WHITE PAPER
DE NIEUWE CAMERAWET
(JUNI 2018)

SECURITAS

Inhoudstafel

1.

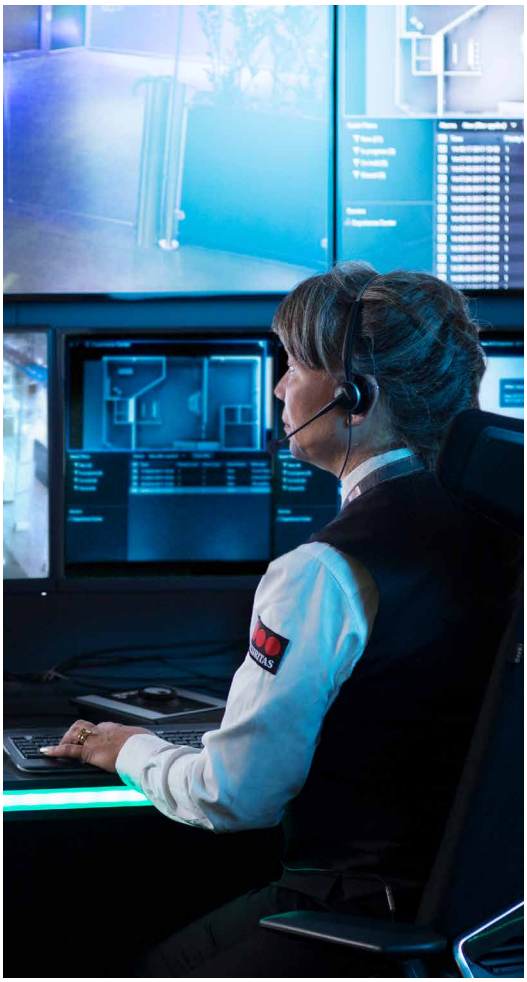
Camerawet en private veiligheid

In het Belgisch Staatsblad van 16 april 2018 werden de Wetsaanpassingen van de zogenaamde 'Camerawet' gepubliceerd. De nieuwe Wet is in werking getreden op 25 mei 2018 en is een herziening van de Camerawetgeving uit 2007, om zich zo aan te sluiten bij de vele nieuwe ontwikkelingen in dit domein. Er zijn bovendien nauwe linken met de Wet op de Private en Bijzondere Veiligheid en de GDPR of Algemene Verordening Gegevensbescherming. Welke veranderingen dat allemaal met zich brengt, leest u hier.

Je kan de Camerawet niet los zien van andere Wetgevingen. Eén ervan is de Wet op Private Veiligheid, van kracht sinds oktober 2017.

Sinds de nieuwe Wet kunnen bewakingsagenten, in bepaalde gevallen en onder voorwaarden, realtime beelden bekijken afkomstig van bewakingscamera's die, vanop een bewaakte site, gericht zijn op de openbare weg.

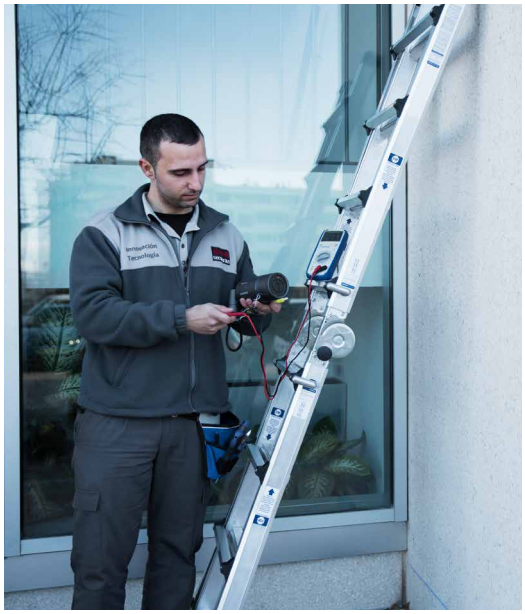
Tevens kunnen bewakingsagenten in **real time beelden bekijken** afkomstig van bewakingscamera's geplaatst óp de openbare weg. Bij deze laatste vorm geldt wel de voorwaarde dat dit enkel mag gebeuren binnen de lokalen van de overheid én onder toezicht van politiefunctionarissen. De beelden kunnen dus niet worden doorgestuurd naar de alarmcentrale of dispatching van de bewakingsonderneming.

