogelijk zou zijn. Verder leidden de nauwe banden tussen de producenten en buitenlandse mogendheden ook tot ethische vragen.

Om lokale besturen te ondersteunen in het beveiligen doorheen de aankoop en/of gebruik van camerasystemen werd wordt op vraag van het Agentschap Binnenlands Bestuur, in samenwerking met VVSG onderstaande beveiligingsrichtlijn ontwikkeld, ter aanvulling van de bestaande toolkit cyberveiligheid.

Deze beveiligingsrichtlijn voor camerasystemen is opgezet vanuit het perspectief van een lokaal bestuur dat een camerasysteem wenst aan te kopen of heeft aangekocht en dit verder dient te onderhouden. Hierbij werd rekening gehouden met goede praktijken alsook wereldwijd erkende modellen voor informatiebeveiliging.

Deze richtlijnen werden in samenwerking met verschillende belanghebbenden opgesteld, zoals het Agentschap Binnenlands Bestuur, in samenwerking met VVSG, experten uit lokale besturen, deelnemers uit de werkgroep "lerend netwerk camerabeleid" en private organisaties en gebaseerd op ervaringen uit het veld en kennis uit de literatuur.

Dit document kadert in het Project Cyberveilige Gemeenten, dat als doel heeft om lokale besturen voor te bereiden op de dreigingen van cybercriminaliteit. Dit project kwam tot stand uit een samenwerking met minister van Binnenlands Bestuur Bart Somers, het Agentschap Binnenlands Bestuur (ABB), de Vereniging van Steden en Gemeenten (VVSG), Audit Vlaanderen, Digitaal Vlaanderen, de taskforce van dit project, op basis van bestaand bronmateriaal van lokale besturen en externe partners.

Beveiligingsrichtlijnen camerasystemen	
Datum	
Versienummer	
Opdrachtgever	

INHOUDSTAFEL

Verklarende woordenlijst

Term	Verduidelijking
RACI Matrix	Matrix waarmee de rollen en verantwoordelijkheden van verschillende personen binnen een project of organisatie worden verduidelijkt & afgelijnd.
NDA	*Non-disclosure agreement of* "Vertrouwelijkheidsovereenkomst". Dergelijk document wordt gebruikt om vertrouwelijke informatie uit te wisselen binnen een vooraf bepaald kader.
DPO/ FvG	*Data protection officer (DPO) of* "Functionaris voor Gegevensbescherming" (FvG). De DPO is de persoon die toezicht houdt op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG) binnen het lokaal bestuur.
CISO	*Chief Information Security Officer* of "Hoofd voor informatiebeveiliging" is de eindverantwoordelijke voor informatieveiligheid binnen het lokaal bestuur.
DPIA	*Data protection impact assessment of* Gegevensbeschermingseffectbeoordeling, wordt gebruikt om privacy risico's in kaart te brengen bij het gebruik van persoonsgegevens.
IDS	*Intrusion detection system*, een systeem dat verdachte activiteit (zoals poging tot hacken of ongeautoriseerde toegang tot een netwerk) detecteert. Het is een soort alarmsysteem voor de IT-omgeving van het lokaal bestuur.
IPS	*Intrusion prevention system*, een systeem dat verdachte activiteiten op het netwerk identificeert én automatisch actie onderneemt om deze in te perken (bv. het rapporteren & blokkeren van verdachte activiteiten).
SSL	*Secure Sockets Layer*, een beveiligingsprotocol dat versleuteling en authenticatie biedt tussen computersystemen.
VPN	*Een virtual private network* creëert een versleutelde verbinding tussen een systeem en een gebruiker. Dit bemoeilijkt interceptie van informatie door onbevoegden en waarborgt de privacy van de gebruiker.
MFA	Multi-Factor Authenticatie is een authenticatiemethode die vereist dat een gebruiker verschillende authenticatiemiddelen gebruiken om toegang te krijgen tot een systeem of service. Op die manier zorgt een organisatie voor een sterkere beveiliging voor toegang van vanop afstand.
TLS	*Transport Layer Security*, de opvolger van SSL.
UPS	*Uninterruptible power supply*, of "ononderbroken stroomvoorziening". Een UPS wordt gebruikt om tijdelijk noodstroom te voorzien aan ICT-apparatuur.
IPsec	*Internet Protocol Security*, een standaard voor het beveiligen van internetprotocol door middel van encryptie en/of authenticatie. Dit biedt een veilige en betrouwbare manier om gevoelige informatie over te dragen via openbare netwerken.
SOC	*Security Operations Center*, een centrale eenheid die verantwoordelijk is voor het bewaken en analyseren van (onderdelen van) de IT omgeving van een organisatie. Het SOC speurt proactief naar kwetsbaarheden in beveiligingscontroles en vreemde gebeurtenissen in de IT omgeving. Daarnaast reageert dergelijk team ook doorgaans op beveiligingsincidenten om zo de informatiebeveiliging van een organisatie te waarborgen en te verbeteren.

Inleiding

In de afgelopen jaren is het belang en gebruik van camerasystemen steeds meer toegenomen voor lokale besturen en steden. Door o.a. de toename van criminaliteit en veiligheidsproblemen, zien lokale besturen een camerasysteem als een nuttige en effectieve maatregel om de veiligheid van hun inwoners te waarborgen. Tevens zorgt technologische vooruitgang er ook voor dat camerasystemen voor verschillende andere toepassingen gebruikt kan worden om zo ook een oplossing te bieden aan uitdagingen voor een lokaal bestuur. Denk bijvoorbeeld maar aan het tellen van verkeersstromen of beboeten van foutparkeerders.

Het gebruik van dergelijke camerasystemen heeft ook bepaalde gevolgen. Zo neemt het aantal vragen omtrent de inzet van camerasystemen, de beveiliging ervan en de impact op de privacy van burgers, sterk toe. In een recente bevraging van de VVSG waarbij verschillende IT-verantwoordelijken en functionarissen voor gegevensbescherming geraadpleegd werden omtrent camerasystemen en hun gebruik en beveiliging, kwamen de volgende resultaten naar voor:

- Het overgrote deel van bevraagde besturen voerde nog geen gegevensbeschermingseffectbeoordeling (GEB) uit om na te gaan of het verwerken van gegevens via het camerasysteem overeenstemt met de vereisten uit de Algemene Verordening Gegevensbescherming (AVG).
- Het merendeel van de deelnemende lokale besturen onderwerpt haar camerasystemen niet aan (periodieke) beveiligingstesten of werkt deze niet periodiek bij om kwetsbaarheden te verhelpen.
- Minder dan de helft van lokale besturen zorgt ervoor dat de informatiestromen van camerasystemen op een apart netwerksegment worden verstuurd en zo afgeschermd zijn van de rest van het netwerk. Tevens kunnen de meeste camerasystemen gegevens doorsturen naar de buitenwereld.
- Meer dan de helft van de bevraagde entiteiten voert geen regelmatige updates uit op systemen om kwetsbaarheden te beperken of maakt geen back-ups om gegevens uit camerasystemen voor een langere periode te bewaren.

Deze resultaten benadrukken dat lokale besturen baat hebben aan beleidsrichtlijnen of handvaten omtrent het beveiligen van camerasystemen en dat ze deze kunnen raadplegen bij de aankoop, implementatie of onderhoud van dergelijke systemen. Zo kunnen ze zowel de veiligheid als de privacy van burgers waarborgen. Dit document biedt een overzicht van de belangrijkste beveiligingsaspecten die lokale besturen in overweging moeten nemen bij het gebruik van hun camerasystemen.

Doelstelling

Het doel van dit document is om lokale besturen te helpen bij het ontwikkelen en implementeren van effectieve en efficiënte camerabewakingsrichtlijnen waarmee de veiligheid en privacy van burgers wordt gewaarborgd.

De richtlijnen bieden een overzicht van de belangrijkste aandachtspunten en goede praktijken inzake camerasystemen en een verzameling van praktische richtlijnen die lokale besturen kunnen gebruiken als basis. De volgorde waarin de verschillende onderwerpen die aan bod komen, is gebaseerd op gekende raamwerken en liggen ook in lijn met het auditraamwerk van de tweede thema-audit “Informatiebeveiliging” van Audit Vlaanderen.

De richtlijnen stellen lokale besturen in staat om zowel preventieve & reactieve maatregelen te nemen op basis van een op risico’s gestoelde aanpak. Zo kan een lokaal bestuur adequate maatregelen nemen die op maat zijn van het lokaal bestuur en die in verhouding staan tot de mogelijke gevolgen van het risico.

Overzicht leerpunten

Onderstaand stappenplan geeft een indicatie van de meest belangrijke stappen waar een lokaal bestuur mee rekening dient te houden bij de aankoop en implementatie van een camerasysteem. Meer gedetailleerde beveiligingsvereisten staan elders in dit document verduidelijkt.

1. Bepaal het doel en finaliteit van het camerasysteem.
2. Maak de afweging: zijn camera's wel noodzakelijk zijn voor het vooropgestelde doeleinde. Bijvoorbeeld: men kan fietsers tellen aan de hand van ANPR camera's, maar hiervoor kan ook een eenvoudig telsysteem voor gebruiken.
3. Voer een risicobeoordeling uit om mogelijke beveiligingsrisico's in proactief in kaart te brengen. Dit kan in parallel met de gegevensbeschermingseffectenbeoordeling (GEB) en definieer de nodige maatregelen om te voldoen aan de bestaande wetgeving.
4. Verkrijg het gunstig advies van de gemeenteraad en raadpleeg de lokale korpschef.
5. Definieer de functionele, technische en beveiligingsmaatregelen voor de aanbesteding en doorloop het proces voor de aanbesteding.
6. Koop het camerasysteem aan. Neem hierbij ook confidentialiteitsclausules, verwerkingsovereenkomsten, service level agreement (SLA, enz. in acht. Zie hiervoor ook 10. Beheer van leveranciers.
7. Wijs rollen en verantwoordelijkheden toe voor beheer en onderhoud van het camerasysteem en zie toe op de uitvoering ervan.
8. Implementeer het camerasysteem, volgens de reeds bestaande beleidsrichtlijnen van het lokaal bestuur:
    - Identificeer de locatie voor plaatsing. Sta hierbij stil bij de bepalingen uit de camerawet en AVG.
    - Registreer de camera op het e-loket van de FOD Binnenlandse zaken. Indien het een bewakingscamera betreft: maak een melding bij de lokale politiediensten en dit uiterlijk de dag voor die waarop de bewakingscamera in gebruik wordt genomen.
    - Installeer de camera's. Voorzie fysieke beveiligingsmaatregelen voor de camera en het camerasysteem, zoals stevige behuizingen, hek of draadwerk, kabelgoten voor stroom en netwerkkabels, het afsluiten van de serverruimte, voorzien van noodstroomoplossingen, enz.
    - Hang de nodige pictogrammen op als de camerawet dit voor deze camera vereist.
    - Registreer alle camera's, het camerasysteem en ondersteunende camerasysteem in het overzicht van bedrijfsmiddelen.

- Stel rollen op voor het toegangsbeheer tot de camera's en hun beelden en pas deze toe. Zorg daarvoor dat er rekening gehouden wordt met functiescheidingen en gebruik de reeds bestaande processen binnen het lokaal bestuur om toegangen tot het camerasysteem aan te vragen en toe te kennen. Zorg ook dat elke gebruiker een unieke ID heeft en veilig (vanop afstand) toegang krijgt tot het systeem en de authenticatievereisten worden afgedwongen. Waar mogelijk kan gebruik gemaakt worden van SSO.
- Zorg ervoor dat het verkeer van en naar de camera's en camerasystemen op een veilige manier verloopt. Voorzie hiervoor het gebruik van sterke versleutelingsmethodes en hanteer de netwerksegmentatiestrategie van het lokaal bestuur. Zo moet het beheer van de camera's en het systeem via een aparte verbinding verlopen, zijn beveiligingsmaatregelen zoals firewall, anti-malware en -virus, IDS of IPS aanwezig en moet er voldoende redundantie zijn voorzien.
- Beperk niet-noodzakelijke functionaliteiten en poorten (hardening). Zorg dat alle standaard wachtwoorden voor zowel de standaard (gewone als geprivilegieerde) accounts van de fabrikant gewijzigd zijn door sterke en complexe wachtwoorden en schakel ze uit waar mogelijk.
- Zet de nodige logging op opdat gebeurtenissen m.b.t. de beschikbaarheid, confidentialiteit of integriteit van de camerabeelden kunnen opgemerkt en opgespoord worden. Voorzie hiervoor ook de nodige alarmen en bescherm de logs.
- Verifieer of het camerasysteem juist is geplaatst en voer testen uit. Deze testen vinden best plaats in non-productieomgevingen met anonieme of fictieve gegevens.
- Werk periodiek het camerasysteem bij om updates uit te voeren of zie erop toe dat de leverancier dit doet. Hiervoor scant het lokaal bestuur best periodiek naar kwetsbaarheden of raadpleegt het haar leverancier daarvoor. Om kwetsbaarheden te verhelpen, verwijzen we naar de bestaande wijzigingsbeheersprocessen van het lokaal bestuur.
- Volg handelingen van leveranciers regelmatig op om na te gaan of zij hun taken volledig naleven. Voorzie daarvoor frequente overlegmomenten waarop statusrapportering wordt voorzien.
- Voorzie voldoende opslag voor camerabeelden en zorg ervoor dat alarmen worden gegenereerd wanneer deze tekort schiet. Neem hierbij ook de opslagtermijnen uit de camerawet en AVG in acht en zorg ervoor dat de camerabeelden versleuteld zijn opgeslagen en er back-up van gemaakt worden. Test ook periodiek of deze back-ups hersteld kunnen worden.
- Zorg ervoor dat ook de camera's mee in de processen voor het beheer van incidenten worden opgenomen.
- Weeg af of de camera's en camerasystemen deel uit maken van kritieke bedrijfsprocessen. Zo ja, werk het bedrijfscontinuïteitsbeheersplan bij.

9. Werk het verwerkingsregister bij, herzie het periodiek en werk bij waar relevant.

1. Beleidsrichtlijnen & interne organisatie

1.1 Beleid

Om het gebruik en onderhoud van camerasystemen in goede banen te leiden, is het belangrijk dat het lokale bestuur een informatiebeveiligingsbeleid heeft. Een dergelijk beleid beschrijft hoe een lokaal bestuur waakt over de vertrouwelijkheid, integriteit en beschikbaarheid van systemen en informatie die door de medewerkers van het lokaal bestuur worden gebruikt. Een lokaal bestuur moet onderzoeken op welke manier het zal omgaan met haar (camera)systemen.

