Collectieve camerabewaking Stichting Beveiliging Bedrijven Hardinxveld-Giessendam

Data Protection Impact Assessment

Versie
13 mei 2024

Auteur
Sander Flight
info@sanderflight.nl | 06 – 41 31 5432

Inhoud

Afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
DPIA	Data Protection Impact Assessment
EDPB	European Data Protection Board
EVRM	Europees Verdrag voor Rechten van de Mens en fundamentele vrijheden
FG	Functionaris voor Gegevensbescherming
GEB	Gegevensbeschermingseffectbeoordeling
OvJ	Officier van Justitie
OM	Openbaar Ministerie
SBBHG	Stichting Beveiliging Bedrijven Hardinxveld-Giessendam
SV	Wetboek van Strafvordering
VbV	Verzekeringsbureau Voertuigcriminaliteit
Wpg	Wet politiegegevens

Definities

Betrokkene	de natuurlijke persoon wiens persoonsgegevens worden verwerkt
Persoonsgegevens	alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon
Verwerkings-verantwoordelijke	de (rechts)persoon die het doel van en de middelen voor de verwerking van persoonsgegeven vaststelt
Verwerker	de (rechts)persoon die persoonsgegevens verwerkt in opdracht van de verwerkingsverantwoordelijke

1 Inleiding

Op bedrijventerreinen in de gemeente Hardinxveld-Giessendam is collectieve camerabewaking aanwezig. Deze camerasystemen worden geplaatst en beheerd in opdracht van de Stichting Beveiliging Bedrijven Hardinxveld-Giessendam (SBBHG, hierna de Stichting). De Stichting is een samenwerking van ondernemers, gemeente, brandweer en politie. De burgemeester van Hardinxveld-Giessendam is voorzitter van het bestuur. Een deel van de bewakingscamera's brengt openbare plaatsen in beeld. Dat is alleen toegestaan onder bepaalde voorwaarden. In deze DPIA toont de Stichting aan dat aan alle relevante wet- en regelgeving wordt voldaan.

Geen openbare orde, wel openbare plaats

In principe is de inzet van camera's op openbare plaatsen voorbehouden aan de overheid. Gemeenten kunnen camera's plaatsen voor handhaving van de openbare orde op grond van artikel 151c van de Gemeentewet. De burgemeester van Hardinxveld-Giessendam kiest vooralsnog niet voor deze vorm van cameratoezicht op de bedrijventerreinen. De incidenten op de bedrijventerreinen zijn namelijk niet van dien aard dat sprake is van verstoring van de openbare orde. Het gaat vooral om inbraken, diefstallen, vernielingen en dergelijke. Dat zijn incidenten met grote impact op bedrijven, maar het valt niet onder verstoring van de openbare orde en dus is artikel 151c van de Gemeentewet niet het passende juridische kader voor dit soort camerabewaking. De gemeente vindt het tegelijkertijd wel van groot belang dat bedrijventerreinen in de gemeente goed worden beveiligd. Dat is van belang voor een gezonde lokale economie en een aantrekkelijk vestigingsklimaat voor ondernemers. Daarom stimuleert de gemeente ook het werk van de Stichting en is de burgemeester voorzitter van het bestuur. De Stichting is van mening dat het noodzakelijk is camerabewaking in te stellen om de bedrijven te beveiligen. Daarbij is het onvermijdelijk voor het bereiken van het doel dat ook openbare plaatsen in beeld worden gebracht met de bewakingscamera's. Onder bepaalde voorwaarden is dat toegestaan.

Autoriteit Persoonsgegevens: onder voorwaarden toegestaan

In de *Beleidsregels cameratoezicht* van de Autoriteit Persoonsgegevens[1] staat dat in het algemeen geldt dat camerabewaking door private organisaties niet verder mag reiken dan tot hetgeen onder hun eigen verantwoordelijkheid valt. Er kunnen zich echter situaties voordoen waarin private organisaties eveneens delen van openbare plaatsen filmen. Private organisaties kunnen een gerechtvaardigd belang hebben bij de beveiliging van de personen en goederen die aan de zorg van de betreffende private organisaties zijn toevertrouwd. De private organisaties zijn in dat geval verantwoordelijk voor de verwerking van persoonsgegevens die voor dit doeleinde worden verwerkt. Daarbij mogen geen grotere delen van de openbare plaatsen in beeld worden gebracht dan noodzakelijk om dit doeleinde te bereiken.

Verder staat in de *Beleidsregels cameratoezicht* dat private organisaties die openbare plaatsen in beeld willen brengen met camera's aandacht moeten besteden aan de volgende punten:

Noot 1 Zie *Beleidsregels cameratoezicht* van de Autoriteit Persoonsgegevens: https://wetten.overheid.nl/BWBR0037591/2016-02-02 (geldend van 02-02-2016 tot heden; geraadpleegd op 27-09-2023).

- Stel vast wie de verwerkingsverantwoordelijke is.
- Bepaal de doeleinden.
- Stel vast op welke grondslag de verwerking is gebaseerd: in dit geval artikel 6.1.f AVG.
- Stel vast dat de camerabewaking noodzakelijk is: op de belangen van de betrokkenen mag geen onevenredige inbreuk worden gemaakt (proportionaliteit) en camera's zijn niet toegestaan als er andere, relatief lichtere, instrumenten beschikbaar zijn waarmee de doeleinden ook kunnen worden bereikt (subsidiariteit).
- Bepaal het soort camera's en softwaretechniek die gerechtvaardigd zijn om in te zetten, rekening houdend met de belangen van betrokkenen.
- Bepaal wat er met de camerabeelden zal worden gedaan.
- Zorg voor adequate beveiliging van de camerabeelden.
- Bepaal of de betrokkenen geïnformeerd moeten worden.
- Zorg dat betrokkenen hun rechten kunnen uitoefenen.

In deze DPIA wordt aan al deze zaken aandacht besteed. Hiermee vult de Stichting haar verantwoordelijkheid als verwerkingsverantwoordelijke in de zin van de AVG in.