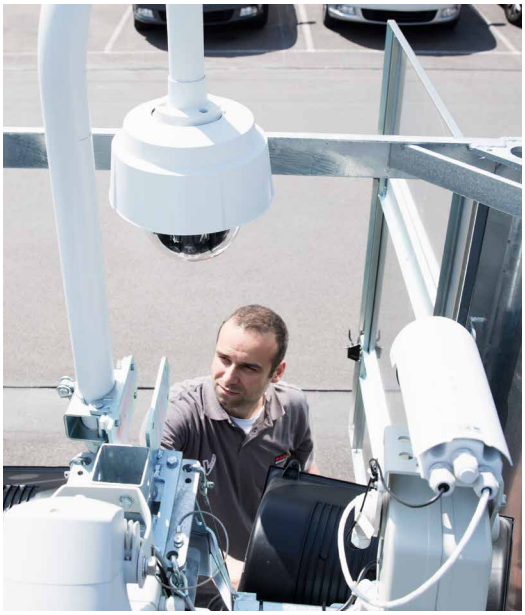


2.

Camerawet en installateurs

Een bijkomende verandering die voortvloeit uit de Wet op de Private Veiligheid en de Camerawet is dat installateurs van camerasystemen nu onder de Wet op de Private Veiligheid vallen. Dit houdt in dat het installeren, onderhouden, herstellen én concipiëren van camerasystemen enkel kan gebeuren na het verkrijgen van een vergunning.





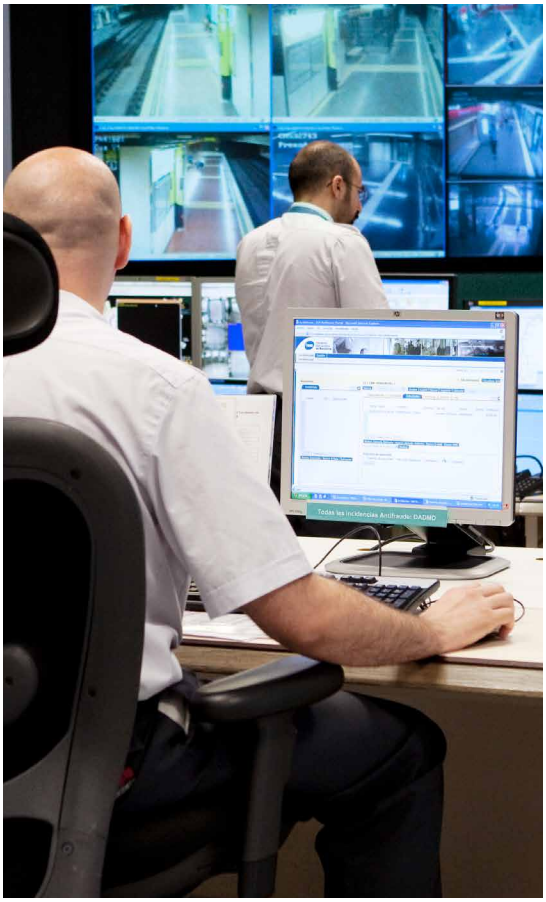
Voorheen waren de installateurs van camerasystemen niet gebonden aan wettelijke richtlijnen. Een beslissing nemen over het plaatsen van camera's in een woning of gebouw is echter nauw verbonden aan de privacy van personen. Het was dus belangrijk om dit wettelijk beter te omkaderen. De verplichting om een vergunning te hebben als installateur zorgt op die manier voor een **kwaliteitsgarantie vanuit de sector**.

3.

Camerawet en GDPR

Zoals reeds gesteld treedt de nieuwe Camerawet in werking op 25 mei 2018. Dit is niet toevallig dezelfde dag dat de GDPR effectief van toepassing wordt. Dit is de Europese Algemene Verordening Gegevensbescherming, de nieuwe Europese privacywetgeving over de bescherming en beveiliging van persoonlijke data. Belangrijk om weten is dat beiden vanaf dan zullen moeten worden toegepast, maar opgelet: de principes van de GDPR primeren op Camerawet.