Aangezien technologische vooruitgang kan leiden tot verouderde vereisten in het beleid, is het van belang dat een lokaal bestuur dit periodiek evalueert en indien nodig bijwerkt. Idealiter werkt een lokaal bestuur daarom een levenscyclus uit voor haar beleidsrichtlijnen waarbij de rekening houdt met de manier waarop ze beleidsrichtlijnen zal opstellen, communiceren, implementeren, opvolgen, herzien en wijzigen.

Dit beleid zal nadien in de praktijk moeten worden toegepast. Hiervoor stelt het lokaal bestuur een doordacht veiligheidsplan op om proactief gekende zwakheden weg te werken en tegemoet te komen aan geldende normen en richtlijnen. De VVSG werkte reeds een uitgewerkt sjabloon voor een veiligheidsplan uit dat als houvast kan dienen bij dit proces.

1.2 Beheersstructuur

Om beveiligingsrisico's die gepaard gaan met camerasystemen te beheren, dient een lokaal bestuur deze risico's eerst in kaart te brengen. Hiervoor dient de verantwoordelijke voor informatiebeveiliging samen met de DPO en medewerkers die het camerasysteem wensen aan te kopen of zullen gebruiken, na te gaan welke beveiligingsrisico's er aanwezig zijn. Dit gebeurt d.m.v. een gegevensbeschermingseffectbeoordeling (GEB). Een dergelijke beoordeling moet ook uitgevoerd worden als het camerasysteem voor andere doeleinden zal gebruikt worden dan initieel voorzien.

Elk mogelijk risico dient gecapteerd te worden in een overzicht, waarbij het een impact en waarschijnlijkheid krijgt toegewezen. Op basis daarvan worden prioriteiten aan risico's toegekend, net als een risicostrategie. Zo kan een lokaal bestuur een risico accepteren, overdragen aan een derde partij (bv. outsourcing), vermijden (door de activiteiten stop te zetten) of behandelen door bijkomende risicobeperkende maatregelen te nemen. In de volgende secties van dit document, staan dergelijke risicobeperkende maatregelen beschreven. Belangrijk is dat elk risico aan een verantwoordelijke wordt toegewezen, die over het risico en de (implementatie van) risicobeperkende maatregelen waakt.

Een lokaal bestuur moet een beheerstructuur opzetten om haar informatiebeveiligingsbeleid uit te voeren. Een effectieve beheersstructuur houdt in dat een lokaal bestuur rollen en verantwoordelijkheden inzake informatiebeveiliging voorziet voor haar camerasysteem, toewijst en de uitvoering ervan opvolgt (zowel bij aankoop, implementatie als onderhoud). Het doel hiervan is om verantwoordelijkheden eenduidig toe te wijzen zodat deze correct kunnen opgevolgd worden. “Het nakijken van systemen op kwetsbaarheden en deze verhelpen” of “het toekennen en periodiek nakijken van logische toegangen tot camerasystemen” zijn bijvoorbeeld verantwoordelijkheden die moeten opgevolgd worden.

Rollen en verantwoordelijkheden worden gedefinieerd door middel van een **RACI-matrix**. Een RACI-matrix wordt in het Nederlands een VERI-matrix genoemd, waarbij de aanduiding als volgt luidt: verantwoordelijk, eindverantwoordelijk, raadplegen en informeren. De tabel op volgende pagina zorgt voor verduidelijking.

		Beschrijving
R	Responsible of verantwoordelijk	De persoon die het werk doet om de taak te volbrengen.
A	Accountable of eindverantwoordelijke	Degene die uiteindelijk verantwoordelijk is voor het correct en grondig voltooien van de opdracht, en degene die het werk delegeert aan de *verantwoordelijken*.
C	Consulted of raadplegen	Personen wiens mening wordt gevraagd, doorgaans experten op het domein, en met wie er sprake is van wederzijdse communicatie.
I	Informed of informeren	Personen die op de hoogte worden gehouden van de voortgang, vaak pas na voltooiing van de taak of het resultaat; en met wie er slechts eenrichtingsverkeer is.

In onderstaande tabel kan de lezer enkele rollen en verantwoordelijkheden met betrekking tot de inhoud van dit beleid raadplegen. Let op, dit is geen exhaustieve lijst. Het de taak van het lokaal bestuur om deze verantwoordelijkheden te definiëren en toe te kennen.

	Algemeen Directeur	Hoofd ICT	DPO	Technische dienst
Opstellen en onderhouden van procedures voor het aanschaffen, ontwikkelen en onderhouden van camerasystemen	A	R	C	I
Opstellen, analyseren en bewaken van informatiebeveiligingsvereisten	C	A/R	R	I
Opstellen, analyseren en bewaken van de vereisten aangaande persoonsgegevens zoals geformuleerd in het AVG	C	R	A/R	
Plaatsen van camera's en waken over de fysieke beveiliging ervan	A	C	C	R
Toepassingen op publieke netwerken beveiligen	I	A/R	C	
Verlenen van logische toegang tot camerasystemen	A	R	I	
Implementeren en controleren van wijzigingen aan systemen		A/R	C/I	
Testen van systeembeveiliging	I	A/R	C	
Bewaken & rapporten van het naleven van de beveiligingsrichtlijnen	A	R	C	
Het communiceren naar autoriteiten (bv naar de gegevensbeschermingsautoriteit (GBA), Vlaamse toezichtcommissie (VTC) of het Centre for Cyber Security Belgium (CCB)).	A	C	R	

Opgelet!
Bij het definiëren van de rollen en verantwoordelijkheden moet rekening gehouden met het scheiden van rollen en verantwoordelijkheden en kan er slechts één eindverantwoordelijke aangewezen worden. Gedeelde verantwoordelijkheden of rollen zijn mogelijk, maar verhogen de kans op fouten. Voor kleinere organisaties kan het moeilijk zijn om functiescheiding te realiseren, maar het principe moet pragmatisch en zoveel mogelijk worden toegepast.

2. Beheer van middelen van het lokaal bestuur

2.1 Middelen van het lokaal bestuur

Overzicht van middelen

Om zich ervan te verzekeren dat alle camerasystemen, camera's en bijhorende infrastructuur (zoals servers) opgevolgd worden, is het cruciaal dat een lokaal bestuur een overzicht opstelt van haar middelen zoals systemen, infrastructuur of informatie.

Opgelet!
Een dergelijk overzicht bevat minstens de volgende elementen:

- Een **uniek identificatienummer** of benaming per camera en per ondersteunende component
- De geassocieerde **hardware** en **software** (en de versie daarvan)
- Fysieke **locatie**
- **IP-adres**(sen)
- **Opslagsystemen**
- De **eigenaar** van het toestel
- De relevante (software)**leverancier**

Opvolgen van middelen

Daarnaast is het belangrijk dat een lokaal bestuur dit overzicht periodiek bijwerkt om de juistheid van de informatie van dit overzicht te vrijwaren. Zo kan men bijvoorbeeld snel nagaan welke kwetsbaarheden aanwezig zijn op het camerasysteem (versie van software), de afhankelijkheden identificeren bij storing of simpelweg de juiste contactpersonen raadplegen wanneer er vragen zijn.

Hiervoor stelt het lokaal bestuur best een procedure op waarin het beschrijft hoe iemand dit overzicht moet nakijken, hoe frequent dat dient te gebeuren en aan wie de resultaten van dit nazicht dienen gecommuniceerd te worden. Bijvoorbeeld: een medewerker van het team ICT kijkt halfjaarlijks na of de informatie in het overzicht wel klopt. Belangrijke wijzigingen worden aan het hoofd van het team ICT en de verantwoordelijke voor de camera of het camerasysteem gemeld.

Idealiter zorgt het lokaal bestuur ervoor dat haar overzicht van middelen (automatisch) bijgewerkt wordt wanneer een installatie van of wijziging aan een toestel (bv. camera) plaats vindt. Zoals aangegeven moet elke stuk informatie, systeem of infrastructuur ook aan een eigenaar worden toegewezen. Deze eigenaar moet:

- Vereisten opstellen over hoe er met de middelen moet omgesprongen worden (bv. in een gedragscode die deel uitmaakt van het informatieveiligheidsbeleid) en toezien op de naleving ervan.
- Ervoor zorgen dat informatiemiddelen (zoals camerabeelden) geïnventariseerd worden en de informatie in dit overzicht ook actueel gehouden wordt. Daarbij moet ook rekening gehouden worden met de (koppelingen met) andere ondersteunende toepassingen en bedrijfsmiddelen.
- Ervoor zorgen dat aan de informatiemiddelen een passend informatieclassificatieniveau worden toegewezen en dat deze middelen overeenkomstig met dat classificatieniveau worden beschermd. Camerabeelden moeten ingedeeld worden volgens het toepasselijk informatieclassificatiemodel op basis van de gevoeligheid van de verwerkte gegevens. Dit niveau bepaalt ook de relevante graad van bescherming. Hiervoor rijkt Digitaal Vlaanderen het volgende informatieclassificatiemodel aan, maar een lokaal bestuur kan perfect een eigen model opstellen, zoals een model dat uit 4 niveau's bestaat, waar bij "Geheim" de meest gevoelige vorm van informatie is, gevolgd door "Vertrouwelijk", "Beperkt" en "Publiek beschikbaar".
- Periodiek de toegekende classificatie labels controleren en nagaan of er juist met de informatie wordt omgesprongen, bijvoorbeeld dat camerabeelden van de inkomhal van het gemeentehuis niet op een publieke locatie zijn opgeslagen.
- Ervoor zorgen dat de juiste methode van verwijdering of vernietiging wordt toegepast op informatiemiddelen volgens hun informatieclassificatieniveau, zoals het vernietigen van harde schijven door een gespecialiseerde firma.
- Toegangsbeperkingen definiëren in overeenstemming met het informatieclassificatieniveau en periodiek controleren of deze beperkingen worden gehandhaafd. Zo hebben publieke beelden (Bv. een webcam met zicht op een plein) geen beperking nodig, terwijl beelden van de serverruimte wel beperkt moeten zijn (tot enkel medewerkers van het IT team).
- Verzekeren dat bij het verwijderen van apparatuur alle aanwezige informatie correct gewist wordt met behulp van technieken die het onmogelijk maken om de originele informatie terug te halen.

Een eigenaar mag operationele/routinematige activiteiten delegeren aan een afgevaardigde. Dat kan bijv. een andere medewerker binnen het lokaal bestuur zijn of een medewerker van de leverancier die operationele taken voor het lokaal bestuur uitvoert. De eigenaar blijft echter verantwoordelijk voor dat bedrijfsmiddel, in dit geval de camera of het camerasysteem.

Opgelet!
Indien een camera mobiel gebruikt wordt en meegenomen kan worden, dient de eigenaar ook op te volgen aan wie het toestel werd uitgeleend. De eigenaar volgt dit ook op als medewerkers een andere functie krijgen binnen het lokaal bestuur of het lokaal bestuur verlaten.

Verwijderbare gegevensdragers

Wanneer gebruik gemaakt wordt van verwijderbare opslagmedia (e.g. verwijderbare schijven, cameratapes, etc.), dienen volgende maatregelen te worden genomen:

- Zorg ervoor dat het gebruik van USB-poorten enkel mogelijk is, als daar een nood voor is binnen het lokaal bestuur (bv. voor het kopiëren en delen van bestanden via USB) en blokkeer ze waar mogelijk. Dat kan logisch (d.m.v. een specifieke toepassing of instelling op het systeem) of fysiek (d.m.v. een USB port lock);
- Het lokaal bestuur moet een autorisatieprocedure hebben voor het verwijderen van opslagmedia en houdt daarbij bewijs van bij in een logboek. Dat kan bijvoorbeeld in een toepassing van de helpdesk waarbij een ticket de datum, het toestel, de actie en verantwoordelijke/uitvoerende medewerker vermeldt, maar ook simpelweg een toevoeging aan een digitale lijst;
- Om het risico op het verloren gaan van camerabeelden, omdat het medium waarop de informatie opgeslagen wordt verouderd is, verder te beperken en te verminderen, moet informatie tijdig overgezet worden naar een nieuw opslagmedium voordat de informatie onleesbaar wordt.
- Waardevolle informatie moet op meerdere aparte opslagmedia worden opgeslagen.

2.2 Het transporteren van informatie & gegevensdragers

Bij het versturen of doorgeven van informatie zoals beelden of gegevensdragers zoals tapes of harde schijven dient de beveiliging van de informatie ook steeds gegarandeerd te worden. Richtlijnen omtrent netwerkbeveiliging of cloud-omgevingen staat verder beschreven. Zo worden camerabeelden best op een veilige manier doorgegeven in plaats van een publiek beschikbare locatie/link. Daarnaast neemt het lokaal bestuur ook best de volgende maatregelen in acht:

- Wijs verantwoordelijkheden toe aan medewerkers die instaan voor het controleren en melden van de overdracht, verzending en ontvangst van het toestel.
- De verpakking moet de inhoud van het pakket beschermen tegen fysieke schade die tijdens het transport kan ontstaan. Bv. een medewerker van het lokaal bestuur zal bij het versturen van een pakket met tapes waar camerabeelden op staan, ervoor zorgen dat de tapes ingepakt zijn met noppenfolie en zorgt dat deze medewerker ook de verzendingsbon van het pakket bewaart. Neem hiervoor ook de specificaties van de fabrikant in acht.
- Hanteer enkel geautoriseerde (betrouwbare) koeriers om cameratoestellen of andere onderdelen te transporteren. Hier stelt het lokaal bestuur best proactief een lijst van toegestane koeriers op.
- Tot slot houdt een lokaal bestuur ook best een logboek bij waarin het de gehele lijn van overdracht (vanaf beslissing tot verzending tot aftekening ontvangst) in capteert. Dat kan eenvoudigweg een lijst zijn waarin elke actie staat beschreven, met bijhorende datum en handtekening van de verantwoordelijke. “15 Mei 2023 – Johan Peeters – Verzenden van harde schijf voor camerasysteem XYZ via postdienst ABC”.

Naargelang de gevoeligheid van bv. de beelden op het toestel, kan een lokaal bestuur ook overwegen om het pakket te verzegelen of daarop te controleren, door een zegel aan te brengen op het pakket en na te gaan of deze bij ontvangst al dan niet verbroken is.