Verantwoordelijkheid
De Autoriteit Persoonsgegevens heeft onderzoek gedaan naar collectieve camerabewaking op een bedrijventerrein in Vianen. Dat is rechtmatig onder een aantal voorwaarden. De eerste voorwaarde is dat de verantwoordelijkheid van de (rechts)persoon die een camera op straat richt zich moet uitstrekken tot degenen die in beeld worden gebracht. Dat is op de bedrijventerreinen in Hardinxveld-Giessendam het geval. De Stichting Beveiliging Bedrijven Hardinxveld-Giessendam heeft in de statuten opgenomen dat beveiliging van de bedrijven het doel van de Stichting is. Ook is in een convenant tussen gemeente en Stichting vastgelegd dat de verantwoordelijkheid aan de Stichting kan worden toegekend.
De tweede voorwaarde is dat de Stichting aantoonbaar aan de privacywetgeving moet voldoen, met de AVG als belangrijkste kader. De gemeente heeft in het convenant vastgelegd dat de Stichting haar verantwoordelijkheid onder andere moet invullen door het opstellen van een Data Protection Impact Assessment. Om aan die eis te voldoen heeft de Stichting deze DPIA laten opstellen.

Over deze DPIA
In deze DPIA beschrijft de Stichting hoe de camerabewaking werkt en waarom de verwerking van persoonsgegevens rechtmatig en noodzakelijk is. Daarna worden de privacyrisico's beschreven en worden maatregelen getroffen om die risico's te mitigeren.

Een DPIA is in principe nooit 'af', want de techniek evolueert voortdurend. Dat levert weer nieuwe risico's of juist nieuwe beschermingsmogelijkheden op. Verder veranderen de wet- en regelgeving, soms formeel, maar soms ook door nieuwe richtlijnen van de toezichthouder of door jurisprudentie. Daarnaast zijn er maatschappelijke ontwikkelingen waardoor dat wat betrokkenen 'normaal' vinden qua privacybescherming in de loop der tijd kan veranderen. Daarom wordt deze DPIA na elke grote verandering in de techniek of wetgeving herzien.

Openbaarheid
Deze DPIA wordt niet openbaar gemaakt, maar er wordt wel informatie over de camerabewaking aangeboden aan de betrokkenen op de website van de Stichting en via informatieborden op straat.

Overige documentatie
Deze DPIA heeft als belangrijkste doel de risico's voor betrokkenen bij het verwerken van persoonsgegevens te mitigeren. Daarnaast zijn de volgende documenten ook relevant:

- Convenant camerabewaking tussen Gemeente Hardinxveld-Giessendam en SBBHG (dit convenant is in het bezit van de partijen)

- Verwerkersovereenkomst SBBHG met Alert Security BV / Viewcontrol BV (deze overeenkomst is als bijlage aan deze DPIA toegevoegd)

- Convenant Camerabewaking met kentekenherkenning tussen SBBHG, Viewcontrol en Stichting Verzekeringsbureau Voertuigcriminaliteit (dit convenant is in het bezit van de partijen)

2 Beschrijving camerasysteem

Op vijf bedrijventerreinen in Hardinxveld-Giessendam is collectieve camerabewaking gerealiseerd door de Stichting:

- Boven-Hardinxveld
- De Peulen
- Nieuweweg
- Lange Veer
- Blauwe Zoom

2.1. Doel

Het doel van de collectieve camerabewaking is het vergroten van de veiligheid op de bedrijventerreinen.

1. Het primaire doel is het voorkomen van criminaliteit door het preventieve effect dat van camerabewaking uitgaat. De camera's worden goed zichtbaar geplaatst en er komen informatieborden om mensen te wijzen op de camera's.

2. Een secundair doel van de camera's is het signaleren van gestolen of vermiste voertuigen op basis van het kenteken zodat daarvan een melding kan worden gedaan bij de politie.

3. Een ander secundair doel is het daadwerkelijk maken van opnames, zodat die door de politie kunnen worden gebruikt als bewijsmateriaal na strafbare feiten.

Er worden geen andere doelen nagestreefd met de camera's.

2.2. Technische beschrijving: camera's, verbindingen, opslag

Camera's
Op elk van de vijf bedrijventerreinen staan gecombineerde camera's van het merk Dahua. De eerste camera is een reguliere camera voor overzicht (IPC-HFW5442ZE). De tweede camera is een infraroodcamera voor kentekenherkenning (ITC-237-PW6M-IR) met ingebouwd algoritme voor het lezen van letters en cijfers op kentekens.

Verbindingen, opslag en videomanagementsysteem
De camera's zijn via glasvezel aan Viewcontrol in Sliedrecht verbonden. Viewcontrol is een door de Minister van Justitie erkende alarm- en servicecentrale (PAC102) en videocentrale (VTC11) – onderdeel van Alert Security BV. Alle camerabeelden van de reguliere overzichtscamera's worden opgeslagen op een server van Viewcontrol. De gegevens van de kentekencamera's komen binnen op een FTP-server van Viewcontrol.
De gegevens worden uitsluitend in Nederland verwerkt en niet daarbuiten. Daarmee wordt ook voldaan aan de eisen die gelden voor verwerking van persoonsgegevens in landen buiten de Europese Economische Ruimte. Daarvan is in dit geval immers geen sprake, aangezien de persoonsgegevens uitsluitend in Nederland worden verwerkt.

2.3. Functionele beschrijving: live toezicht, kentekenherkenning en gebruik opnames

Live toezicht
De camera's staan continu aan en de beelden worden opgeslagen. Alarmen worden daarnaast rechtstreeks bekeken door Viewcontrol. De beelden worden dus alleen bekeken op de alarmcentrale op het moment dat er een alarm trigger is bij een van de aangesloten bedrijven of als er hitmelding komt op een van de kentekencamera's.

Kentekenherkenning
De data van de camera's met automatische kentekenherkenning (ANPR) wordt gecontroleerd door het Verzekeringsbureau Voertuigcriminaliteit (VbV). Dit is een Stichting die is opgericht door alle Nederlandse schadeverzekeraars die bij het Verbond van Verzekeraars zijn aangesloten. Doel van het VbV is het bestrijden van voertuiggerelateerde criminaliteit.