De GDPR handelt over de verwerking van persoonsgegevens. De **verantwoordelijkheid ligt bij de gebruiker (en niet bij de installateur of leverancier)** die verantwoordelijk is voor de bescherming van de persoonsgegevens, en erover moet waken dat de opname en verwerking kadert binnen de vastgelegde finaliteit.



Beide regelgevingen stellen dat er algemeen geen heimelijk gebruik mag worden gemaakt van camerabeelden en dat de opnames beveiligd zijn tegen wat men toevallige of kwaadwillige nieuwsgierigheid noemt. Dat gaat zelfs zo ver tot de inrichting van de dispatching, waar geen publiek zicht op de beelden mogelijk mag zijn.

Voor de burger moeten er **pictogrammen** worden aangebracht, die aangeven waar er zich camera's bevinden. Bovendien hebben de personen op deze beelden recht van toegang tot inzage, verbetering of om hun gegevens te laten verwijderen. Een belangrijk element van de GDPR is immers dat iedereen eigenaar is van zijn eigen persoonsgegevens.

De boetes binnen de GDPR kunnen oplopen tot maximum 20 miljoen euro, of tot 4 procent van de totale omzet van het bedrijf.

4.

Wijzigingen in de Camerawet

Een fundamentele aanpassing in de nieuwe Camerawet is dat het gebruik van camera's door politiediensten en camera's voor de beveiliging in een bedrijf niet langer onder dezelfde wetgeving vallen. De **regels voor de politie zijn uit de Camerawet gehaald** en onder de Wet op het Politieambt ondergebracht.

Een tweede belangrijke bijsturing vindt plaats op het vlak van de verantwoordelijkheid voor de verwerking. Voorheen had de Belgische Privacycommissie onder meer de taak om de aangegeven registratie van camera's bij te houden, dit is met de nieuwe Camerawet afgeschaft.

Deze taak behoort nu toe aan de verantwoordelijke van de verwerking, door het vervolledigen van het zogenaamde «intern activiteitenregister» dat ter plaatse blijft, en dat hij ter beschikking moet stellen van de Gegevensbeschermingsautoriteit. Ook de kennisgeving aan de Lokale Politie zit in zijn takenpakket. Tegelijk heeft de Gegevensbeschermingsautoriteit (voorheen de Privacycommissie) vanaf nu een versterkte controle- en sanctioneringsfunctie. De verwerker dient steeds een verwerkingsovereenkomst te sluiten met verschillende partijen.

Een ander belangrijk element in de vernieuwde Camerawet is de focus op de **finaliteit** en dit in combinatie met het **proportionaliteitsbeginsel**. Men gaat met andere woorden eerst kijken wat met het camerasysteem wordt beoogd, wat het concrete doel is, om op basis daarvan de concrete uitwerking uit te voeren.

Hieronder gaan we dieper in op enkele specifieke aanpassingen.

4.1 De verantwoordelijke voor de verwerking

De GDPR stelt dat men altijd een verantwoordelijke moet aanduiden bij de verwerking van persoonsgegevens. Aangezien dit een Europese verordening betreft, kunnen de specifieke regels per land verschillen en kan dit praktisch gezien moeilijk iemand zijn in het buitenland, bijvoorbeeld in de hoofdzetel van een internationaal bedrijf. Een verantwoordelijke per land, per site of zelfs per camerasysteem is hierdoor aan te raden.

Zoals reeds kort aangehaald is de **aangifteplicht** van camerasystemen bij de Belgische Privacycommissie afgeschaft en nu een **taak van de verantwoordelijke voor de verwerking**. Hij voert deze taak uit door onder meer een intern reglement en register op te stellen waarin alle verwerkingsactiviteiten opgenomen zijn. Dat is heel uitgebreid en moet continu worden bijgehouden en geüpdatet. De verantwoordelijke voor de verwerking moet ervoor zorgen dat de gegevens altijd actueel zijn en dat het inplantingsplan nog steeds klopt.