3. Toegangsbeheer

3.1 Lokale en externe toegang

Om de toegang tot (beelden van) camerasystemen te beperken, dient een lokaal bestuur een beleid op te stellen voor haar toegangsbeveiliging. Indien dit reeds aanwezig is, past het lokaal bestuur dit toe op haar camerasystemen. Hierbij dient ook rekening gehouden te worden met de vereisten van het lokaal bestuur, wetgeving en informatiebeveiligingseisen.

Alvorens een persoon toegang krijgt tot (beelden van) het camerasysteem, dient dit te worden aangevraagd, door middel van een gedocumenteerde procedure. De volgende zaken dienen minstens aanwezig te zijn in deze aanvraag: datum, aanvrager, persoon voor wie rechten gevraagd wordt, gevraagde rechten (ook de desbetreffende systemen), de motivatie om toegang te krijgen tot het systeem en de einddatum van rechten indien van toepassing. Documenteer eveneens de goedkeuring van de aanvraag. Dat kan bijvoorbeeld via een tickettingoplossing.

Hieronder lijsten we enkele vereisten op die doorgaans mee in een dergelijk beleid omtrent het beheer van toegangen aan bod kunnen komen:

- Elke gebruiker van het camerasysteem dient een unieke identificatie te hebben. Hierbij maakt een lokaal bestuur best een onderscheid in de benaming van haar accounts om eigen medewerkers of medewerkers van derde partijen eenvoudig te kunnen onderscheiden. Dat kan eenvoudigweg door een prefix toe te voegen aan accounts van derde partijen, zoals “EXT_gebruikersnaam”.
- Elke gebruiker dient zich te authentiseren alvorens gebruik te maken van zijn account. Idealiter gaat die via de reeds bestaande oplossing van het lokaal bestuur en door middel van single sign-on (SSO). Indien toegang vanop afstand verkregen wordt, bv. omwille van thuiswerken of toezicht houden vanop een controlepost op een andere locatie, is een bijkomende authenticatiefactor (MFA) aangeraden, net zoals een beveiligde netwerkverbinding (bv. via VPN).
- Indien externen toegang nodig hebben tot het camerasysteem, omdat ze voor het lokaal bestuur werken, dienen deze personen ook het beleid omtrent toegangsbeveiliging van het lokaal bestuur na te leven. Hiervoor kan het lokaal bestuur vereisen dat de derde partij het informatieveiligheidsbeleid van het lokaal bestuur accepteert en zich hier naar schikt. Dit moet bij de aanbesteding afgesproken worden.
- Toegang tot informatie en/of systemen dient beperkt te worden tot een strikt minimum. Hierbij zal het lokaal bestuur rekening houden met het takenpakket van de gebruiker.

- Toegang tot (informatie uit) het camerasysteem dient gegeven te worden aan de hand van rollen en functies. Een rol moet specifiek dienen voor één systeem (bv. het bekijken van beelden van een specifiek camerasysteem) en een functie moet een functie zijn die eigen is aan de organisatie (bv. toezichthouder van de sportzaal die in het beheer is van het lokaal bestuur).
- De verantwoordelijke voor het camerasysteem dient de toegangsrechten van gebruikers regelmatig te beoordelen. De frequentie van dit nazicht (zoals maandelijks, per kwartaal, halfjaarlijks of jaarlijks) dient gestuurd te worden door de gevoeligheid van de informatie waartoe deze toegangsrechten toegang hebben. De gevoeliger de beelden/informatie, de frequenter de toegangsrechten dienen nagekeken te worden. Hier dient ook rekening gehouden te worden met het type werknemer (extern of intern). Dit kan tevens deels geautomatiseerd worden door bijvoorbeeld accounts uit te schakelen als ze voor een langere periode (bv. na 6 weken) niet meer gebruikt zijn.

Naast gewone gebruikersaccounts, komen er nog andere types van accounts voor, nl. generieke accounts en geprivilegieerde accounts. De eerste categorie zijn accounts waar een of meerdere medewerkers gebruik van kunnen maken, maar waar de account niet terug te leiden is tot 1 persoon. Dit bemoeilijkt het achterhalen wie met dit soort account acties uitvoerde. Geprivilegieerde accounts zijn accounts waarmee beheerdersopdrachten kunnen worden uitgevoerd en die dus meer vergaande en gevoelige handelingen toelaten. Bijvoorbeeld: rechten die de mogelijkheid geven om wijzigingen door te voeren aan het netwerk, systemen, beveiliging en applicaties.

Generieke accounts

Standaard zijn generieke gebruikers niet toegelaten enenkel toegestaan als daar een gegronde reden voor is. Waar dit toch nodig zou zijn, moet het aanmaken van dergelijke account door de verantwoordelijke voor informatiebeveiliging (vaak ook het hoofd ICT) worden goedgekeurd Daarnaast moet er voor accounts die niet gelinkt zijn aan één persoon, een eigenaar bepaald worden die opvolgt welke personen allemaal toegang hebben tot dit generieke account.

Wanneer een generieke gebruiker wordt aangemaakt om gebruikt te worden door een systeem of toepassing, moet de motivatie en goedkeuring hiervan ook gecapteerd worden. De eigenaar zal verzekeren dat het wachtwoord gewijzigd zal worden bij vertrek of wijziging van functie van één van de mensen die toegang tot dit generieke account hebben.

Geprivilegieerde accounts

Voor geprivilegieerde accounts, gaat het lokaal bestuur best na welke geprivilegieerde accounts er op haar camerasystemen aanwezig zijn en stelt hier en overzicht van op.

Zorg dat alle standaard wachtwoorden voor zowel de standaard (gewone als geprivilegieerde) accounts van de fabrikant gewijzigd zijn door sterke en complexe wachtwoorden en schakel ze uit waar mogelijk.

Daarnaast dient het toewijzen en gebruik van dergelijke accounts te worden beperkt en beheerst. Dit kan eventueel via het reeds bestaande proces om toegangen en rechten toe te kennen, maar extra aandacht dient gegeven te worden aan het goedkeuren van dit type verzoeken (bv. enkel de algemeen directeur of hoofd van IT kan dit goedkeuren en deze rechten toekennen).

Verder dient een lokaal bestuur er ook voor te zorgen dat het gebruik van speciale toegangsrechten gelogd en nagekeken worden en dat deze logs van sterkere beveiliging genieten (door bijvoorbeeld encryptie toe te passen, door het wijzigingen van dit soort logs onmogelijk te maken, door back-ups of een extra locatie te voorzien, enz.). De toegang tot deze toegangsrechten dient zo beperkt mogelijk te zijn. Daarom gaat het lokaal bestuur ook na welke gebruikers toegang mogen hebben tot dit type accounts en beperkt dit zoveel mogelijk. Daarnaast dienen de wachtwoordvereisten strikter te zijn en wordt er best gebruik gemaakt van multi-factor authenticatie (MFA).

3.2 Authenticatie

Doorgaans melden gebruikers zich aan (authentiseren) met een gebruikersnaam en wachtwoord. Waar mogelijk, gaat het lokaal bestuur ook na of het mogelijks is om het authenticatiemechanisme van het camerasysteem te enten op een reeds aanwezig oplossing en zo dus gebruik te maken van single sign-on (SSO).

Het toewijzen van geheime authenticatie-informatie (zoals gebruikersnaam & wachtwoord) moet op een veilige en gestructureerde manier gebeuren.

- Wachtwoorden moeten enkel kunnen aangemaakt en gereset worden door mensen die daarvoor zijn aangewezen (zoals een helpdesk of het team ICT).
- Het wachtwoord dient gecommuniceerd te worden naar de gebruiker via een ander medium dan waar de gebruikersnaam werd gecommuniceerd. Een gebruikersnaam kan bijvoorbeeld per mail gestuurd worden en het wachtwoord wordt mondeling gecommuniceerd per telefoon of per sms verzonden.
- Het initiële wachtwoord dient willekeurig te zijn.
- De gebruiker moet verplicht worden om het wachtwoord te wijzigen bij het eerste gebruik.
- Wanneer het wachtwoord van een gebruiker bekend is of het vermoeden daarvan bestaat, dient het wachtwoord zo snel mogelijk gewijzigd te worden.

Toegang tot informatie en systeemfuncties van het camerasysteem moet worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging van het lokaal bestuur. Indien het beleid voor toegangsbeveiliging of de risicobeoordeling dit vereist, moet toegang tot het camerasysteem te worden beheerst door een beveiligde inlogprocedure. Hierbij stellen we enkele maatregelen voor:

- Een wachtwoord dient in een niet leesbaar formaat weergegeven worden en
- Een wachtwoord dient voldoende lang en complex te zijn
- Na inloggen dient het systeem weer te geven wanneer de gebruiker voor het laatste aangemeld was.
- Na foutief aanmelden mag het systeem niet zeggen waarom het aanmelden exact niet gelukt is.
- Authenticatie informatie dient versleuteld verstuurd worden.
- Na een aantal gefaalde inlogpogingen dient de gebruiker geblokkeerd te worden.
- De gebruikerssessie dient vergrendeld te worden na een bepaalde duur van inactiviteit.
- Het gebruik van een bijkomende authenticatiefactor (MFA) naargelang de gevoeligheid van de beelden van de camera's of locatie vanwaar de gebruiker aanmeldt (vanop afstand).
- Het loggen van gelukte en gefaalde authenticatiepogingen en blokkeren van herhaaldelijke foutieve aanmeldpogingen. Daarnaast kan een lokaal bestuur ook kiezen om authenticatiepogingen vanuit het buitenland onmogelijk te maken omdat daar geen medewerkers van het lokale bestuur actief zijn.

Systemen voor wachtwoordbeheer behoren interactief te zijn Het is noodzakelijk om authenticatie te verplichten voor het verkrijgen van toegang tot niet-publieke informatie. Bovendien moeten wachtwoorden automatisch worden gecontroleerd wanneer mogelijk. Indien mogelijk moet er gebruik worden gemaakt van multi-factor authenticatie.

Opgelet!
Om de veiligheid van wachtwoorden te waarborgen, moeten ten minste de volgende parameters aanwezig zijn volgens NIST:

- lengte (bv. 8 karakters)
- complexiteit (combinatie van verschillende characters zoals cijfers, letters, leestekens en andere)
- vervaldatum (naargelang de complexiteit kan deze vervaldatum ruimer ingesteld worden of zelfs vervallen – Let op, enkel voor zeer complexe wachtwoorden)
- wachtwoorden worden best naast een lijst van gekende databases van gelekte wachtwoorden
- Er mogen geen gelijkaardige voorgaande wachtwoorden gehanteerd worden
- Het is verplicht om het wachtwoord bij eerste gebruik te wijzigen
- Na 10 foutieve pogingen dient het account automatisch vergrendeld te worden.
- Systemen mogen geen hints naar wachtwoorden meer geven
- SMS geldt niet langer als veilige authenticatiemethode voor MFA.

4. Netwerkbeheer

4.1 Integratie en/of opdeling van het netwerk

Om te vermijden dat een aanvaller zich eenvoudig doorheen de IT omgeving van een lokaal bestuur kan bewegen, is het belangrijk om het netwerk in netwerkzones op te delen en deze van elkaar af te schermen. Vergelijk het met een appartementsgebouw: alle bewoners kunnen door de voordeur binnen, maar niet iedereen krijgt toegang tot hetzelfde appartement (netwerksegment). De gegevens van de camera's worden via een netwerk naar het camerasysteem verstuurd, daarom is het belangrijk dat de verbinding altijd beschikbaar en veilig is. Daarnaast wordt het bijvoorbeeld quasi onmogelijk om de camerabeelden te raadplegen, zonder netwerkverbinding. Om de beveiliging van het netwerkverkeer van een camera(systeem) te waarborgen, voert een lokaal bestuur eerst een risicobeoordeling uit om de benodigde beveiligingsmaatregelen te bepalen.

Op basis daarvan dienen de volgende maatregelen al dan niet (strikter) geïmplementeerd te worden:

Maatregel	Acties
Netwerksegmentatie	Om ervoor te zorgen dat camera's en bijbehorende datastromen beveiligd zijn, is het best om deze te scheiden van de rest van het netwerk. Dit kan bereikt worden door ze in een apart deel van het netwerk te plaatsen, wat we een "netwerksegment" noemen. Hierdoor voorkomt een lokaal bestuur dat een hacker of een virus zich door het hele netwerk kan verspreiden. De beslissing om een netwerksegment te maken wordt genomen op basis van factoren zoals de gevoeligheid van de informatie die aanwezig is en het type gebruikers (bijvoorbeeld een wifi-netwerk voor bezoeker).
Gescheiden beheer van camerasysteem en netwerk	De twee verbindingen (voor gebruik en beheer) moeten voor verschillende doeleinden worden gebruikt en idealiter via een aparte netwerkverbinding worden uitgevoerd. Op deze manier voorkomt een lokale bestuur dat camera's en systemen niet geraadpleegd kunnen worden in geval van een calamiteit. Dit verkleint het aanvalsoppervlak voor hackers omdat ze een specifiek en meer beveiligde netwerkverbinding moeten onderscheppen. Een lokaal bestuur moet ook een plan opstellen waarin staat hoe het netwerk zal worden beheerd en hoe wijzigingen in de netwerkconfiguratie worden uitgevoerd.