Als een van de kentekencamera's een vermist of gestolen voertuig signaleert, ontvangt de centralist van Viewcontrol een melding. De centralist zet de melding door naar de politie en zet een surveillanceauto in om het voertuig te volgen tot het moment dat de politie ter plaatse is. Voor deze samenwerking is een samenwerkingsovereenkomst gesloten tussen de SBBHG, Viewcontrol en Stichting VbV (getekend 15 juli 2022, looptijd onbepaald).

Beelden leveren aan politie
Camerabeelden kunnen op twee manieren aan de politie geleverd worden: spontaan en vrijwillig of op basis van een vordering.

1. Spontaan en vrijwillig
   Als een ondernemer constateert dat er een strafbaar feit is gepleegd, moet hij of zij daarvan aangifte doen bij de politie. De ondernemer kan een verzoek indienen bij Viewcontrol zodat de functioneel beheerder van het camerasysteem de camerabeelden voor en na het vermoedelijke tijdstip veilig kan stellen. De aangever krijgt de beelden dus zelf niet te zien. De functioneel beheerder van Viewcontrol verstrekt een beveiligde link aan de opsporingsambtenaar van de politie die de aangifte in behandeling neemt of degene die het opsporingsonderzoek doet. Dit is een spontane en vrijwillige verstrekking van camerabeelden. De ondernemer die aangifte doet bij de politie doet tegelijkertijd een verzoek via ICT@alert-group.nl bij de functioneel beheerder van Viewcontrol om camerabeelden veilig te stellen. De ondernemer geeft daarbij de contactgegevens door van de opsporingsambtenaar van politie die het onderzoek gaat doen. De functioneel beheerder stelt de gevraagde beelden veilig en verstrekt deze op verzoek aan de politie door de beelden te uploaden via een beveiligde link die de politie doorgeeft.

2. Vordering
   Als een opsporingsambtenaar informatie heeft dat er een strafbaar feit is gepleegd op een van de bedrijventerreinen, kan deze opsporingsambtenaar op grond van art. 126nda Wetboek van Strafvordering de relevante beelden vorderen bij de Stichting. De opsporingambtenaar dient de vordering in bij de beheerder van de Stichting die daarna contact opneemt met de functioneel beheerder van het camerasysteem bij Viewcontrol. Voor de rest van het proces verloopt de werkwijze identiek als bij de vrijwillige en spontane verstrekking: de functioneel beheerder van Viewcontrol stelt de gevorderde beelden veilig en uploadt de beelden via de beveiligde link die is ontvangen van de opsporingsambtenaar die de beelden vorderde. Overigens kunnen camerabeelden ook worden gevorderd door een officier van justitie (op grond van 126nd Wetboek van Strafvordering), al dan niet op basis van een schriftelijke machtiging door een rechter-commissaris.

Overgang van AVG naar Wpg

Als camerabeelden nodig zijn voor opsporingsonderzoek, wordt er door de verwerkingsverantwoordelijke een kopie van de relevante opnames aan de politie verstrekt. Vanaf dat moment van verstrekking valt de verwerking van de kopie niet meer onder de AVG, maar onder de Wet politiegegevens (Wpg). Vanaf dat moment is de Stichting dus ook niet meer verantwoordelijk voor de verdere verwerking van de politiegegevens. Het origineel wordt bewaard tot na afronding van het opsporingsonderzoek, om ervoor te zorgen dat indien nodig nogmaals een kopie kan worden verstrekt. Maar het is de politie die daadwerkelijk met de camerabeelden aan de slag gaat. Voor die verdere verwerking geldt de Wet politiegegevens met eigen bewaartermijnen en andere voorwaarden. Ook de rechten van betrokkenen worden dus als het ware verdeeld over twee verwerkingen. De Stichting moet betrokkenen in de gelegenheid stellen hun rechten, zoals het inzagerecht, uit te oefenen op de informatie die onder de AVG valt. De politie moet datzelfde doen voor de verwerking van de kopie van de informatie die onder de Wpg valt. Als een betrokkene een inzageverzoek doet bij de Stichting, zal bij het voldoen aan dat verzoek – indien van toepassing – ook worden gewezen op het feit dat er een kopie is verstrekt aan de politie. De

betrokkene krijgt daarbij ook te horen waar en hoe een inzageverzoek (of een beroep op een ander recht dat uit de Wpg volgt) kan worden gedaan bij de politie.

2.4. Soorten persoonsgegevens

Normale persoonsgegevens
De opgenomen beelden bevatten informatie die tot individuen kan worden herleid. Dit zijn 'gewone' persoonsgegevens.

Bijzondere persoonsgegevens
Het is onvermijdelijk dat uit camerabeelden in principe ook informatie kan worden afgeleid over bijvoorbeeld iemands etniciteit of gezondheid. Het verwerken van dergelijke 'bijzondere persoonsgegevens' is in principe verboden. Dat zou echter betekenen dat alle bewakingscamera's in principe verboden zijn. Daarom heeft de Autoriteit Persoonsgegevens, om opportuniteitsredenen, bepaald dat voor camerabeelden een uitzondering geldt op het verbod tot verwerking van bijzondere persoonsgegevens mits het niet de bedoeling van de verwerking is om onderscheid te maken op grond van deze bijzondere persoonsgegevens. Dat is het geval bij onderhavige verwerking en daarom is het verbod op verwerken van bijzondere persoonsgegevens niet van toepassing op dit camerasysteem.

Strafrechtelijke gegevens
De camerabeelden kunnen uiteraard strafrechtelijke gegevens bevatten als iemand een strafbaar feit pleegt in het zicht van een van de camera's. Het verwerken van strafrechtelijke gegevens is echter niet het doel van de verwerking voor de verwerkingsverantwoordelijke: alleen de politie voert opsporingsonderzoeken uit. Voor die onderzoeken geldt niet de AVG, maar de Wpg. Het is niet de Stichting, maar de politie die de verwerkingsverantwoordelijke is voor de verwerking van de politiegegevens in opsporingsonderzoeken.