Bij het bekijken van real time beelden door bewakingsagenten afkomstig van bewakingscamera's die, vanop de bewaakte site, gericht zijn op de openbare weg is de **verantwoordelijke** van de verwerking, **tevens de opdrachtgever** van de bewakingsactiviteit. Het is ook een van zijn verantwoordelijkheden dat de correcte **pictogrammen** aangebracht zijn die aangeven waar camera's bevinden.

De verantwoordelijke voor de verwerking kan een natuurlijk persoon zijn, maar ook een openbaar bestuur, een feitelijke vereniging (bijvoorbeeld voor evenementen) of een rechtspersoon. Dat laatste is sterk aan te raden voor bedrijven, zodat **niet alle verantwoordelijkheid bij één persoon** terecht komt. De coördinaten van de verantwoordelijken moeten worden meegedeeld aan de lokale politie, bevoegd voor de plaats van de installatie van camerasystemen.

4.2 De verwerker en derden

De verantwoordelijke voor de verwerkingsactiviteiten mag taken delegeren naar de verwerker, maar behoudt hierbij altijd de eindverantwoordelijkheid. Met elke verwerker wordt – indien er geen hiërarchische band is maar met een andere dienst of externe partij wordt samengewerkt – elke keer een verwerkingsovereenkomst gemaakt, met een beschrijving van de gedelegeerde taken. Anderzijds is er een belangrijke tweespalt in de hiërarchische verhouding tussen de verantwoordelijke en zijn leidinggevende: bewakingsagenten zijn verantwoording verschuldigd aan hun leidinggevende, maar de **verantwoordelijke voor de verwerking behoudt alle eindverantwoordelijkheid**, hem toegekend door de privacywetten.

Naast de verwerker kunnen ook derden betrokken worden bij de verwerking van camerabeelden. Dat is iedereen die niet valt onder de verantwoordelijke voor de verwerking of de verwerker zelf. Bijvoorbeeld de politie of mensen die in de buurt wonen en na een misdrijf ongeval beelden opvragen. Hoe wordt met hen omgegaan? Hoe worden vragen behandeld? Die beslissingen liggen in handen van de verantwoordelijke.

4.3 De finaliteit: waarvoor ga je beelden verwerken?

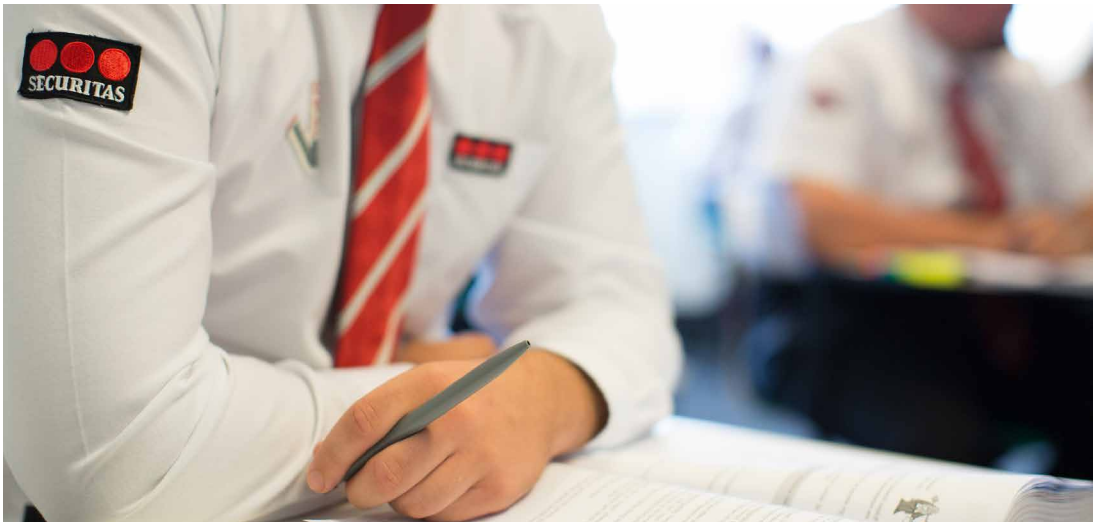
De nieuwe Camerawet biedt heel wat mogelijkheden, maar alles draait rond de finaliteit. Waarom ga je persoonsgegevens verwerken door middel van een 'observatiesysteem' waarbij beelden worden verwerkt? Camera's in een winkel kunnen vooral worden ingezet tegen winkeldiefstallen, maar ook tegen diefstal door personeel. Dit is een verschil van finaliteit die je beiden op voorhand al moet uitschrijven. De privacywetgeving staat hier boven het arbeidsreglement. Het is daarom aan te raden om dit ook in het arbeids- en andere reglementen op te nemen.