Maatregel	Acties
Redundantie	Kritieke netwerkapparaten en verbindingen voor camerasystemen en/of camera's moeten redundant worden opgezet om beschikbaarheid te garanderen en dat er geen single points of failure zijn (zoals verschillende servers op slechts één netwerkswitch aan te sluiten). Door deze zwakke plekken te identificeren, kan een lokaal bestuur maatregelen nemen om de continuïteit van systemen en processen te verbeteren.
Authenticatie	Sterke authenticatie moet worden toegepast om toegang te krijgen tot het netwerk waar het camerasysteem of camera op is aangesloten.
Beveiliging communicatie over het netwerk	Er moeten maatregelen worden genomen om de vertrouwelijkheid en integriteit van de informatie die via het netwerk verzonden wordt, te waarborgen zoals het gebruik van veilige netwerkprotocollen (SSL of TLS) voor het beveiligen van de communicatie tussen de camera's en andere apparaten op het netwerk. Tevens moet het lokaal bestuur vermijden dat zwakke, kwetsbare of verouderde algoritmen voor versleuteling worden gebruikt.
Aanvullende beveiligingstechnologieën	Proxy, firewalls, oplossingen voor de preventie van gegevenslekken, inbraakdetectiesystemen (IDS), inbraakpreventiesystemen (IPS), enz. dienen aanwezig te zijn op zowel op de grens het netwerk van het lokaal bestuur en externe netwerken als tussen interne netwerksegmenten.
Logging en monitoring	Het is belangrijk om de acties die van invloed kunnen zijn op de beveiliging van de camera's of het systeem zorgvuldig bij te houden. Dit kan gebeuren door middel van logging en monitoring van deze acties. Door deze logs te analyseren, kan worden bepaald of er ongebruikelijke of verdachte activiteiten plaatsvinden en kunnen de nodige maatregelen worden genomen. Het is ook belangrijk dat er alarmfuncties worden geïmplementeerd, zodat het lokaal bestuur direct op de hoogte is in geval van een beveiligingsincident. Voor elke beveiligingsmaatregel moet een verantwoordelijke aangewezen worden, die deze toegewezen maatregel zal opvolgen.
Evaluatie	Periodiek, minstens één keer per jaar, dient een evaluatie te worden uitgevoerd om na te gaan of informatiesystemen zich nog in de juiste netwerksegmenten bevinden.
Audit en beheer van netwerken	Het auditeren en beheren van netwerken dient plaats te vinden vanuit een minimaal logisch gescheiden netwerksegment

Maatregel	Acties
Beveiliging netwerkproviders	Om ervoor te zorgen dat informatie die van en naar camera's gestuurd wordt altijd beveiligd en beschikbaar blijft, moet een lokaal bestuur de netwerkproviders opvolgen en verzekeren dat ze de afgesproken beveiligingsmaatregelen implementeren. Dit kan onder andere door periodiek overleg. De overeenkomsten met netwerkproviders moeten daarom afspraken bevatten die aangeven dat het lokaal bestuur het recht behoudt om een onafhankelijke audit uit te voeren om de huidige beveiligingsmaatregelen en hun implementatie en doeltreffendheid na te gaan. Dit zorgt ervoor dat er een transparante en verantwoordelijke relatie tussen het lokaal bestuur en de netwerkproviders bestaat en dat eventuele beveiligingsrisico's kunnen worden geïdentificeerd een aangepakt.

Opgelet!
Wanneer een lokaal bestuur zelf geen audits wenst uit te voeren op haar derde partijen of de derde partij dit niet toestaan, moet het lokaal bestuur om garanties omtrent de kwaliteit van dienstverlening vragen via daarvoor voorziene certificeringen, zoals bijvoorbeeld een SOC 2 rapport, of ISO 27001 certificering voor informatieveiligheid of ISO 9001 voor kwaliteitsbeheer.

Wanneer het nodig is om het netwerksegment waarin het camerasysteem zich bevindt (op het interne netwerk van een lokaal bestuur) te beveiligen met firewalls, moet de verantwoordelijkheid en het beheer van deze firewalls op de externe grens van dit netwerksegment worden toegewezen bij het ICT-team. De grens van zo een netwerksegment mag niet direct verbonden zijn met de buitenwereld. Daarnaast moeten dergelijke externe verbindingen of netwerken met camera's of camerasystemen beveiligd en gemonitord worden door minstens 1 firewall, die onder het beheer van het lokaal bestuur valt.

Verbindingen van camerasystemen met externe netwerken moeten minimaal worden beschermd door een 'stateful inspection firewall' met uitgebreide logging-, monitoring- en alarmfuncties.

Zo dient het lokaal bestuur ook maatregelen te nemen om misbruik en onbevoegde toegang tot het netwerk te detecteren. Het is belangrijk om firewalls te configureren zodat ongeautoriseerde verbindingen worden geblokkeerd om de verspreiding en het misbruik van malware te beperken. Daarnaast moet het netwerkverkeer van en naar camera's en camerasystemen worden gemonitord en beperkt, zodat enkel vooraf toegestane verschillende types van verkeer kunnen plaats vinden.

Tot slot reikt Digitaal Vlaanderen ook in haar minimale maatregelen nog bijkomende veiligheidscontroles aan, naargelang de gevoeligheid van de informatie die verwerkt wordt.

5. Fysieke beveiliging

5.1 Fysieke maatregelen

Om de informatie en camerasystemen te beschermen, is het van cruciaal belang om de juiste beveiligingsmaatregelen te nemen. Beveiligingsperimeters moeten worden en gebruikt om de ruimtes te beschermen waar informatie en camera's zich bevinden om zo ongeoorloofde fysieke toegang, schade en inmenging te voorkomen. Naast het gebruik van een beveiligingsperimeter, kunnen volgende factoren bijdragen tot de bescherming van camera's:

- **Bescherming tegen vandalisme en weersomstandigheden**: Plaats camera's in schuilplaatsen of gebruik van beschermingskappen of stevige behuizingen. Daarnaast moeten camera's moeten op de juiste hoogte worden geplaatst om een goed overzicht te hebben en om de fysieke toegang te beperken. Zo plaatste de stad Genk haar camera's rondom het stadion van KRC Genk ver buiten bereik van mogelijke vandalen.
- **Bescherming van kabels**: Beveilig kabels die stroom of data doorsturen en beschermen tegen onderschepping, interferentie of schade. Er moet bijvoorbeeld rekening gehouden worden met ondergrondse kabels en kabelgoten. Het labelen van kabels aan beide uiteindes zorgt voor een snelle fysieke identificatie en inspectie van de kabels. Het scheiden van stroomkabels van communicatiekabels is ook een goede manier om interferentie te voorkomen.
- **Bescherming tegen stroomstoringen**: Het is ook belangrijk om te zorgen voor een betrouwbare stroomvoorziening voor de camera's. Dit kan worden bereikt door gebruik te maken van batterijen, zonne-energie of een back-upgenerator om te voorkomen dat de camera's uitvallen tijdens een stroomstoring.
- **Bescherming tegen diefstal**: schrik vandalisme of diefstal af door bv. geëlektrificeerd hekwerk (met bijhorende waarschuwing), prikkeldraad of bewegingssensoren verbonden met een alarm of verklikker licht, te plaatsen. Indien de camera geen beelden registreert zoals een normale camera, kan het aangewezen zijn om een bijkomende camera te installeren. Denk bijvoorbeeld aan de frequent voorkomende combinatie van een ANPR camera en een 360° camera.

Er zijn tot slot nog andere functionele overwegingen die in acht dienen genomen te worden.

5.2 Overwegingen omtrent plaatsing en verwijdering

Om de veiligheid en privacy van mensen te waarborgen bij het plaatsen en verwijderen van camerasystemen, is het belangrijk om stil te staan waarvoor de camera's gebruikt zullen worden en waar ze geplaatst zullen worden. Zo zijn er ook beperkingen daaromtrent: er mag bijvoorbeeld geen heimelijk gebruik plaatsvinden en mogen beelden de privacy van personen niet schenden, zoals in kleedkamers, toiletten en douchekamers. Er bestaan ook vereisten voor het plaatsen van camera's, die afhankelijk zijn van de locatie en het doel van de camera's. Raadpleeg hiervoor relevante wet- en regelgeving zoals de algemene verordening gegevensbescherming en de camerawet.

Verder staat het lokaal bestuur ook best stil bij de ruimte(s) waarin de beelden van de systemen zal/zullen geraadpleegd worden. Deze locaties zijn idealiter afgesloten van het publiek of de beeldschermen zijn moeilijk/onmogelijk te bezichtigen door derden. Dit kan bijvoorbeeld door het scherm weg te draaien van onbevoegden of een privacy filter te gebruiken op het scherm.

Elke gebruiker moet op de hoogte gebracht worden van zijn/haar verantwoordelijkheden voor het beschermen van zijn/haar toestel wanneer het onbeheerd achtergelaten wordt. Wanneer dat toestel niet actief gebruikt wordt, moet het worden beschermd door een automatische vergrendeling en een wachtwoord. Het ontgrendelen/heractiveren dient te gebeuren door middel van gebruikersidentificatie en authenticatie. Dat wil zeggen dat gebruikers:

- Hun actieve sessies volledig afsluiten of vergrendelen wanneer ze het camerasysteem onbeheerd achterlaten of op het einde van hun werk/taken.
- Zichzelf afmelden op applicaties of netwerkdiensten wanneer ze deze applicaties/diensten niet meer nodig hebben.

Verder moet er rekening gehouden worden met het transport van apparatuur zoals camera's, servers en fysieke back-ups. Het is van belang dat deze via veilige kanalen en de daarvoor bestemde diensten worden vervoerd om diefstal of verlies te voorkomen. Waar mogelijk past het lokaal bestuur beveiligingsmaatregelen toe om de hardware te beschermen bij transport.

5.3 Fysieke toegang

Daarnaast is het ook essentieel om beveiligde gebieden te beschermen door middel van passende toegangscontroles om ongeoorloofde toegang tot camerasystemen te voorkomen. Enerzijds houdt dit in dat de ruimtes waarin de camerabeelden te raadplegen zijn of waarin het lokale bestuur werkt, beveiligd zijn tegen ongeautoriseerde toegang. Zo zijn er ruimtes die voor het publiek toegankelijk dienen te zijn en ruimtes dat dit niet zijn.

Voor niet publieke ruimtes moet het lokaal bestuur ervoor zorgen dat toegangscontroles aanwezig zijn die daarover waken. Enkele voorbeelden zijn: het afsluiten van lokalen door middel van een (beveiligde) sleutel (of code), gebruik van badgesystemen, controle door een bewakingsagent, enz.

Daarnaast moet een onderscheid gemaakt worden in ruimtes waarin alle medewerkers van het lokaal bestuur mogen komen en meer besloten ruimtes zoals de serverruimte. De toegang tot deze ruimte dient beperkt te worden tot enkel de mensen voor wie toegang noodzakelijk is.

Beveiliging van data- of serverruimtes

Daarnaast dient de infrastructuur waarop camerasystemen draaien in deze ruimte, ook beschermd te worden tegen omgevingsfactoren. Hiervoor dient het volgende minstens aanwezig te zijn:

- Brand-, vocht- en temperatuurmelders om over omgevingsfactoren te waken zodat de werking van infrastructuur geen hinder ondervindt.
- Er moet een geschikte energiebron zijn die voldoet aan de specificaties van de leverancier van de apparatuur.
- Ter ondersteuning van bedrijfskritische activiteiten die camerasystemen ondersteunen, dient een niet-verstoorbare energiebron (Uninterruptible Power Supply (UPS)) en/of één of meerdere stroomaggregaten te worden geïnstalleerd. De werking en capaciteit hiervan dient regelmatig gecontroleerd en getest te worden om na te gaan of dit nog in lijn ligt met de vooropgestelde vereisten, liefst door de leverancier.
- Ondersteunende voorzieningen moeten regelmatig geïnspecteerd en getest worden om de goede werking daarvan te garanderen en het risico op storingen te verminderen. Wanneer dit door een leverancier gebeurt, dient de medewerker van deze derde partij ten allen tijde vergezeld te worden door een medewerker van het lokaal bestuur.

Verder dient apparatuur correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen. Dit gebeurt volgens de onderhoudsintervallen en specificaties van de leverancier. Tevens mogen herstellingen aan en onderhoud van apparatuur alleen uitgevoerd worden door bevoegd onderhoudspersoneel.

Om te voorkomen dat er geknoeid wordt met apparatuur in beveiligde ruimtes kan er gebruik worden gemaakt van een (combinatie van) bepaalde beveiligingssystemen (ook wel Physical Intrusion Detection Systems (PIDS)) zoals cameratoezicht, bewegingssensoren, sensoren die het breken van glas opmerken, enz. en die bij detectie het relevant beveiligingspersoneel op de hoogte brengen.

6. Operationele overwegingen omtrent beveiliging

6.1 Cryptografische maatregelen

Het is van groot belang om informatie te versleutelen wanneer deze verstuurd op opgeslagen wordt. Hierbij dient rekening te worden gehouden met het vereiste niveau van beveiliging en classificatie van informatie om het type, de sterkte en kwaliteit van de cryptografische algoritmes te bepalen.

De vereisten voor de cryptografische maatregelen moeten bepaald worden op basis van een risicobeoordeling die periodiek herhaald wordt. Let bovendien op voor (inter)nationale wetgeving of restricties die van toepassing zijn voor het gebruik van encryptie. Door het ontwikkelen en implementeren van een dergelijk beleid en het toepassen van passende cryptografische maatregelen, kan de vertrouwelijkheid, integriteit en beschikbaarheid van gevoelige informatie worden gewaarborgd. De Vlaamse Overheid voorziet in haar minimale normen ook aanbevelingen rond cryptografie. Om deze te waarborgen dient ten minste het volgende aanwezig te zijn:

- **Versleuteling van gegevens in rust**: camerasystemen moeten versleuteling gebruiken om opgeslagen gegevens, zoals videobeelden, te beschermen tegen ongeoorloofde toegang. Dit kan worden bereikt met behulp van symmetrische of asymmetrische versleutelingsalgoritmen, afhankelijk van de specifieke use case.
- **Versleuteling van gegevens tijdens verzending**: camerasystemen moeten versleuteling gebruiken om gegevens te beschermen die worden verzonden via netwerken of andere communicatiekanalen, zoals videofeeds of besturingssignalen. Dit kan worden bereikt met behulp van protocollen zoals SSL/TLS of IPsec. Hierbij wordt snelheid verkozen boven langdurige beveiliging door de grote hoeveelheid van data die getransporteerd wordt.
- **Veilig sleutelbeheer**: camerasystemen moeten veilige sleutelbeheerpraktijken gebruiken om coderingssleutels te beschermen tegen ongeoorloofde toegang of openbaarmaking. Dit kan mee opgenomen worden in bestaande richtlijnen.

Daarnaast kan het gebruik van cryptografische maatregelen ook de onweerlegbaarheid van camerabeelden waarborgen, zodat de beelden ook als bewijstukken kunnen gebruikt worden.

6.2 Malwarebescherming

Voorzie camerasystemen van anti-malware oplossingen. Waar het niet mogelijk is om een dergelijke oplossing op het toestel te installeren, moet het lokaal bestuur voorzien dat een anti-malware oplossing aanwezig is op de grens van het netwerksegment waarin dat de camera's of het camerasysteem geplaats wordt.

Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers. Het gebruik van enkel een anti-malware oplossing voor het opsporen en blokkeren van malware is meestal niet voldoende. Een lokaal bestuur dient ten minste de volgende overwegingen in acht te nemen:

- Stel regels en procedures op die het gebruik van ongeautoriseerde software voorkomen op infrastructuur waar de camerasystemen op draaien (Bv. voordat nieuwe en niet-gekende software mag geïnstalleerd worden, moet het hoofd van het team ICT hier eerst goedkeuring voor geven).
- Valideer regelmatig of de aanwezige software is goedgekeurd en verwijder niet-toegestane software. Dit kan tegelijkertijd gedaan worden met het actueel houden van het overzicht van bedrijfsmiddelen.
- In de verschillende lagen van de gehele keten binnen de ICT-infrastructuur waar de camera's of camerasystemen gebruik van maken, dient antivirus en anti-malware software aanwezig te zijn.
- Bescherming tegen malware, virussen en Trojaanse paarden dient toegepast en geplaatst te worden op alle communicatie van en naar het camerasysteem (en andere systemen).
- Voer regelmatig een volledige scan uit van de camerasystemen om naar virussen, Trojaanse paarden en andere malware te speuren.
- Realtime scans, zoals on-access en runtime scans, moeten uitgevoerd worden om virussen, Trojaanse paarden en andere malware op het camerasysteem te identificeren. Zorg daarvoor dat de malwaredefinities en oplossingen om malware te scannen geregeld worden bijgewerkt.
- Voorzie een bedrijfscontinuïteitsbeheersplan en herstellingsprocedures om voorbereid te zijn op de situatie waar het (camera)systeem de organisatie slachtoffer is van malware. Voorzie hierbij dat deze maatregelen aansluiten op de reeds bestaande procedures voor het beheer van incidenten binnen het lokaal bestuur.
- Zorg dat de gebruikers van de camerasystemen de nodige gedragscode en training krijgen omtrent het herkennen van cyberdreigingen zoals malware om het niveau van bewustzijn en weerbaarheid te verhogen.
- Zorg ervoor dat de beheerders van het camerasysteem op de hoogte blijven van nieuwe ontwikkelingen inzake mogelijke cyberdreigingen voor de systemen in kwestie. Voorzie hiervoor de nodige acties zodat een lokaal bestuur op de hoogte is van cyberdreigingen. Dit kan door in te schrijven op bronnen die periodiek nieuwe cyberdreigingen communiceren.

7. Beheer & onderhoud van camerasystemen

7.1 Aankoop software/systemen

Voor de aankoop van camera's of een camerasysteem moet het lokale bestuur functionele, technische, beveiligings- en privacy vereisten definiëren en opnemen in de aanbesteding. Bij het opmaken van deze vereisten moet er rekening worden gehouden met de doeleinden waarvoor de camera's worden gebruikt.

Enkele voorbeelden zijn:

- **Functionele vereisten**: het registreren van geluid, de camera moet kunnen bewegen, de camera moet vanop afstand aangestuurd kunnen worden, enz.
- **Technische vereisten**: een hoge resolutie is nodig wanneer beelden in detail moeten worden vastgelegd (zoals een nummerplaat of het duidelijk identificeren van een persoon), terwijl een lage resolutie volstaat wanneer er geen noodzaak is voor gedetailleerde beelden (zoals het tellen van het aantal voertuigen of personen in een bepaalde straat). Daarnaast kan er een verlichtingsplan worden voorzien, bijvoorbeeld door gebruik te maken van straatverlichting, verlichting op de camera's zelf te installeren of infraroodverlichting te gebruiken.
- **Beveiligingsvereisten**: ondersteunen van bepaalde encryptiestandaarden en veilige netwerkprotocollen, aanwezigheid van logfunctionaliteiten, enz.
- **Privacy vereisten**: informatie kan automatisch gewist worden, personen moeten onherkenbaar gemaakt worden d.m.v. blurring, enz.

7.2 Installatie software/systemen

Als lokaal bestuur is het belangrijk om voorafgaand de installatie van een camerasysteem minstens de volgende activiteiten uit te voeren:

- Het uitvoeren van een risicoanalyse op het op alle nieuwe software en systemen die het lokaal bestuur installeert. Hierdoor kan de impact op de informatieveiligheid ingeschat worden en kunnen passende maatregelen genomen worden om de veiligheid te waarborgen.
- Installeer nieuwe software/systemen pas na uitgebreide en succesvolle testen. Door het uitvoeren van testen kan een lokaal bestuur de kans op onverwachte problemen aanzienlijk verkleinen.
- Bij het uitvoeren van installaties moet ook altijd het proces van wijzigingsbeheer worden gevolgd.

Wanneer een lokaal bestuur besluit om de installatie door derden (de leverancier) te laten uitvoeren, is het belangrijk dat alle vereiste procedures worden gevolgd. Bovendien moeten de activiteiten van de leverancier of aanbieder worden gecontroleerd en gemonitord. Dit kan bereikt worden door middel van:

- Logging van activiteiten van leveranciers, haar medewerkers en controle hierop
- Adequate Service Level Agreements (SLA's)
- Regelmatige rapportage over de activiteiten
- Periodieke audits van derde partij of opvragen van de nodige certificeringen die de leverancier behaalde.

7.3 Wijzigingsbeheer

In het geval van wijzigingen, moet een lokaal bestuur procedures voor wijzigingsbeheer opstellen. Hiervoor reikt Digitaal Vlaanderen bijvoorbeeld het volgende proces aan. Een wijzigingsbeheersproces helpt om veranderingen in een lokaal bestuur op een gecontroleerde en gestructureerde manier door te voeren, met als resultaat een vermindering van risico's. Voor camera's of camerasystemen raden we aan dat het lokaal bestuur ook dezelfde processen hanteert voor wijzigingsbeheer als ze reeds documenteerde. Doorgaans wil dit zeggen vooraleer wijzigingen worden geïmplementeerd, het eerst de volgende stappen doorloopt:

1. **Aanvraag van de wijziging**
   Een gebruiker vraagt een wijziging aan het camerasysteem aan.

2. **Analyse & goedkeuring aanvraag**
   De verantwoordelijke voor het camerasysteem en team ICT analyseren het verzoek, gaan mogelijke risico's na, keuren het verzoek goed of wijzen het af. In de analyse van de wijziging staat het lokaal bestuur stil bij de impact die de wijziging heeft op het camerasysteem en de beveiligingsmaatregelen ervan. Daarnaast kennen ze een prioriteit aan het verzoek toe, op basis van de impact en urgentie van de wijziging.

3. **Ontwikkeling van de wijziging**
   Het team ICT werkt de wijziging uit en ontwikkelt de nodige wijzigingspakketten. Voordat wijzigingen worden doorgevoerd moet een plan zijn uitgewerkt om terug te keren naar de initiële status (rollback strategie). Dit laat toe om snel en effectieve terug te keren naar een werkende omgeving in het geval dat er zich fouten tijdens de implementatie van wijzigingen.

4. **Testen van de wijziging(en)**
   Om na te gaan of de wijziging het verhoopte resultaat heeft, test het lokaal bestuur de wijziging eerst (zowel functioneel, technisch als op het vlak van veiligheid & privacy). Hiervoor worden testscenario's opgesteld in samenwerking met de verantwoordelijke voor het camerasysteem en worden deze uitgevoerd.

5. **Implementatie**
   De organisatie implementeert de wijziging. Naargelang impact van de wijziging op het systeem, kan dit al dan niet tijdens de werkuren gedaan worden. Het moment van uitvoeren moet ook met de toepassingsverantwoordelijke worden afgestemd.

6. **Eindvalidatie**
   Doorheen de eindvalidatie werk het lokaal bestuur haar nodige documentatie bij, inclusief de bedrijfscontinuïteitsbeheersplannen.

Indien een lokaal bestuur haar wijzigingen laat uitvoeren door een derde partij (zoals de leverancier, aanbieder of andere entiteit), moet ze zien dat dit volgens haar vereisten verloopt. Daarbij waakt het lokaal bestuur over: de prestatieniveaus van de dienstverlening, de wijzigingen die werden doorgevoerd (aan bestaande diensten, nieuwe systemen of camera's, netwerken, enz.) of aanpassingen aan beveiligingsmaatregelen die betrekking hebben op het beheer van incidenten of bedrijfscontinuïteitsbeheer.

Bij het doorvoeren van wijzigingen is het van groot belang dat een lokaal bestuur gaat controleren of er een negatieve impact is op de beveiligingsmaatregelen. Daarom wordt het aangeraden om gebruik te maken van een testomgeving, zonder dat productiegegevens worden gebruikt in de testomgeving. Om te voorkomen dat er productiegegevens gebruikt worden in een testomgeving, kan een lokaal bestuur verschillende maatregelen nemen zoals data masking of dummy data. Op deze manier worden wijzigingen op een veilige en gecontroleerde manier doorgevoerd.

Opgelet!
Wijzigingen aan "kant en klare" camerasystemen die aangekocht of gehuurd worden, moeten beperkt worden tot hoogstnoodzakelijke wijzigingen en dienen enkel uitgevoerd te worden als het bijhorende risico beperkt is. Idealiter worden wijzigingen aan camerasystemen van een derde partij, door de derde partij zelf uitgevoerd.

7.4 Beperken van niet-noodzakelijke functionaliteiten

Camerasystemen dienen geen functionaliteiten te bevatten die niet noodzakelijk zijn (bv. onbeperkte bewegingsmogelijkheden van camera's, zoomfunctie, radioverzending, analysefuncties en geluidsopnamen). Het lokaal bestuur gaat daarom na welke functionaliteiten aanwezig, maar niet noodzakelijk, zijn en schakelt deze uit. Elke niet noodzakelijke functionaliteit brengt een risico met zich mee dat uitgebuit zou kunnen worden of in strijd is met bestaande wet- of regelgeving. Neem daarom een goed onderbouwde beslissing.

7.5 Beheer van kwetsbaarheden

Door kwetsbaarheden in software, systemen en camera's te identificeren en te beheren, kan een lokaal bestuur haar beveiligingsrisico's verminderen. Het beheer van kwetsbaarheden omvat het identificeren en prioriteren van kwetsbaarheden, het implementeren van passende beveiligingsmaatregelen en het monitoren en bijwerken van systemen om ervoor te zorgen dat ze veilig blijven. Om wijzigingen door te voeren die kwestbaarheden verhelpen, dient het wijzigingsbeheersproces van het lokaal bestuur gehanteerd te worden.

Om kwestbaarheden te verhelpen, dienen ze eerst geïdentificeerd te worden. Stel hiervoor een procedure die beschrijft hoe het lokaal bestuur kwetsbaarheden zal opsporen in de gebruikte producten en systemen en pas deze toe. Het overzicht van de bedrijfsmiddelen is tevens ook een eerste vereiste voor het goed beheer van kwetsbaarheden. Daarmee kan het lokaal bestuur nagaan welke camerasystemen in haar bezit zijn maar ook op welke versie zij bijvoorbeeld draaien. Het periodiek uitvoeren van (geautomatiseerde) scans naar kwetsbaarheden door gebruikt te maken van een daarvoor voorziene oplossing is hier al een eerste stap. Daarnaast kan het lokaal bestuur doorgaans ook intekenen op een distributielijst van haar leverancier waarmee het lokaal bestuur verwittigd wordt van nieuwe updates of bestaande kwetsbaarheden.

Zorg ook dat medewerkers die kwetsbaarheden aantreffen, deze kunnen melden op een centraal meldpunt. Daarnaast kan het lokaal bestuur ook toestaan dat ethische hackers naar kwetsbaarheden speuren en deze melden. Daarvoor kan gebruik gemaakt worden van responsible disclosure of beleid voor de gecoördineerde bekendmaking van kwetsbaarheden. Zo creëer je een kader voor ethische hackers die het lokaal bestuur willen helpen om kwetsbaarheden op te sporen en aan te pakken.
Wanneer een relevante nieuwe kwetsbaarheid aan het camerasysteem gesignaleerd wordt, dient tijdig actie te worden ondernomen om het bijbehorende risico te mitigeren. Om te bepalen hoe en wanneer de kwetsbaarheid moet worden gemitigeerd, moeten de betrokken medewerkers een risico-inschatting maken op basis van het belang van de informatie of camerasysteem, de impact van de kwetsbaarheid, het risico op misbruik en eventuele bestaande beveiligingsmaatregelen. Zo implementeert het lokaal bestuur bijvoorbeeld patches voor kritieke kwetsbaarheden best nog de dag zelf waarop het deze identificeerde. Voor updates die eerder functioneel of minder urgent zijn, kan de organisatie de nodige tijd nemen om haar proces met bijvoorbeeld teststappen, te doorlopen. Om updates te implementeren die kwetsbaarheden verhelpen, maakt het lokaal bestuur gebruik van haar stappenplan voor wijzigingsbeheer.

Als het lokaal bestuur koos voor een derde partij (zoals de leverancier of andere dienstverlener) om kwetsbaarheden te verhelpen, dient dit te gebeuren via veilige en daarvoor bestemde kanalen. Derde partijen dienen op voorhand aan te geven op welke tijdstippen de updates plaatsvinden. Op deze manier kan een lokaal bestuur garanderen dat de camerabewakingssystemen up-to-date blijven en optimaal functioneren.

Indien de opslag van data en het beheer van kwetsbaarheden deel uit maken van de verantwoordelijkheden van de leverancier (zoals bij outsourcing of cloudoplossingen), dan moet dit deel uitmaken van de periodieke gesprekken om het niveau van dienstverlening na te gaan (SLAs). Maak daarnaast afspraken met de leverancier van het systeem en/of andere derde partijen om geïnformeerd te worden wanneer zij kwetsbaarheden in het systeem aantreffen en hoe zij deze behandelen.

Wanneer camerasystemen en producten die niet meer ondersteund worden door de leverancier dienen zo spoedig mogelijk te worden vervangen aangezien de kwetsbaarheden in het systeem niet meer verholpen kunnen worden.

Om te valideren dat de kwetsbaarheid daadwerkelijk verholpen is, voert het lokaal bestuur best periodieke penetratietest uit op haar camerasysteem. Dat kan eventueel met een derde partij. Daarbij dienen de nodige maatregelen in acht te worden genomen (zoals het gebruik van een geheimhoudingsovereenkomst & maatregelen voor toezicht & bewaking)

8. Logging & monitoring

8.1 Gebeurtenissen registreren

Om goed toezicht te kunnen uitoefenen op haar omgeving, dient een lokaal bestuur te beginnen met het bepalen welke logs ze wil capteren, om dit nadien uit te voeren. Doorgaans bevat dit logbestanden van gebeurtenissen met betrekking tot gebruikersactiviteiten, uitzonderingen en gebeurtenissen m.b.t. informatieveiligheid.