Geen bijzondere technieken
Er is geen sprake van automatische persoonsherkenning, biometrie of automatische besluitvorming.

3 Verantwoordelijkheid en rechtmatigheid

Camerabewaking is een inbreuk op de privacy van de personen die in beeld komen. Dat is alleen toegestaan als het voor een gerechtvaardigd belang van de verwerkingsverantwoordelijke gebeurt en als het noodzakelijk is voor het bereiken van dat doel. De rechtmatigheid vereist een grondslag in de wet. De noodzakelijkheid hangt af van de proportionaliteit en subsidiariteit. In dit hoofdstuk wordt de rechtmatigheid aangetoond.

3.1. Verantwoordelijkheid

Ook als particulieren openbare plaatsen met camera's beveiligen kan de gemeente zich niet aan haar verantwoordelijkheid onttrekken, aldus de *Beleidsregels cameratoezicht* van de Autoriteit Persoonsgegevens. Op welke wijze de burgemeester invulling kan geven aan zijn verantwoordelijkheid, is afhankelijk van de situatie. Zo is het mogelijk dat de burgemeester cameratoezicht instelt op de openbare plaatsen die mede door de private organisaties worden gefilmd. Een ander voorbeeld is dat de burgemeester eisen stelt aan de reikwijdte van het cameratoezicht op de openbare plaatsen door private organisaties of aan de wijze waarop betrokkenen over dit cameratoezicht moeten worden geïnformeerd.

Convenant Stichting en gemeente Hardinxveld-Giessendam
Voor dat laatste is in Hardinxveld-Giessendam gekozen. Daarom hebben de Stichting en de gemeente in een convenant afspraken gemaakt over de collectieve camerabewaking. Het convenant is in deze DPIA opgenomen. In het convenant is geregeld dat de verantwoordelijkheid van de gemeente voor de openbare ruimte goed wordt ingevuld. Tegelijkertijd is vastgelegd dat de Stichting verantwoordelijk is voor het voldoen aan de relevante wet- en regelgeving op het gebied van de bescherming van fundamentele rechten en de bescherming van persoonsgegevens. Door het opstellen van deze DPIA voldoet de Stichting aan het convenant.

Verantwoordelijkheid Stichting
De verantwoordelijkheid van de Stichting strekt zich uit, zo blijkt uit de statuten, tot de hele bedrijventerreinen, dus de bedrijfspercelen en de tussenliggende wegen. Het doel van de Stichting zoals opgenomen in de statuten is: "het bevorderen van een ongestoord gebruik door de bij de stichting aangesloten ondernemers van goederen en zaken op bedrijventerreinen en van goederen en zaken van niet op een bedrijventerrein gevestigde bedrijven te Hardinxveld-Giessendam." De verwerkingsverantwoordelijkheid in de zin van de AVG voor de camerabewaking op de bedrijventerreinen kan dan toebedeeld worden aan de Stichting.

3.2. Rechtmatigheid

Nu is vastgesteld dat de Stichting verantwoordelijk is voor de verwerking van persoonsgegevens met camerabewaking. Maar voor een rechtmatige inzet van camera's is ook nog een grondslag in een wet vereist. In dit geval baseert de Stichting zich op de grondslag 'gerechtvaardigd

belang' zoals verwoord in art. 6, lid 1, onder f van de AVG. Om dit als rechtsgrond te mogen kiezen, moet aan drie cumulatieve voorwaarden zijn voldaan, zo blijkt uit de jurisprudentie en onderzoeken door de Autoriteit Persoonsgegevens:

1. De camerabewaking moet rechtmatig zijn op basis van een voldoende specifieke verwoording en niet speculatief (dus een werkelijk aanwezig belang vertegenwoordigend);

2. De camerabewaking moet noodzakelijk zijn wat inhoudt dat moet voldaan zijn aan de eisen van proportionaliteit en subsidiariteit;

3. Uit een belangenafweging moet blijken dat de belangen van de verwerkingsverantwoordelijke bij de camerabewaking zwaarder wegen dan de belangen van de betrokkenen bij bescherming van hun privacy.

Voorwaarde 1: Gerechtvaardigd belang
De Stichting heeft een gerechtvaardigd belang bij de beveiliging van personen, goederen, terreinen, zaken en productieprocessen door middel van camerabewaking. De bescherming van eigendommen vormt de uitoefening van een fundamenteel recht zoals opgenomen in artikel 17 van het Handvest van de Grondrechten van de Europese Unie en artikel 1 van het eerste protocol bij het Europees Verdrag voor de Rechten van de Mens. Het belang van de Stichting bij het beveiligen van eigendommen van de aangesloten ondernemers is dus in overeenstemming met EU-recht.
Voorts is het belang voldoende specifiek te zijn en niet speculatief. Kortom: er moeten daadwerkelijk incidenten plaatsvinden. Dit komt hieronder aan bod bij de bespreking van de proportionaliteit.

Voorwaarde 2: Noodzakelijkheid
Noodzakelijkheid wordt in de jurisprudentie en door de Autoriteit Persoonsgegevens geoperationaliseerd door te kijken of aan de eisen van proportionaliteit en subsidiariteit wordt voldaan.

Proportionaliteit gaat over de vraag of het middel camerabewaking in evenwichtige verhouding staat tot het doel. Anders gezegd: rechtvaardigen de criminaliteit en onveiligheid de inzet van de camerabewaking? De omvang van de veiligheidsproblematiek op de bedrijventerreinen in Hardinxveld-Giessendam wordt continu in de gaten gehouden in het kader van het Keurmerk Veilig Ondernemen. De meest recente cijfers laten zien dat dankzij de inspanningen de veiligheid is vergroot, maar dat er nog altijd incidenten gebeuren. In 2018 ging het op de vijf bedrijventerreinen volgens politieregistraties om 44 incidenten; in 2021 waren dat er 29. Er is dus sprake van een verbetering, maar de problemen zijn niet weg. Daarbij dient overigens rekening te worden gehouden met het feit dat de politie niet alle incidenten registreert. In 2018 werd volgens een enquête onder bedrijven 39 procent van de incidenten gemeld of aangegeven bij de politie. Het werkelijke aantal incidenten is dus naar schatting twee keer zo groot als het aantal door de politie geregistreerde incidenten. Belangrijkste conclusie is dat onder andere inbraken en vernielingen een reëel bestaand probleem zijn op de bedrijventerreinen. Daarmee is het belang dat de verwerkingsverantwoordelijke heeft bij de camerabewaking daadwerkelijk aanwezig en niet speculatief. Dat maakt de camerabewaking een proportionele maatregel.