Bij het opgeven van de finaliteit is **proportionaliteit een belangrijk element**. Als je een goede toegangscontrole kunt opzetten met 1 camera, dan mag je er geen 5 zetten. Maar kun je de finaliteit (een goede en veilige toegangscontrole) enkel bereiken met 5 camera's, dan moet je er 5 plaatsen. Het is de verantwoordelijke van de verwerking die hierover moet oordelen.

Dit betekent dat we op het vlak van security anders moeten denken. Vroeger ging men uit van risicoanalyses om op basis van de lijst van risico's een beveiliging op te zetten, nu mogen camera's enkel nog worden gebruikt binnen de finaliteit. Om die reden kan de verantwoordelijke best een soort van **draaiboek** maken, zodat elke verwerker individueel weet hoe er moet gewerkt worden.

4.4 Bijkomende informatie

Het monitoren van camerabeelden wordt een echte specialisatie. Externe bewakingsagenten zullen de camerabeelden enkel kunnen bekijken als ze daarvoor een **specifieke opleiding** volgen. Dergelijke opleiding wordt momenteel reeds gegeven door Securitas Academy.



De nieuwe Camerawet biedt veel mogelijkheden, maar de grenzen die GDPR oplegt, zijn strikt. Er zijn voorbeelden van een supermarktketen die met camera's controleerde hoe lang het personeel op het toilet zat: dit werd gezien als een ernstige inbreuk op de privacy. Ook hier geldt dus de wet van de proportionaliteit.

Als de politie binnen hun wettelijk takenpakket camerabeelden opvraagt, moeten die kosteloos worden aangeboden. Op risicovolle sites kan voorafgaand een akkoord worden gesloten dat de beelden in real time naar de politie worden gestreamd. Echter, ook al komt de vraag vanwege de politie, het is altijd de verantwoordelijke die daarover beslist. Een uitzondering is er wanneer de Wet dit oplegt, bijvoorbeeld voor de metro en de NMBS.

De termijn voor het **bewaren van beelden** ligt op **maximaal één maand**. In bedrijven met een verhoogd risico, zoal luchthavens en havens, internationale treinstations, nucleaire sites, en internationale instellingen is de maximum bewaartermijn van de camerabeelden echter opgetrokken van één naar drie maanden. De opsomming van deze bedrijven en sectoren zal gebeuren in een Koninklijk Besluit, maar bijkomend zal nog altijd toestemming moeten worden gevraagd aan de gemeenteraad.

Mobiele bewakingscamera's, zoals **drones of bodycams** worden toegelaten, maar enkel in de volgende gevallen:

- Indien ze gebruikt worden door bewakingsagenten in het kader van hun bevoegdheden van de Wet op de private veiligheid;
- In besloten plaatsen waar niemand verondersteld wordt aanwezig te zijn;
- Bij gebruik door een natuurlijke persoon voor persoonlijke en huishoudelijke doeleinden in een niet voor het publiek toegankelijke besloten plaats.

5.

Camerabeelden op specifieke plaatsen

5.1 Camerabeelden op de openbare weg

Intelligente bewakingscamera's zijn binnen deze wetgeving toegelaten, aangezien deze niet gekoppeld zijn aan persoonsgegevensbestanden. Dit zijn bijvoorbeeld camera's die geluiden of bewegingen detecteren. Gaat het om intelligente camera's die gekoppeld zijn aan persoonsgegevensbestanden, dan zijn enkel de ANPR-camera's voor nummerplaatherkenning toegelaten. Het **persoonsgegevensbestand** moet worden verwerkt overeenkomstig de wetgeving op de persoonlijke levenssfeer.