Enkele voorbeelden van dergelijke vereisten zijn: de unieke gebruikersnaam, activiteiten van het camerasysteem, het IP-adres, gebruikte netwerkprotocol, capaciteit van opslag of netwerk, wijzigingen aan de configuratie van het systeem, gebruik van speciale accounts of ondersteunende toepassingen, handelingen door gebruikers, etc.

Daarnaast is het van groot belang dat deze logs op een veilige manier bewaard worden en regelmatig worden beoordeeld. Daarbij dient een onderscheid gemaakt te worden tussen wat het lokaal bestuur vast legt met betrekking tot de beschikbaarheid (bijvoorbeeld prestatieniveau of geheugencapaciteit) van het camerasysteem en wat wordt vastgelegd met betrekking tot vertrouwelijkheid en integriteit (bijvoorbeeld toegang tot of het wijzigen van informatie) voor de camerasystemen.

Een monitoringoplossing moet voorzien worden om tijdig en snel problemen met camera's of camerasystemen te identificeren. Dit is van toepassing op abnormale gedragingen van het camerasysteem en mogelijke beveiligingsincidenten, maar ook op de opslagcapaciteit die beschikbaar is voor het camerasysteem. De monitoroplossing moet in dat laatste geval voorzien zijn van een alarm (e.g. notificatie systeem) dat waarschuwt wanneer de maximumcapaciteit kan worden voorzien. Soms zit deze functionaliteit al deels verwerkt in het camerasysteem zelf. Andere keren dienen de logs van het camerasysteem in een monitoringoplossing van het lokale bestuur te worden opgenomen.

Wanneer die monitoroplossing een incident detecteert, moeten de relevante personen op de hoogte worden gesteld. Om dit correct en efficiënt te onderzoeken en op te lossen moet een lokaal bestuur over een duidelijk plan beschikken opdat de impact van een incident geminimaliseerd wordt. De logs die de monitoroplossing verzamelt, spelen een belangrijke rol bij het onderzoeken van incidenten en het identificeren van de oorzaak. Het is daarom van cruciaal belang dat deze logs beschermd worden en dat het lokaal bestuur daarnaast regelmatig controleert of deze logs nog steeds beschikbaar en integer zijn.

8.2 Beheren van logging

Om gebeurtenissen en potentiële incidenten te identificeren, heeft het lokaal bestuur haar logs nodig waaruit het deze kan opmerken. Daarom moet het lokaal bestuur geregeld haar logs herzien en rapporteren over de patronen of anomalieën dat het opmerkt. Enkele voorbeelden zijn: onverwachte gedragingen van gebruikers die meermaals foutief aanmeldden, plotse grote hoeveelheden van bestanden die van naam veranderen, een grote hoeveelheid van informatie die verzonden wordt, het gebruik van bepaalde protocollen die afwijken van de norm, enz. De termijn voor de rapportering en het herzien van logs moet afhangen van het risico op misbruik en de schade van het camerasysteem.

Naast het rapporteren en het herzien van logs, is het ook belangrijk om effectieve maatregelen te implementeren om de integriteit van de logs te garanderen. Dit kan onder meer betrekking hebben op het beperken van toegang tot logs of indien gewenst, de implementatie van een Security Incident and Event Management (SIEM) systeem. Andere praktische voorbeelden zijn:

- Pas encryptie toe om ervoor te zorgen dat onbevoegden de informatie niet kunnen raadplegen of aanpassen;
- Hash logs door het toepassen van een algoritme, opdat er gecontroleerd kan worden of logs ongewijzigd blijven. Dit is als het ware een digitale vingerafdruk bestaande uit een reeks letters en cijfers die uniek zijn voor de specifieke set gegevens. Wanneer de inhoud wordt aangepast, zal de hash eveneens veranderen;
- Kopieer logbestanden automatisch naar een locatie waar gebruikers geen (logische en fysieke) toegang hebben;
- Wijzigingen aan de instellingen van het logmechanisme moeten het wijzigingsbeheerproces van het lokaal bestuur volgen (proces van aanvraag, goedkeuring en uitvoering);
- Maak regelmatig back-ups en sla deze op een veilige locatie op opdat logs niet verloren gaan ten gevolge van bijvoorbeeld een storing of cyberaanval.

Bovendien is het van belang om de logs van camerasystemen te bewaren zo lang als wettelijk vereist is. Indien een verplichte opslagtermijn ontbreekt, kan het lokaal bestuur een eigen opslagtermijn hanteren voor beheersactiviteiten. Net als de opslagcapaciteit voor camerabeelden, dient de opslagcapaciteit voor logbestanden te worden bewaakt. Wanneer een bepaalde limiet bereikt wordt of wanneer opslag niet mogelijk is, moet er een automatisch alarm afgaan.

9. Beheer van leveranciers

9.1 Beveiligingsvereisten in overeenkomsten & toeleveringsketen

Als het lokale bestuur besluit om het gebruik en de opvolging van camerasystemen uit te besteden, moet de leverancier zorgvuldig worden geselecteerd. Daarbij maakt het lokaal bestuur individuele afspraken met haar derde partij om te voorkomen dat misverstanden ontstaan over de rollen en verantwoordelijkheden die aanwezig zijn om informatiebeveiliging te waarborgen. Sta tevens stil bij de nauwkeurigheid en volledigheid van de beveiligingsmaatregelen die de potentiële leverancier voorstelt om de betrouwbaarheid, beschikbaarheid en integriteit van de informatie uit camerasystemen te waarborgen. Daarnaast moet ook een verwerkingsovereenskomst met de leverancier en alle relevante partijen afgesloten worden. Hiervoor voorziet de VVSG ook reeds een leidraad.

Gebruik onderstaande opsomming als leidraad:

- Controleer de reputatie en achtergrond van potentiële leveranciers om te bepalen of ze betrouwbaar en veilig zijn.
- Kies camerasystemen die de minstens de maatregelen uit deze beveiligingsrichtlijn ondersteunen, inclusief;
    - Toegangscontroles;
    - Het beheer van incidenten;
    - Behandeling van informatie;
    - Naleving van wetgeving/privacy vereisten;
    - Recht op audit;
    - Contactpersonen;
    - Achtergrondonderzoek naar de integriteit van medewerkers, zie daarvoor ook de vereisten uit Arbeidsovereenkomstenwet van 3 juli 1978
    - Onderhoudsvoorwaarden (overeenkomstig met richtlijnen van producent);
    - Transport van camera's en camerasystemen en garantie op informatieveiligheid tijdens transport;
    - Volgen van informatieclassificatieschema;
    - Opvolgen van ondersteuningsvoorwaarden vanuit de leverancier (beheer van incidenten en kwetsbaarheden, opvolging van naleving, continuïteitsbeheer en herstelactiviteiten);
    - Verplichtingen van de leverancier om periodiek een onafhankelijk rapport af te leveren.
- Vereis dat de data uit camera's en bijbehorende systemen nooit de Europese Economische Ruimte (EER) verlaat.
- Overweeg of de aankoop van camera's en camerasysteem in eenzelfde pakket interessanter is en meer aansluit bij de behoeften van het lokale bestuur.

Bij de aankoop van een product of dienst moeten overeenkomsten worden afgesloten waarin de rollen en verantwoordelijkheden (zoals patch- en VM-beheer, SOC, enz.) en

vertrouwelijkheidskwesties worden vastgelegd. Bij het uitwisselen van informatie met derde partijen met betrekking tot applicatiediensten is het belangrijk om extra voorzichtig te zijn bij het gebruik van openbare netwerken en om te zorgen dat de uitwisseling van informatie op een veilige manier plaatsvindt om te beschermen tegen frauduleuze activiteiten, contractgeschillen en ongeoorloofde bekendmaking.

Opgelet!
Wanneer onderaannemers gebruikt worden, dient de derde partij de nodige veiligheidsvereisten van het lokale bestuur af te dwingen ten aanzien van de onderaannemer. De onderaannemers moeten voorafgaandelijk bekend worden gemaakt aan het lokale bestuur zodat dit meegenomen kan worden in de risicoanalyse betreffende informatieveiligheid.

9.2 Opvolging van dienstverlening

Dankzij duidelijke afspraken kan een lokaal bestuur de dienstverlening van derde partijen monitoren, beoordelen en auditeren. Deze afspraken worden vastgelegd in een SLA die onder andere afspraken bevatten omtrent de beschikbaarheid van de dienstverlening, reactietijd bij storingen en de verantwoordelijkheden van de derde partij.

Voor het opvolgen van de dienstverlening kan een lokaal bestuur gebruik maken van verschillende methoden, zoals het regelmatig uitvoeren van audits, het opstellen van prestatie-indicatoren of het periodiek evalueren van de dienstverlening.

Via audits kan het lokale bestuur controleren of de derde partij voldoet aan de gestelde eisen en of de afspraken uit de SLA worden nageleefd. Zo kan een lokaal bestuur bijvoorbeeld toegang krijgen tot onderhoudsrapporten voor de camera’s en systemen. Door middel van prestatie-indicatorenkunnen de prestaties van de derde partij worden gemeten en geëvalueerd of deze voldoen aan de gestelde eisen.

Daarnaast is het van groot belang dat een lokaal bestuur regelmatig contact heeft met de derde partij (leverancier) en dat de communicatie vlot verloopt tussen beiden. Op deze manier kan er snel worden ingespeeld op eventuele problemen en kan de dienstverlening zo optimaal mogelijk worden gehouden. Dit geldt eveneens voor wijzigingen die bij een derde partij kunnen optreden.

In de SLA kunnen bijvoorbeeld afspraken worden gemaakt over de frequentie en inhoud van rapportage over wijzigingen en updates aan de systemen of diensten die geleverd worden. Een lokaal bestuur kan zelf ook proactief informatie opvragen bij de derde partij over wijzigingen en updates of kan dit opvragen tijdens een audit. Dit is echter niet beperkt tot softwarematige wijzigingen, maar ook betreffende beveiligingspraktijken en dienstverlening.

10. Opslag en back-up

Het beschermen van camerabeelden verschilt in essentie niet veel van het opslaan van andere vormen van informatie. De informatie moet veilig opgeslagen en beschermd worden tegen ongeautoriseerde toegang, wijziging of verwijdering gedurende hun hele levenscyclus. Het is belangrijk om te onthouden dat camerabeelden persoonlijke en gevoelige informatie kunnen bevatten en daarom moeten worden behandeld volgens de relevante wet- en regelgeving met betrekking tot de bescherming van persoonsgegevens.

10.1 Opslaan van informatie

Informatie kan niet voor een onbepaalde tijd worden opgeslagen omwille van 2 redenen:

- Enerzijds wordt vanuit bepaalde wet of regelgeving een beperking opgelegd m.b.t. bewaartermijnen (zoals bv. de AVG) en;
- Anderzijds is het vanuit een kosten-baten perspectief niet efficiënt om meer informatie op te slagen dan nodig, omwille van de bijkomende kosten.

Bepaal daarom in samenspraak met de DPO de retentieperiodes, die bepalen hoelang informatie opgeslagen mag worden, en stem dit ook af met de nodige diensten binnen het lokaal bestuur.

Wanneer het lokaal bestuur beslist om gebruik te maken van cloud-opslag zijn de retentieperiodes eveneens van toepassing. Wanneer het gebruik van cloud-opslag de voorkeur geniet, moeten minstens de volgende elementen in acht worden genomen:

- Definieer de rollen en verantwoordelijkheden voor zowel de cloud serviceprovider als voor het lokaal bestuur.
- Definieer en communiceer de verwachtingen voor informatiebeveiliging naar de cloud serviceprovider toe.
- De technische vereisten dienen te worden afgetoetst aan het advies verschaft doorde VTC: Advies uit eigen beweging VTC nr. 2022/02.
- Daarnaast heeft de VTC een beslissingsmatrix opgesteld voor het selecteren van cloud serviceproviders, raadpleeg deze in Advies VTC nr. 2020/05 pagina 10.

10.2 Back-up van informatie

In het kader van het beschikbaar houden van informatie of bedrijfscontinuïteit moet het lokaal bestuur periodiek back-ups maken. Hiervoor kan het lokaal bestuur gebruik maken van haar reeds bestaande beleidsrichtlijnen en procedures. Daarnaast bepaalt het lokaal bestuur vooraf de hersteltijddoelstelling (RTO) en herstelpuntdoelstelling (RPO) voor de uitvoering van haar back-ups. . RTO verwijst naar de maximale aanvaarde tijd dat een systeem of camera offline kan zijn bij een storing, terwijl de RPO doelt op het maximale toegestane verlies van data, uitgedrukt in een tijdspanne, in geval van een storing. Beide doelstellingen komen dienen tot stand te komen uit overleg tussen de medewerkers van de dienst ICT en de gebruikers van het camerasysteem. Zo kan een goed beeld gevormd worden van de noden en daar naar gehandeld worden.

Bewaar back-ups op een aparte opslagmedia die zich op een veilige en afgelegen locatie bevindt. Dit zorgt ervoor dat de back-ups geen schade oplopen door een calamiteit (e.g. malware aanval, brand, etc.), raadpleeg hiervoor de sectie ‘Fysieke Beveiliging’.

Bij het back-up beleid staat het **3-2-1 principe** voorop. Dit wil zeggen dat het lokaal bestuur ten minste 3 verschillende kopieën van de belangrijkste data uit het camerasysteem opslaat op minstens 2 verschillende opslagmedia en nog 1 versie op een aparte offline locatie. Hierbij kan eventueel ook nog een aparte kopie in een cloud omgeving aan toegevoegd worden, waar nodig.

Test periodiek de back-ups opdat een lokaal bestuur de camerasystemen zo spoedig mogelijk kan herstellen wanneer een calamiteit zich voordoet en laat het succes van deze testen ook valideren door gebruikers van het camerasysteem en bv. niet enkel door medewerkers van het ICT-team. Door het regelmatig testen van de back-ups kan een lokaal bestuur het verlies van data beperken tot een minimum. Wees ervan bewust dat ook back-ups de vastgelegde bewaartermijnen moeten respecteren.