De kentekenherkenning is proportioneel omdat reguliere camera's niet in staat zijn kentekens nauwkeurig waar te nemen waardoor veel camerabeelden onbruikbaar zijn voor opsporingsonderzoek door de politie. De automatische kentekenherkenning is nodig om goed onderbouwd aangifte te kunnen doen bij de politie na incidenten. De politie krijgt dan niet alleen de 'ruwe' camerabeelden te zien, maar krijgt ook een lijst met kentekens die voor of na het incident het industriegebied op zijn gereden. Daarbij worden alleen die kentekens geleverd die relevant kunnen zijn voor het opsporingsonderzoek in dat specifieke geval. De beoordeling van wat relevant is, wordt door de politie gemaakt na de aangifte. Zij dienen een verzoek in bij de Stichting waarbij ze aangeven over welke periode en van welke cameraposities ze de gelezen kentekens nodig hebben.

Aan de subsidiariteitseis wordt ook voldaan: het beoogde doel kan niet op een andere, voor betrokkenen minder nadelige, wijze worden verwezenlijkt. Naast de camera's is reeds een uitgebreid pakket aan andere maatregelen en instrumenten ingezet voor de beveiliging van de ondernemingen:

- Bewustwording bij ondernemers door nieuwsbrieven
- Verbodsborden op de terreinen
- Alarmsystemen geïnstalleerd
- Verbeteren onderhoud aan wegen, groen en dergelijke
- Revitalisering bedrijventerreinen door betere infrastructuur
- Betere openbare verlichting op basis van halfjaarlijkse schouw
- Hekken en slagbomen geïnstalleerd
- Fysieke surveillance door Alert Security

Deze maatregelen en instrumenten hebben allemaal hun waarde, maar kunnen de veiligheid niet voldoende waarborgen. Camerabewaking voegt een uniek extra ingrediënt toe aan het maatregelenpakket: het mogelijk maken goed onderbouwd aangifte te doen bij de politie na strafbare feiten. Dit doel kan niet op een voor de betrokkene minder nadelige wijze worden verwezenlijkt.

Uit eerder onderzoek door de Autoriteit Persoonsgegevens naar bewakingscamera's op een bedrijventerrein in Vianen blijkt dat de proportionaliteit en subsidiariteit van de gegevensverwerking ook worden vergroot als de volgende maatregelen worden getroffen:

- Er worden niet meer camera's geplaatst dan noodzakelijk voor het bereiken van het doel;
- Er worden niet meer plaatsen en personen in beeld gebracht dan noodzakelijk voor het bereiken van het doel;
- De gegevensverwerking is zo mimimaal mogelijk ingericht, zoals blijkt uit het hoofdstuk bij de bespreking van de principes van de verwerking, waaronder dataminimalisatie.

Ook deze maatregelen zijn getroffen door de verwerkingsverantwoordelijke waardoor zo goed mogelijk wordt voldaan aan de eisen van proportionaliteit en subsidiariteit.

Voorwaarde 3: Belangenafweging
In de AVG staat bij de gekozen grondslag gerechtvaardigd belang het volgende:

> "de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke, 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."

De AVG vereist dus dat er een expliciete afweging wordt gemaakt tussen aan de ene kant het gerechtvaardigde belang van de Stichting bij camerabewaking en aan de andere kant de privacy van de personen die in beeld kunnen komen. Bij die afweging moet worden meegewogen welke (ongewenste) gevolgen de camerabewaking heeft voor betrokkenen alsmede de waarborgen die de verantwoordelijke heeft getroffen ter voorkoming en beperking van de ongewenste gevolgen.

Er zijn geen enquêtes gehouden op de bedrijventerreinen. Wel heeft de Stichting gesprekken gevoerd met bewoners van enkele bedrijfswoningen: die maakten geen bezwaar tegen de camerabewaking. En sinds de start van het cameratoezicht heeft geen van de bewoners een klacht ingediend over de camerabewaking bij de Stichting.

De Stichting komt na zorgvuldige weging tot de conclusie dat het belang bij camerabewaking zwaarder weegt dan het belang van betrokkenen bij bescherming van hun privacy. In deze DPIA worden waarborgen beschreven die de verwerkingsverantwoordelijke heeft getroffen om de ongewenste gevolgen te beperken.

Kortom: de Stichting heeft een gerechtvaardigd belang bij de camerabewaking. De omvang en de ernst van de criminaliteit rechtvaardigen de inzet van een relatief zwaar middel als camerabewaking. Minder ingrijpende maatregelen die hetzelfde doel kunnen bereiken zijn er niet. Tevens zijn er maatregelen getroffen om de privacyrisico's voor betrokkenen weg te nemen: deze staan in het volgende hoofdstuk. Het restrisico dat overblijft is laag en dus acceptabel volgens de verwerkingsverantwoordelijke.

4 Risicobeoordeling en maatregelen

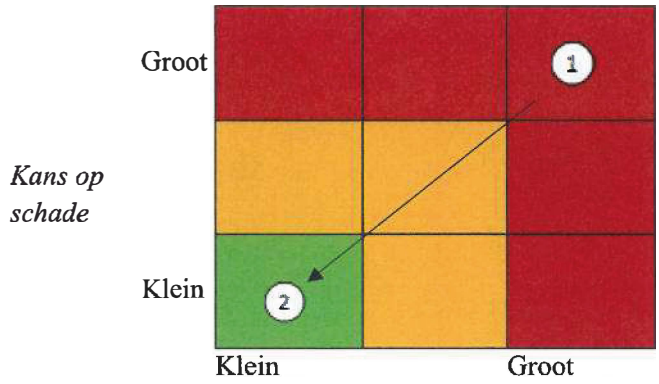
4.1. Methodiek

Het privacyrisico van het camerasysteem hangt af van de schade die een betrokkene kan ondervinden, gecombineerd met de kans dat die schade zich zal voordoen: risico = schade X kans.