Zoals reeds gesteld mogen camerabeelden van op de openbare weg bekeken worden door bewakingsagenten, weliswaar onder toezicht van een politieagent. Met de nieuwe Wet zullen niet alleen de politiediensten, maar ook gemeentelijke overheden en de bewakingsfirma's die voor hen werken, mobiele ANPR-camera's kunnen bekijken om parkeeroverlast en verkeersovertredingen te voorkomen, vast te stellen of op te sporen.

Het gebruik van mobiele ANPR-camera's op de openbare weg moet eerst worden goedgekeurd door de gemeenteraad, in overleg met de korpschef. Tevens dient de gemeente het bestaan van het camerasysteem ook mee te delen aan de politiediensten en aan de burgers, door middel van o.a. een pictogram op het voertuig.

5.2 Camera's voor toegangscontrole

Wanneer bedrijven camera's inzetten voor toegangscontrole, mogen ze deze niet specifiek richten op de straat of het voetpad. Wil een **shoppingcenter** bijvoorbeeld een camera op de parking plaatsen, die tegelijk een stuk van de openbare weg bestrijkt, dan moet het daarvoor een aanvraag indienen bij de gemeente en toestemming vragen aan de politie, waarna dit wordt vastgelegd in de gemeenteraad.

Deze aanvraag moet gebeuren voor het camerasysteem als geheel, wat bij grote camerasystemen heel wat administratie kan meebrengen. Een alternatief is om die ene camera die zich deels richt op de openbare weg, onder te brengen in een apart systeem, of om de camerabeelden te 'blacken' voor het deel van de openbare weg. Opgelet: dit 'blacken' moet niet enkel gebeuren op het scherm, maar ook op de harde schijf, zodat de privacy ook nadien gewaarborgd blijft.

5.3 Camera's in winkels

In winkels zie je vaak jezelf als klant op een televisiescherm door middel van camerabeelden. Dergelijke livestream is toegelaten, op voorwaarde dat het camerabeeld onmiddellijk 'live' op het scherm wordt getoond. De **beelden mogen evenwel niet worden opgenomen**, want op dat moment spreken we al over een 'verwerking'. Indien er toch beelden worden opgenomen, dan valt dit onder een andere wetgeving met bijkomende verplichtingen. Zo moet er dan onder andere aan de ingang een pictogram worden aangebracht, zodat klanten en werknemers weten dat er van hen beelden worden gemaakt.

5.4 Camera's op privédomein

Wie in zijn eigen woning een bewakingscamera installeert voor persoonlijke en huishoudelijke doeleinden, moet **geen aangifte** doen, noch een register invullen of een pictogram gebruiken. Een belangrijk bijkomend element is dat voor camerasystemen bij privégebruik het altijd de eigenaar is die verantwoordelijk is voor het bijhouden van beelden.

Daarnaast mag je beelden waar andere mensen opstaan wel bijhouden voor persoonlijk of huishoudelijk gebruik, maar bijvoorbeeld **niet op sociale media plaatsen**. In dat geval vindt er een zogenaamde 'tweede' verwerking van de beelden plaats en pleeg je een inbreuk op de Wet op de privacy.

6.

Besluit

Het is duidelijk: de nieuwe Camerawet – en parallel de GDPR en de Wet op de Private Veiligheid – brengen grote veranderingen met zich mee. De nieuwe regels inzake camerabewaking voorzien dan wel een overgangsbepaling waardoor bedrijven 2 jaar tijd hebben om hun systemen aan te melden bij politie, toch blijft het kort dag. De tijd dringt om zich in orde te stellen met de regelgeving inzake privacy, private veiligheid en camerabewaking.

Het spreekt evenwel voor zich dat de nieuwe technologieën en ontwikkelingen in de sector continue bijsturingen vragen. Voor elk bedrijf wordt het een uitdaging om er constant mee bezig te zijn, om zo up-to-date te blijven op het drieluik technologie, organisatorisch en op het vlak van awareness.