Wanneer de back-up capaciteiten worden uitbesteed aan een opslagprovider, dient een lokaal bestuur deze vereisten mee op te nemen in de SLA. Deze dienen ten minste het volgende te bevatten:

- Monitoring op het herstel en de synchronisatie, waarbij fouten op korte termijn moeten gesignaleerd en verholpen worden;
- Periodieke rapportage van het back-up- en herstelproces met onder andere de beschikbare opslagcapaciteit en voorspelde groei;
- Logische toegang tot back-ups;
- Frequentie en tijden waarop back-ups moeten worden gemaakt en prestatieniveaus (de maximale tijd die nodig is om een back-up te maken en de maximale tijd die nodig is om een back-up te herstellen);
- Verantwoordelijkheden van alle partijen die betrokken zijn bij het back-upproces;
- Procedures voor het aanbrengen van wijzigingen in de SLA;
- Afhankelijk van het belang en de locatie van de gegevens moet een acceptabel niveau van encryptie worden toegepast op de reservekopieën.

10.3 Verwijderen van gegevens

Een beleid bevat steeds richtlijnen voor het veilig hergebruiken of verwijderen van opslagmedia. Na de wettelijk vereiste bewaarperiode moeten camerabeelden worden verwijderd om onnodige risico’s, kosten en inbreuken op wetgeving te vermijden. Wanneer een lokaal bestuur overgaat tot de verwijdering van informatie moet steeds rekening gehouden worden met de classificatie van de data.

Het is van essentieel belang dat de richtlijnen en/of controles voor het verwijderen van camerabeelden regelmatig geëvalueerd en bijgewerkt worden. Dit kan onder meer via periodieke controles om te bevestigen dat informatie permanent vernietigd is en dat er geen resterende informatie achterblijft.

11. Beheer van incidenten en continuïteitsbeheer

11.1 Incidentenbeheer

Een lokaal bestuur dient voorbereid te zijn op informatiebeveiligingsincidenten. Hierbij moet proactief worden stilgestaan bij de manier waarop ze dat zal doen en welke taken toegewezen en uitgevoerd worden. Hiervoor reikt de VVSG de volgende handvaten aan:

- Het draaiboek cybercrime: dit geeft een omvattende en pragmatische aanpak weer voor het bestrijden van cyberveiligheidsincidenten.

Voor de camerasystemen sluit het lokaal bestuur best aan op haar reeds bestaande processen zoals incident response. Voorzie minstens:

- Een manier waarop informatiebeveiligingsgebeurtenissen gemeld en beoordeeld kunnen worden. Dit omvat o.a. een contactpunt, een schaal om de impact en urgentie uniform te bepalen, een meldingsprocedure en escalatielijnen voor o.a. crisiscommunicatie. Neem ook het communiceren naar autoriteiten in acht: zo kan het zijn dat een lokaal bestuur naar autoriteiten (zoals de gegevensbeschermingsautoriteit (GBA), de Vlaamse toezichtcommissie (VTC) of het Centre For Cyber Security Belgium (CCB)) dient te communiceren bij een incident;
- Een checklist crisisbeheer;
- Rollen en verantwoordelijkheden om incidenten en calamiteiten te verhelpen. Hiervoor kan het lokaal bestuur ook een RACI matrix opstellen;
- Incidentenregister bijhouden voor raadpleging door DPO en correcte melding aan VTC binnen de 72 uur van incident;
- Het trekken van conclusies en leren uit ervaring na een incident.

11.2 Bedrijfscontinuïteitsbeheer

Daarnaast voorziet het lokaal bestuur ook de continuïteit van haar camerasystemen via haar bedrijfscontinuïteitsbeheersplan, als het een van de kritieke processen van de organisatie ondersteunt. Daarbij gaat het lokaal bestuur eerst haar kritieke processen in kaart brengen (via *business impact assessments of BIA's)*. De VVSG biedt reeds een sjabloon aan om deze BIA's uit te voeren en om tot een bedrijfscontinuïteitsbeheersplan te komen.

In een tweede stap gaat het lokaal bestuur na welke systemen deze processen ondersteunen. Indien een camerasysteem nodig is om een kritiek proces uit te voeren, gaat het lokaal bestuur na of er tekortkomingen zijn binnen de organisatie om de beschikbaarheid van camerasystemen te waarborgen, zoals het voorzien van redundante netwerkverbindingen en infrastructuur, noodstroomvoorziening, het simultaan wegschrijven van informatie naar 2 aparte opslaglocaties, enz.

Daarnaast voorziet het lokaal bestuur ook een alternatieve manier van werken om haar kritieke processen tijdelijk verder te zetten als het ondersteunende camerasysteem niet werkt omwille van een calamiteit. Een voorbeeld is om bijvoorbeeld een bewaker in de inkomhal van het gemeentehuis te plaatsen wanneer de camera's niet bruikbaar zijn om toezicht te houden. Tot slot hanteert het lokaal bestuur haar stappenplan om systemen en back-ups te herstellen om zo terug te keren naar een normale manier van werken.

12. Naleving wetgeving

Het gebruik van camera's en camerasystemen werpt vaak een legio aan vragen op. Zo worden er vragen gesteld rond de veiligheidsvereisten, zijn er vragen of camera's de meest gepast oplossing zijn, maar ook of er bepaalde wetgeving is die nageleefd dient te worden.

De wetgeving die van toepassing is op het plaatsen en gebruiken van camera's door lokale besturen bestaat enerzijds uit specifieke regelgeving voor camera's, namelijk de Wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's ("Camerawet"). Anderzijds is er de Algemene Verordening Gegevensbescherming ("AVG" of "GDPR") die van toepassing is op alle verwerkingen van persoonsgegevens, aangevuld door de adviezen en richtlijnen van de Vlaamse Toezichtscommissie ("VTC"), de autoriteit die bevoegd is voor verwerkingen van persoonsgegevens door lokale besturen. De Camerawet dient aanzien te worden als een bijzondere wet die voorrang heeft op de AVG en concrete invulling geeft aan een aantal principes en verplichtingen uit de AVG.

De volgende sectie licht enkele zaken toe die doorheen de aankoop en implementatie van een camerasysteem in acht dienen te worden. Let op: dit is geen exhaustieve opsomming. Deze richtlijn zal dus niet alle verplichtingen in het kader van de camerawetgeving en de AVG opsommen. Betrek doorheen dit proces ook de functionaris voor gegevensbescherming van het lokale bestuur, net als de juridische adviseur(s).

12.1 Camerawet

Wie een bewakingscamera installeert moet de wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's naleven en dient samen gelezen te worden met de Omzendbrief van 10/12/2009. De Camerawet is van toepassing op het gebruik van bewakingscamera's voor volgende doeleinden, nl. om misdrijven (artikel 3) en overlast (artikel 135 van de nieuwe gemeentewet) te voorkomen, vast te stellen of op te sporen, de naleving van gemeentelijke reglementen te controleren of de openbare orde te handhaven.

De Camerawet is van toepassing bij het gebruik van bewakingscamera's door lokale besturen, zowel wanneer ze gebruikt worden voor veiligheid, het bestrijden van overlast als voor het controleren van de gemeentelijke reglementen (parkeren, sluikstorten). De Camerawet is dus niet van toepassing wanneer lokale besturen de camera's gebruiken voor andere doeleinden.

De Camerawet legt bepaalde verplichtingen op bij het gebruik van beveiligingscamera's, afhankelijk van de plaats (niet-besloten, besloten publiek, besloten niet publiek) en het type camera (vast of mobiel). Daarnaast bevat de Camerawet onder andere regelgeving met betrekking tot het bekijken van de beelden in real-time en stelt duidelijke limieten aan het gebruik van ANPR camera's.

Plaatsen & soorten camera's

De Camerawet bevat specifieke regels afhankelijk van de plaats waar de camera's worden geplaatst en maakt een onderscheid tussen onderstaande plaatsen:

- **Niet-besloten plaats**: Elke plaats die niet door een omsluiting is afgebakend en vrij toegankelijk is voor het publiek, waaronder de openbare weg.
- **Publiek toegankelijke besloten plaats**: Elk gebouw of elke door een omsluiting afgebakende plaats bestemd voor het gebruik door het publiek waar diensten aan het publiek kunnen worden verstrekt.
- **Niet voor het publiek toegankelijke besloten plaats**: elk gebouw of elke door een omsluiting afgebakende plaats, die uitsluitend bestemd is voor het gebruik door de gewoonlijke gebruikers.

Voor meer details omtrent de soorten plaatsen, raadpleeg "Welke plaatsen?" van BeSafe.

Verder maakt de camerawet een onderscheid tussen de volgende soorten bewakingscamera's:

- **Vaste bewakingscamera's** die voor onbepaalde duur worden geplaatst op een locatie en worden vastgehecht zoals bewakingscamera's in de inkomhal van gebouwen of op straat voor algemeen toezicht.
- **Tijdelijk vaste bewakingscamera's** die voor een beperkte tijd op een plaats worden opgesteld met als doel hetzij een welbepaald evenement te bewaken, hetzij op regelmatige tijdstippen te worden verplaatst om op een andere plaats te worden opgesteld overeenkomstig de doeleinden die eraan werden toegewezen zoals camerabewaking tijdens muziek- of sportevenementen of kerstmarkten.
- **Mobiele bewakingscamera's** die tijdens de observatie worden verplaatst om vanaf verschillende plaatsen of posities te filmen camera's gemonteerd op rijdende voertuigen om overtredingen vast te stellen.

Beslissingsprocedure

Om camera's te plaatsen, dient een lokaal bestuur een beslissingsprocedure te doorlopen. Naargelang de plaats, verschilt deze procedure, nl.:

- Niet-besloten plaats:
  - Enkel overheden mogen camera's plaatsen op niet-besloten plaatsen;
  - De korpschef van de politie moet om advies gevraagd worden;
  - De gemeenteraad van het lokaal bestuur dient positief advies te geven (tenzij de camera's op een locatie geplaats worden die niet onder de bevoegdheid van de gemeente valt (bv. een openbare weg). Het positief advies van de gemeente is steeds beperkt in de tijd. De wet stelt geen minimum- of maximumtermijnen vast voor het advies. Bij het verstrijken van de periode moet om hernieuwing worden gevraagd;
  - In geval van tijdelijke bewaking, moeten bijzondere doeleinden worden toegelicht.
- Voor het publiek toegankelijke besloten plaats:
  - De verwerkingsverantwoordelijke beslist tot het plaatsen van camera's op voor het publiek toegankelijke besloten plaatsen. Het advies van de gemeenteraad of korpschef is niet vereist.
  - De verwerkingsverantwoordelijke is in de regel de eigenaar van de besloten plaats of de organisator van een evenement op de plaats.
- Niet voor het publiek toegankelijke besloten plaatsen:
  - De verwerkingsverantwoordelijke beslist tot het plaatsen van camera's.

Verwerkingsregister

De verwerkingsverantwoordelijke (overheid) houdt een register bij met de beeldverwerkingsactiviteiten van bewakingscamera's uitgevoerd onder zijn verantwoordelijkheid. Dit register bestaat in schriftelijke vorm, al dan niet elektronische vorm.

Het register bevat minstens volgende elementen:

1. De naam en de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de gezamenlijke verwerkingsverantwoordelijk, van de vertegenwoordiger van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming;
2. De verwerkingsdoeleinden;
3. Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens:
4. De categorieën van ontvangers van persoonsgegevens, onder meer ontvangers in derde landen of internationale organisaties;
5. In voorkomend geval, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de doorgiften bedoeld in artikel 49, paragraaf 1, tweede lid, van de algemene verordening gegevensbescherming, de documenten inzake de passende waarborgen;

6. De beoogde termijnen voor het wissen van de verschillende categorieën van gegevens, in het bijzonder de bewaartermijn van de gegevens, indien de beelden worden opgenomen;
7. Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 32, paragraaf 1, van de algemene verordening gegevensbescherming, waaronder de beveiligingsmaatregelen die worden genomen om de toegang te verhinderen door niet-gemachtigde personen en deze die worden genomen in het kader van de mededeling van gegevens aan derden.
8. De wettelijke basis voor de verwerking;
9. De vermelding van het type plaats;
10. De technische beschrijving van de bewakingscamera's en, indien het gaat om vaste bewakingscamera's, hun locatie, in voorkomend geval aangegeven op een plan;
11. Indien het gaat om tijdelijke of mobiele bewakingscamera's, de beschrijving van de zones die door deze bewakingscamera's worden bewaakt en de gebruiksperiodes.
12. De informatiewijze met betrekking tot de verwerking;
13. De plaats voor het verwerken van de beelden;
14. Het feit dat het bekijken in real-time al dan niet wordt georganiseerd en in voorkomend geval, de manier waarop dat wordt georganiseerd.
15. 15° Wanneer het gaat over de camerabewaking van een niet-besloten plaats of van bewakingscamera's gericht op de perimeter van een besloten plaats conform artikel 8/2 van de wet van 21 maart 2007, bevat het register eveneens, in voorkomend geval, het positief advies van de bevoegde gemeenteraad.

Melding aan politie

De plaatsing van een bewakingscamera dient te worden meegedeeld aan de politiediensten en dit uiterlijk de dag voor die waarop de bewakingscamera in gebruik wordt genomen. Elke aangifte dient tevens bepaalde elementen te bevatten. Daarnaast moet elke wijziging die wordt aangebracht aan de ingezette bewakingscamera’s eveneens gemeld te worden aan de politiediensten. Er dient tevens een jaarlijkse controle/check door de verwerkingsverantwoordelijke te gebeuren. Voor camera’s op niet voor het publiek toegankelijke besloten plaatsen is dit niet nodig wanneer de camera's door een natuurlijke persoon worden aangewend voor persoonlijk of huiselijk gebruik binnen een privéwoning

De aangifte van de plaatsing en het gebruik van een camerabewakingssysteem gebeurt op elektronische wijze via het centraal e-loket voor de aangifte van bewakingscamera's dat door de Federale Overheidsdienst Binnenlandse Zaken ter beschikking wordt gesteld: www.aangiftecamera.be

Toegang real-time beelden

Niet-besloten plaats: Het bekijken van de beelden in real-time is uitsluitend toegestaan onder toezicht van de politiediensten opdat de bevoegde diensten onmiddellijk kunnen ingrijpen bij misdrijf, schade, overlast of verstoring van de openbare orde en deze diensten in hun optreden optimaal kunnen worden gestuurd.