1. Zonder beschermingsmaatregelen zijn camera's altijd een hoog risico voor betrokkenen. De schade voor betrokkenen als hun persoonsgegevens onbeveiligd worden verwerkt kan groot zijn. Ook de kans dat die schade zich voordoet is groot aangezien elk camerasysteem zonder beschermingsmaatregelen kwetsbaar is door opzettelijke of onopzettelijke fouten bij de verwerking van de persoonsgegevens. Daarom is het brutorisico van deze camerabewaking groot.

2. Door het treffen van beschermingsmaatregelen worden de bruto risico's verkleind tot een acceptabel netto risico.

Dat levert deze risicomatrix op:



4.2. Privacyrisico's en beschermingsmaatregelen

Er zijn twee privacyrisico's geïnventariseerd. Daar worden maatregelen voor getroffen om die te minimaliseren.

Risico 1: Heimelijk filmen
Het eerste risico is dat voorbijgangers zonder hun weten – dus heimelijk – worden gefilmd. Het is verboden heimelijk filmopnames te maken volgens het Wetboek van Strafrecht (art. 441b en 139f). In de AVG staat daarnaast dat transparantie over de verwerking door actief informeren van betrokkenen over de gegevensverwerking belangrijk is. De persoonlijke schade kan aanzienlijk zijn als mensen niet weten dat ze worden gefilmd of als ze niet weten wat het doel van

de camera's is, wat er met de opnames mag worden gedaan en wie toegang heeft. Ze kunnen zijn gefilmd op een plek, in een situatie of met andere personen waar ze liever niet gezien willen worden. Ze kunnen zich grote zorgen maken dat de opnames terechtkomen bij mensen die misbruik van die informatie gaan maken. De schade is in dat geval aanzienlijk en de kans dat die zich voordoet is niet te verwaarlozen. Dus is het risico 'gemiddeld' als geen beheersmaatregelen zouden worden getroffen.

Maatregelen

Om te zorgen dat mensen weten dat ze worden gefilmd, wordt op verschillende manieren informatie aangeboden over het camerasysteem. Dat is overigens niet alleen wenselijk om te voldoen aan de privacywetgeving: het vergroot ook het preventieve effect op mogelijke wetsovertreders en draagt dus bij aan de veiligheid op de bedrijventerreinen. Conform de richtlijnen van de European Data Protection Board wordt informatie in twee lagen aangeboden. De eerste informatielaag is fysiek: op straat wordt de belangrijkste informatie aangeboden op borden. De tweede informatielaag is digitaal: online wordt meer informatie aangeboden voor degenen die meer details willen of hun rechten als betrokkene willen uitoefenen, zoals het inzagerecht. De eerste laag van informatie verwijst naar de tweede laag.

Eerste informatielaag: borden op straat

Om het risico op heimelijk filmen te verkleinen tot een acceptabel 'nettorisico' worden voorbijgangers ter plaatse actief geïnformeerd over de camerabewaking. Er staan informatieborden bij alle toegangswegen tot de cameragebieden. Op de borden kan de voorbijganger zien wat het doel van de camerabewaking is en welke organisaties betrokken zijn.

Tweede laag: online informatie

Mensen die meer willen weten over de verwerking van hun persoonsgegevens kunnen terecht op de website van de Stichting. De online informatie over de verwerking persoonsgegevens is op de website van de Stichting gepubliceerd (http://www.sbbhg.nl). Hierop staat informatie over de camerabewaking en kunnen mensen lezen hoe ze als betrokkene hun rechten kunnen uitoefenen, zoals bijvoorbeeld het recht op inzage. Betrokkenen die zich willen beroepen op hun rechten kunnen zich wenden tot de verwerkingsverantwoordelijke van het camerasysteem.

Risico 2: Onbevoegden krijgen toegang tot de opnames

Het tweede risico is een heel breed risico. Er is een kans dat onbevoegden, met opzet of per ongeluk, toegang krijgen tot de camerabeelden, en dus tot de persoonsgegevens. Onbevoegden kunnen bijvoorbeeld hackers zijn, maar het zouden ook degenen kunnen zijn die na een strafbaar feit proberen de gemaakte beelden te wissen. Ook alle anderen die niet geautoriseerd zijn om de persoonsgegevens in te zien, zoals medewerkers van de bedrijven op de terreinen, mogen geen toegang krijgen tot de persoonsgegevens. Het risico bestaat dat onbevoegden opnames bekijken, bewerken, kopiëren, langer bewaren dan afgesproken of juist eerder verwijderen dan de

bedoeling is.

Zonder beschermingsmaatregelen is de kans hierop aanzienlijk. Het beeldmateriaal gaat immers digitaal door de videoketen van camera tot opslag. Zonder goede beveiliging is het mogelijk in die keten de gegevens te onderscheppen en te bewerken. Dit kan aanzienlijke schade opleveren voor de personen die in beeld zijn gekomen. Misbruik van de informatie kan (im)materiële nadelen opleveren, door afpersing of aantasting van de goede naam. Ook het verwijderen van opnames door onbevoegden kan schade opleveren voor de betrokkenen. Opnames kunnen immers nodig zijn als bewijsmateriaal en als ze worden verwijderd is dat niet meer mogelijk. Maar het verwijderen van opnames kan ook andersom nadelige gevolgen hebben. Beelden kunnen immers bewijzen dat een bepaalde persoon niets met het incident te maken heeft en dus ten onrechte als verdachte is aangemerkt. Dan kan die persoon van verder onderzoek worden uitgesloten. Als de beelden er niet meer zijn, vervalt die mogelijkheid en is er dus schade voor de betrokkenen. De mogelijke schade is in deze scenario's aanzienlijk en – zonder beheersmaatregelen – is het waarschijnlijk dat dit scenario zich zal voordoen: dit levert dus een hoog bruto risico op.

Maatregelen

Informatiebeveiliging

De informatieverwerking door Viewcontrol voldoet aan de norm ISO-27001. Voor het behouden van dit certificaat worden periodieke audits op de procedures uitgevoerd. Naar aanleiding van die audits worden aanvullende beschermingsmaatregelen doorgevoerd.

Camera's

De camera's zijn gemonteerd in een beveiligde behuizing die hufterproof is volgens de IP66 classificatie. Dat betekent dat de camera volledig beschermd is tegen stof en bestand is tegen zware weersomstandigheden, zoals stortregen. De camera's hangen op enkele meters hoogte waardoor ze niet eenvoudig bereikbaar zijn voor onbevoegden.

Opslag en videomanagement

De beelden worden opgeslagen op een beveiligde opslagserver in een afgesloten ruimte. Ter beveiliging worden technische, organisatorische en juridische maatregelen getroffen. Viewcontrol draagt er zorg voor dat de infrastructuur en de beelden niet toegankelijk zijn voor onbevoegden. De technisch beheerder zorgt ervoor dat apparatuur en software zodanig worden geselecteerd, geïnstalleerd en beheerd dat beeldmateriaal niet onopgemerkt kan worden bewerkt of gemanipuleerd.

Minimale gegevensverwerking

De politie is de enige instantie die opgenomen beelden mag gebruiken en het enige doel is opsporingsonderzoek. De politie neemt na ontvangst van de kopie van de relevante camerabeelden de verwerkingsverantwoordelijkheid over van de Stichting. De kopie valt onder de Wet politiegegevens, met eigen bewaartermijnen en eigen rechten voor de betrokkenen. Dit valt buiten deze DPIA omdat de politie de verwerkingsverantwoordelijke voor de kopie van de verstrekte

beelden is. Viewcontrol gaat niet in op verzoeken van anderen dan bevoegde opsporingsambtenaren. Het is dus onmogelijk dat een ondernemer of een andere 'derde' een kopie van de beelden krijgt. Dit zorgt voor doelbinding: de camerabeelden kunnen uitsluitend worden gebruikt in het kader van opsporingsonderzoeken en niet voor andere doeleinden. Als een ondernemer wil weten wat het opsporingsonderzoek oplevert, worden zij door de Stichting doorverwezen naar de politie.

Selectie deskundige en betrouwbare cameratoezichthouders
Alleen gekwalificeerde cameratoezichthouders met een daartoe behaald diploma mogen toezicht houden. De cameratoezichthouders worden gescreend door Viewcontrol en door de politie. Zij tekenen ook een geheimhoudingsverklaring.

Verwerkersovereenkomst
De verwerkingsverantwoordelijke (de Stichting) heeft een verwerkersovereenkomst gesloten met de verwerker (Alert Security / Viewcontrol). Daarin zijn afspraken vastgelegd die ervoor zorgen dat de verwerker zich aan dezelfde veiligheidsafspraken houdt als de verwerkingsverantwoordelijke. De basis onder de verwerkersovereenkomst is de hoofdovereenkomst tussen de Stichting en de verwerker. Als de verwerker een subverwerker inschakelt, zorgt de verwerker ervoor dat de afspraken uit de verwerkersovereenkomst ook onderdeel worden van de hoofdovereenkomst met de subverwerker. Zo wordt geborgd dat alle organisaties en werknemers in de gehele videoketen aan dezelfde afspraken gebonden zijn.

4.3. Eindoordeel over restrisico

Het brutorisico van de camera's is groot, maar door de beschermingsmaatregelen wordt dat teruggebracht tot een laag nettorisico. De waarschijnlijkheid dat de beschreven risico's zich voor zullen doen wordt hierdoor aanzienlijk verminderd en er worden beschermingsmaatregelen getroffen die de mogelijke schade voor betrokkenen wegnemen en beperken. De verwerkingsverantwoordelijke komt op grond hiervan tot de conclusie dat het restrisico acceptabel is.

Bijlage 1 – Verwerkersovereenkomst

Stichting Beveiliging Bedrijven Hardinxveld-Giessendam, verder te noemen Verwerkingsverantwoordelijke, hierbij rechtsgeldig vertegenwoordigd door de vice-voorzitter, de heer R.A. den Breejen,

en

Alert Security BV / Viewcontrol BV gevestigd te Sliedrecht, verder te noemen Verwerker, hierbij rechtsgeldig vertegenwoordigd door Commercieel Directeur, de heer J. Klaren,

hierna afzonderlijk te noemen "Partij", of gezamenlijk "Partijen"

Overwegen het volgende:

a) Partijen hebben op 1 juli 2023 een Hoofdovereenkomst afgesloten, op grond waarvan Verwerker camerabewaking levert aan de Verwerkingsverantwoordelijke;
b) Verwerker verwerkt voor de uitvoering van de Hoofdovereenkomst Persoonsgegevens voor Verwerkingsverantwoordelijke;
c) Op de verwerking van Persoonsgegevens door Verwerker zijn de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) van toepassing;
d) Partijen willen in aanvulling op de AVG en de UAVG de volgende afspraken over de verwerking van Persoonsgegevens vastleggen in deze verwerkersovereenkomst (hierna: de Verwerkersovereenkomst);

En komen het volgende overeen:

Artikel 1 Definities

1.1 Begrippen uit de AVG en de UAVG die in deze Verwerkersovereenkomst worden gebruikt, hebben dezelfde betekenis.

1.2 Bijlagen: aanhangsels bij deze Verwerkersovereenkomst, die onlosmakelijk deel uitmaken van deze Verwerkersovereenkomst.

Artikel 2 Ingangsdatum en duur

2.1 Deze Verwerkersovereenkomst gaat in op het moment dat de Hoofdovereenkomst tot stand is gekomen, tenzij Partijen anders overeenkomen.