Besloten plaats: De camerawet voorziet voor besloten plaatsen toegankelijk voor het publiek die, door hun aard, een bijzonder veiligheidsrisico inhouden, de mogelijkheid om in real-time beelden over te dragen aan politiediensten. Hiervoor verwijzen we naar artikel 9,

derde lid, 3°, a), van de wet van de Camerawet. Kort samengevat zijn dit bv. luchthavens, internationale instellingen of ambassades, havenfaciliteiten of plaatsen waar evenementen worden georganiseerd. Daarnaast kan de verwerkingsverantwoordelijke, in de nabijheid van een bewakingscamera, een controlescherm plaatsen dat in real-time de beelden van die camera openbaar verspreidt. Het is een mogelijkheid maar geen verplichting.

Mobiele camera's gebruiksrestricties

Niet-besloten plaats: De mobiele bewakingscamera's mogen in niet-besloten plaatsen enkel gebruikt worden met het oog op de automatische nummerplaatherkenning, door of in opdracht van de gemeentelijke overheden en voor de volgende doeleinden:

7. Voorkomen, vaststellen of opsporen van overlast (Zie artikel 135 van de nieuwe gemeentewet);
8. Controleren van de naleving van de gemeentelijke reglementen inzake betalend parkeren.

Het gebruik van de mobiele bewakingscamera's, kan slechts worden toevertrouwd aan het bij wet aangewezen personeel om vaststellingsopdrachten uit te voeren, binnen hun bevoegdheidsgrenzen.

Besloten plaats: Mobiele camera's in besloten plaatsen zijn enkel toegelaten in volgende gevallen:

1. Het gebruik van mobiele bewakingscamera's (zie artikel 142 van de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid);
2. Het gebruik van mobiele bewakingscamera's op een besloten plaats, of gedeelten van deze besloten plaats, waar niemand wordt verondersteld aanwezig te zijn;
3. Het gebruik van mobiele bewakingscamera's door een natuurlijke persoon, voor persoonlijk of huiselijk gebruik, in een niet voor het publiek toegankelijke besloten plaats.

Pictogram

Artikel 8 van de Camerawet verbiedt het heimelijk gebruik van camera's. Heimelijk gebruik wil zeggen het gebruik van camera's zonder voorafgaandelijke toestemming van de gefilmde persoon.

De toestemming wordt volgens de Camerawet verkregen door een pictogram aan te brengen op de plaats (of het voertuig) waar de camera's zich bevinden. Als er gebruik gemaakt wordt van ANPR camera's dan moet dit uitdrukkelijk op het pictogram worden aangegeven. Een uitvoeringsbesluit legt een aantal vereisten op aan de pictogrammen (qua afmetingen, materiaal).

Bewaartermijnen

De bewaringstermijn is in principe 1 maand, tenzij de beelden dienstig zijn voor het bewijzen van een misdrijf, van schade of van overlast of tot het identificeren van een dader, een verstoorder van de openbare orde, een getuige of een slachtoffer. Echter kan deze bewaartermijn onder bepaalde voorwaarden verlengt worden naar 3 maanden, rekening houdend met de omgeving & risico's.

12.2 Algemene verordening gegevensbescherming (AVG)

Naast de camerawet zal ook de AVG moeten worden nageleefd. Wat volgt is een overzicht van de bepalingen van de AVG die toepasselijk zijn op het verwerken van persoonsgegevens via camera's.

Hiervoor is het identificeren van een duidelijke rechtsgrond primordiaal. Indien de camera's persoonsgegevens verwerken moet in een vroeg stadium één van de rechtsgronden uit de AVG worden gekozen als basis voor de verwerking. De keuze van de rechtsgrond heeft implicaties wat de verdere verplichtingen en (bv. toestemming verzamelen, Legitimate Interest Analysis) de rechten van de betrokkene betreft. Het doel van de verwerking (monitoren met camera's) moet op voorhand uitdrukkelijk bepaald worden. Stem dit ook steeds af met de DPO van het lokaal bestuur.

Toepassingsgebied

De AVG is van toepassing op elke verwerking van persoonsgegevens in de Europese Economische Zone en elke verwerking van persoonsgegevens van EU-burgers. De wetgeving is dus altijd van toepassing in de context van het gebruik van camera's door lokale besturen, tenzij er geen personen/persoonsgegevens mee worden gefilmd. De AVG en de Camerawet moeten, indien van toepassing, samen toegepast worden. De AVG bevat een lijst met algemene principes die op elke verwerking van persoonsgegevens van toepassing zijn.

Rechtmatigheid, behoorlijkheid en transparantie

Persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Dit houdt onder meer in dat de betrokkene behoorlijk geïnformeerd wordt over de (doeleinden van) de verwerking.

Doelbinding

Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd. Een verwerking van persoonsgegevens moet op een van de 6 rechtsgronden gebaseerd worden waarin de AVG voorziet als je persoonsgegevens wil verwerken. Raadpleeg de website van de gegevensbeschermingsautoriteit voor meer details. Neem contact op de DPO van uw lokaal bestuur om de toepasbare rechtsgrond vast te stellen.

Minimale gegevensverwerking

Persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.

Juistheid gegevens

De persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren.

Opslagbeperking

Persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt, mits de vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen.

Integriteit en vertrouwelijkheid

De persoonsgegevens moeten door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Verantwoordingsplicht

De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van de algemene principes en moet dat kunnen aantonen.

Rechtmatigheid van de verwerking

De verwerking is alleen rechtmatig indien en voor zover aan ten minste één van de onderstaande voorwaarden is voldaan:

a) De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden. Deze toestemming is strikt en het betreden van een plaats waar een camera hangt met een pictogram valt niet als een toestemming te aanzien onder de AVG;
b) De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
c) De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
d) De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
e) De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
f) De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Een overheid kan zich niet beroepen op haar gerechtvaardigd belang (punt f) in het kader van de uitoefening van haar taken.

Toestemming zal in de praktijk ook moeilijk zijn voor de overheid om als rechtsgrond te gebruiken, gezien de gezagsverhouding tussen de overheid en de burger, waardoor een burger moeilijk “vrij” zijn toestemming kan geven.

Rechten van betrokkene

Betrokkenen (gefilmde personen) hebben een aantal rechten met betrekking tot hun persoonsgegevens, afhankelijk van de rechtsgrond en het type verwerking. De besturen dienen te zorgen dat deze rechten worden nageleefd. In principe moet een vraag van een betrokkene tot uitoefening van zijn rechten binnen de maand behandeld worden.
De rechten van de betrokkene zijn de volgende:

- Recht op informatie;
- Recht op inzage;
- Recht op rectificatie;
- Recht op gegevenswissing;
- Recht op beperking van de verwerking;
- Recht op overdraagbaarheid van de gegevens;
- Recht van bezwaar en geautomatiseerde individuele besluitvorming.

Privacy by design

Rekening houdend met de stand van de techniek, de uitvoeringskosten, de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst van uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimiseren, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van de verordening en ter bescherming van de rechten van de betrokkenen.

De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

Gegevensbeschermingseffectbeoordeling (GEB/DPIA)

Een GEB is een beoordeling van de verwerking in het licht van de principes van de AVG. De GEB dient steeds aan de Data Protection Officer (DPO) voorgelegd te worden voor advies.
De verwerkingsverantwoordelijke vraagt in voorkomend geval de betrokkenen of hun vertegenwoordigers naar hun mening over de voorgenomen verwerking.

Een GEB heeft tot doel om de risico's voor de persoonsgegevens in kaart te brengen en ervoor te zorgen dat bij de implementatie de principes van de AVG en andere toepasselijke wetgeving inzake verwerking van persoonsgegevens worden nageleefd. De VTC bepaalt in haar advies dat besturen de genomen veiligheidsmaatregelen moeten opsommen, wat gebruikelijk in een GEB gebeurt.

Voor een aantal verwerkingen stelt de AVG een GEB verplicht. De GEB is steeds verplicht bij "stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten". Bij het gebruik van camera's in openbare ruimtes dient er dus quasi altijd een GEB uitgevoerd te worden.

Bij het plaatsen van camera's zal een GEB zeer vaak verplicht zijn, aangezien er bijna altijd sprake is van systematische observatie. De GEB dient vroeg in het proces te worden opgestart en niet achteraf opgemaakt te worden om het gebruik te rechtvaardigen. De GEB dient dus eigenlijk uitgevoerd te worden vooraleer het bestuur beslist tot het plaatsen van camera's.

Zelfs wanneer een bestuur van mening is dat een GEB niet noodzakelijk is voor het gebruik van bepaalde camera's, dient er minstens een 'pre-GEB' uitgevoerd te worden waaruit blijkt dat een volledige GEB niet noodzakelijk is.

De GEB bevat minstens volgende elementen:

a) Een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;
b) Een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
c) Een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
d) De beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.

Wanneer uit de GEB blijkt dat de verwerking een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen, moet er verplicht advies gevraagd worden aan de toezichthoudende autoriteit. Voor lokale besturen is dat de Vlaamse Toezichtcommissie (VTC).

DPIA voor ANPR-camera's

De VTC publiceerde reeds een standpunt over het gebruik van ANPR camera's. Dit standpunt is te raadplegen via volgende link: ANPR-camera's | Vlaanderen Intern

Doorgeven aan derde landen

Bij doorgiften naar derde landen buiten de Europese Economische Ruimte (bv opslag op een server in de US) moet er in een gelijkwaardige bescherming voorzien worden als binnen de EER.

De verwerkingsverantwoordelijke moet dit kunnen aantonen door een Transfer Impact Assessment op te maken waaruit blijkt dat de persoonsgegevens eenzelfde niveau van bescherming genieten als binnen de EER.

Maak daarom als verwerkingsverantwoordelijke de afstemming samen met de DPO van het lokaal bestuur of persoonsgegevens wel daadwerkelijk buiten de EER dienen verwerkt te worden.

Privacybeleid

Het privacybeleid op de website van het lokaal bestuur dient aangepast te worden. De betrokken personen moeten immers alle informatie over de beeldverwerking door middel van bewakingscamera's eenvoudig kunnen raadplegen. In de AVG staan de algemene transparantie- en informatieverplichtingen beschreven in artikel 12 en volgende. Deze moeten worden nageleefd. In het privacybeleid dient ook te worden toegelicht welke de rechten van de betrokkenen zijn (denk hierbij bijvoorbeeld aan recht van inzage, recht van gegevenswissing, recht van bezwaar, etc.) en hoe zij hun rechten kunnen uitoefenen.

Meer info en bronnen

- Informatieclassficatieraamwerk – Digitaal Vlaanderen
- Cybersecurity Toolkit - VVSG
- Veiligheids- en opvolgingsplan - VVSG
- Minimale maatregelen – Netwerken – Digitaal Vlaanderen
- Minimale maatregelen – Cryptografie – Digitaal Vlaanderen
- Minimale maatregelen - ICT systemen – Digitaal Vlaanderen
- Minimale maatregelen - Asset en configuratiebeheer – Digitaal Vlaanderen
- Minimale maatregelen - Beheer aanvragen – Digitaal Vlaanderen
- Minimale maatregelen - Beheer gebeurtenissen – Digitaal Vlaanderen
- Minimale maatregelen – Incidentbeheer – Digitaal Vlaanderen
- Minimale maatregelen - Release en deployment beheer – Digitaal Vlaanderen
- Minimale maatregelen – Toegangsbeheer – Digitaal Vlaanderen
- Minimale maatregelen – Wijzigingsbeheer – Digitaal Vlaanderen
- Minimale maatregelen – Probleembeheer – Digitaal Vlaanderen
- Minimale maatregelen – Veiligheidstesten – Digitaal Vlaanderen
- Minimale maatregelen – IAM – Digitaal Vlaanderen
- Minimale maatregelen - Ontwikkeling en gebruik van toepassingen – Digitaal Vlaanderen
- Minimale maatregelen – Risicomethodiek – Digitaal Vlaanderen
- Minimale maatregelen - Risico analyse – Digitaal Vlaanderen
- Minimale maatregelen - Proces risicobeheer – Digitaal Vlaanderen
- Minimale maatregelen – SIEM – Digitaal Vlaanderen
- Minimale maatregelen – PAM – Digitaal Vlaanderen
- Minimale maatregelen - Fysische maatregelen – Digitaal Vlaanderen
- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- ISO/IEC 27002:2022 (en) — Information security, cybersecurity and privacy protection — Information security controls
- NIST Special Publication 800-63B – Digital Identity Guidelines
- EDPB - Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur
- Schriftelijke vraag nr. 7-1645 van Els Ampe (Open Vld) d.d. 2 juni 2022 aan de minister van Defensie
- De Kamer van Volksvertegenwoordigers - Schriftelijke vraag en antwoord nr 55-177
- Wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's
- Koninklijk besluit van 8 mei 2018 betreffende de aangiften van de plaatsing en het gebruik van bewakingscamera's en betreffende het register van de beeldverwerkingsactiviteiten van bewakingscamera's
- Generieke verwerkingsovereenkomst - VVSG
- Duiding privacyvereisten - Gegevensbeschermingsautoriteit
- Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur, EDPB, 29 januari 2020

Een uitgave van de Vereniging van Vlaamse Steden en Gemeenten
VVSG vzw • Bischoffsheimlaan 1-8 • 1000 Brussel
september 2021

- Verordening (EU), nr. 2016/679, 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Pb.L. 4 mei 2016, afl. 119, 1), afgekort AVG
- https://www.gegevensbeschermingsautoriteit.be/professioneel/avg/rechtsgronden
- https://www.besafe.be/nl/camera
- Advies VTC nr. 2020/05 van 8 september 2020, betreffende Informatieveiligheid en GDPR-conformiteit 4 Platformen Onderwijs – Amazon Web Services (AWS)
- VTC Reactie van 20 oktober 2020 in verband met advies en waarschuwing VTC nr. 2020/05
- Advies VTC nr. 2022/02 van 11 oktober 2022 Betreffende hosting van persoonsgegevens aanvullend bij richtlijn VTC/a/2020/05
- Omzendbrief van 10/12/2009 ministeriele omzendbrief betreffende de wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's, zoals gewijzigd door de wet van 12 november 2009 (openjustice.be)

Een uitgave van de Vereniging van Vlaamse Steden en Gemeenten
VVSG vzw • Bischoffsheimlaan 1-8 • 1000 Brussel
september 2021

vvsg

VVSG vzw • Bischoffsheimlaan 1-8 • 1000 Brussel • T +32 2 211 55 00
info@vvsg.be • www.vvsg.be