2.2 Deze Verwerkersovereenkomst eindigt op het moment dat Verwerker de verwerking van Persoonsgegevens op grond van de Hoofdovereenkomst heeft beëindigd en de afspraken over het teruggeven en/of wissen van Persoonsgegevens zijn nagekomen.

2.3 Wanneer Partijen een (nieuwe) Verwerkersovereenkomst overeenkomen, betekent dat dat de oude Verwerkersovereenkomst komt te vervallen.

Artikel 3 Onderwerp van deze Verwerkersovereenkomst

3.1 Verwerker verwerkt de door of via Verwerkingsverantwoordelijke ter beschikking gestelde Persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke

voor de uitvoering van de Hoofdovereenkomst en uitsluitend overeenkomstig schriftelijke instructies van Verwerkingsverantwoordelijke, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke wettelijke bepaling hem tot verwerking verplicht. In dat geval zal Verwerker Verwerkingsverantwoordelijke, voorafgaand aan de verwerking, daarvan zonder onredelijke vertraging in kennis stellen, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

3.2 De Verwerker voert camerabewaking uit voor de Verwerkingsverantwoordelijke en verwerkt daarbij persoonsgegevens in de vorm van camerabeelden en gescande kentekens.

Artikel 4 Inhoudelijke afspraken

4.1 **Beveiligingsmaatregelen**

Verwerker zorgt voor passende technische en organisatorische maatregelen om de Persoonsgegevens goed te beveiligen, zoals bedoeld in artikel 32 AVG. Door de beschikking over het ISO-27001-certificaat toont Verwerker de passende technische en organisatorische maatregelen aan.

4.2 **Audits**

Verwerker verleent alle benodigde medewerking aan audits uitgevoerd door een gecertificeerde auditor over de nakoming van de afspraken binnen deze Verwerkersovereenkomst, tenzij Verwerker door middel van een geldige certificering, die periodiek door een geaccrediteerde instelling wordt getoetst, heeft aangetoond dat Verwerker de gemaakte afspraken nakomt. De kosten van deze audit worden gedragen door Verwerkingsverantwoordelijke (zowel eigen kosten als kosten van Verwerker), tenzij de auditor één of meer tekortkomingen van niet ondergeschikte aard van Verwerker constateert die ten nadele zijn van Verwerkingsverantwoordelijke.

4.3 **Verwerking buiten de EER**

Verwerker mag Persoonsgegevens niet buiten de Europese Economische Ruimte (laten) verwerken.

4.4 **Geheimhouding**

Personen die werken voor (sub)Verwerker en (sub)Verwerker zelf, moeten Persoonsgegevens waarmee zij werken geheimhouden. De personen die werken voor Verwerker en subverwerkers hebben daarom een geheimhoudingsverklaring getekend, of zich op een andere manier schriftelijk gebonden aan de geheimhouding.

4.5 **Subverwerkers**

Verwerkingsverantwoordelijke verleent toestemming aan de Verwerker voor de inschakeling van subverwerkers, mits de Verwerker aantoonbaar regelt dat de subverwerker aantoonbaar voldoet aan de AVG en aan de afspraken in deze Verwerkersovereenkomst. Verwerker houdt Verwerkingsverantwoordelijke op de hoogte van de beoogde inschakeling van nieuwe subverwerkers.

4.6 **Rechten van betrokkenen**

Als een betrokkene een beroep doet op zijn rechten zoals genoemd in artikel 12 t/m 22 AVG, helpt Verwerker Verwerkingsverantwoordelijke om daarop binnen de wettelijke termijnen een beslissing te nemen.

4.7 **Gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging**

Op verzoek van Verwerkingsverantwoordelijke werkt Verwerker altijd mee aan een gegevensbeschermingseffectbeoordeling (DPIA) en een voorafgaande raadpleging als bedoeld in artikel 35 en 36 AVG.

Artikel 5 Inbreuk in verband met Persoonsgegevens

5.1 Verwerker zal Verwerkingsverantwoordelijke zonder onredelijke vertraging, maar uiterlijk binnen 24 uur, informeren na vaststelling van een (vermoedelijke) Inbreuk in verband met Persoonsgegevens. Verwerker vermeldt hierbij voor zover bekend de vermeende oorzaak van de (vermoedelijke) Inbreuk, de categorie persoonsgegevens, de categorie betrokkenen en het aantal betrokkenen.

5.2 In geval van een Inbreuk neemt Verwerker zonder onredelijke vertraging alle maatregelen om de Inbreuk te herstellen, de gevolgen daarvan te beperken en verdere Inbreuken te voorkomen en houdt de Verwerkingsverantwoordelijke hiervan voortdurend op de hoogte.

5.3 Verwerker heeft een gedetailleerd logboek van de Inbreuken en de maatregelen die op Inbreuken zijn genomen. Verwerkingsverantwoordelijke mag dat inzien, wanneer deze daarom vraagt.

5.4 Verwerkingsverantwoordelijke beslist of de Inbreuk moet worden gemeld bij de toezichthoudende autoriteit en/of Betrokkene. Verwerker ondersteunt de Verwerkingsverantwoordelijke waar nodig bij de melding aan de toezichthoudende autoriteit en/of Betrokkene.

Artikel 6 Aansprakelijkheid

6.1 Eventuele in de Hoofdovereenkomst overeengekomen beperkingen van de aansprakelijkheid hebben ook betrekking op de Verwerkersovereenkomst.

Artikel 7 Beëindigen verwerkersovereenkomst

7.1 Partijen moeten in de Hoofdovereenkomst afspraken maken over de beëindiging van de Hoofdovereenkomst en de daaruit voortvloeiende teruggave en wissing van Persoonsgegevens.

7.2 De geheimhouding geldt ook nog na beëindiging van deze Verwerkersovereenkomst.

Artikel 8 Overige bepalingen

8.1 Op deze overeenkomst is Nederlands recht van toepassing. Alle geschillen, ook als alleen één Partij vindt dat er een geschil is, zullen in eerste instantie worden voorgelegd aan dezelfde bevoegde rechter als genoemd in de Hoofdovereenkomst.