FG-advies

Aan: het gemeentebestuur
Van: de functionaris gegevensbescherming
Betreft: aanbevelingen voor gespreksvoering over camera's

Datum: 9 september 2022
Versie: 1.1

Doel

Gebruik van camera's door de gemeente mondt gemakkelijk uit in privacydiscussies. Met dit advies lever ik graag een bijdrage door te verduidelijken wanneer camera's volgens de privacywetgeving problematisch zijn, en wanneer niet.

Deze notie bevat:

- Drie aanbevelingen voor goed gesprek
- Verdere toelichting

Inleiding

Praten over camera's hangt samen met de bredere vraag: wat voor gemeente wilt u in digitaal opzicht zijn in 2035? In hoeverre passen camera's bij de gemeentelijke visie op de toekomst en kernwaarden? Het antwoord is aan u, en bevindt zich ergens in het spectrum tussen het zijn van een volledig cameraloze gemeente tot aan 'Chinese toestanden'. Hierbinnen positie nemen is een keuze.

Maar die keuze dient wel te passen in het huidige tijdsgewricht. Camera's zijn nu eenmaal breed verkrijgbaar, ze bestaan in soorten en maten, en worden overal gebruikt. Er zitten er zelfs meerdere in je mobiele telefoon. Ook uw gemeente heeft op technologische en maatschappelijke in te spelen. Tegelijk mag je verwachten dat cameraoplossingen nuttig zijn.

1e aanbeveling

*Mijn eerste aanbeveling is daarom om te **praten over het nut** van een specifieke cameratoepassing. Wat kan het precies en waarom heeft dat de voorkeur boven andere oplossingen?*

Degene die daarover gaat, de eigenaar (zie hierna), moet dat kunnen uitleggen.

Privacybescherming

Zoals met alles, hebben camera's ook nadelen. Meestal denken we meteen aan privacyrisico's. Hoe terecht is dat?

In de afgelopen decennia is er veel over privacy gediscussieerd en nagedacht. Dat heeft zowel geresulteerd in afspraken over hoe je privacy beschermt, als de norm 'wat is privacy en wat is privacybescherming?'. Sinds 2016 bepalen EU-verordening 2016/679 (de AVG) en EU-richtlijn 2016/680 het antwoord en, daarachter, het EU-handvest Grondrechten.

Op nationaal niveau zijn er vervolgens nog andere wetten en regelingen om rekening mee te houden. Maar omdat EU-recht prevaleert, schrijf ik deze notitie naar Europees recht. Dat maakt het meteen ook overzichtelijker. Althans; over cameragebruik door gemeenten bevat de Gemeentewet een bijzondere bepaling, artikel 151c, die specifieke aandacht verdient. Ook daarover daarom hierna meer.

Meest belangrijk op dit punt, is om bij gesprekken over camera's de volgende tweedeling voor ogen te houden:

- De AVG beschermt tegen onverantwoord gebruik van camerabeelden die worden gemaakt voor particuliere en bestuurlijke doelen (beeldverwerking in privaatrechtelijke en bestuurlijke informatieketens).

- Richtlijn 2016/680 – in Nederland vooral bekend als de Wet politiegegevens – beschermt tegen te gemakkelijke verkrijging of gebruik van camerabeelden voor opsporing en vervolging van strafbare feiten, en bestraffing (beelden die bestemd zijn voor de justitieketen).

Die tweedeling is terug te voeren op de lessen die nationaal en internationaal zijn getrokken uit de periode 1939-1945, en werden verankerd in mensenrechtenverdragen, waar de AVG en Richtlijn 2016/680 direct mee in verband staan. Om voortaan de rechtsstaat te waarborgen, is door middel van dubbele EU-wetgeving voorzien in twee gescheiden werelden – ieder met zijn eigen spelers (scheiding van machten).

Nederlandse gemeenten vallen voornamelijk onder het regime van de AVG. Maar daar waar een gemeente bijzondere opsporingstaken heeft (denk bijvoorbeeld aan het werk van de leerplicht-ambtenaar), geldt toch ook Richtlijn 2016/680. Evengoed heeft in deze wereld het gemeentebestuur het voor het zeggen. In de opsporingswereld ligt de zeggenschap voornamelijk bij de korpschef of het college van procureurs-generaal.

Dat het twee gescheiden werelden zijn, wil niet zeggen er geen onderlinge uitwisseling van informatie mogelijk is, maar dat moet voldoen aan strenge voorwaarden. Zie voor de regelingen op dit vlak in de eerste plaats het Wetboek van strafvordering, maar ook het al aangehaalde artikel 151c Gemeentewet. Daarnaast zijn er zijn er nog enkele ministeriële regelingen in verband met bijzondere opsporingsbevoegdheid.

In gesprekken over camera's blijft de tweedeling echter vaak onderbelicht, waardoor camera's voor particuliere en bestuurlijke doelen gemakkelijk over één kam geschoren worden met opsporingscamera's ('je wordt in de gaten gehouden'). Maar is dat wel zo? Een particuliere beveiligingscamera houdt in de regel niet joù in de gaten. Neem bijvoorbeeld camera's voor beveiliging van een tankstation. Pas als je wegrijdt zonder te betalen, is het aannemelijk dat camerabeelden worden gebruikt om je te achterhalen. Zolang dat niet speelt, worden beelden al snel weer gewist door ze met nieuwe beelden te overschrijven, bijvoorbeeld na 48 uur.

2e aanbeveling

*Bespreek **het primaire doel** van een cameratoepassing. Hoe werkt de camera? Wie heeft toegang tot de beelden. Wat gebeurt er mee? Met wie worden ze gedeeld?*

- Camera's voor particulier gebruik zijn meestal bedoeld voor beveiliging (gebouwen, persoonsbeveiliging, balies, terreinen), communicatie – denk aan thuiswerken en nieuws of herinneringen voor later.
- Camera's voor bestuurlijk gebruik ondersteunen een gemeentelijke taak op het gebied van dienstverlening, openbare orde, belastingheffing). Typische voorbeelden zijn camera's om het straatbeeld te monitoren, verkeersdoorstroming, de camera's voor controles op betaling van parkeerbelasting of camera's voor ruimtelijke inrichting of bijvoorbeeld vaststelling van WOZ-waarde.
- Camera's in het domein van Richtlijn 2016/680 mogen alleen worden ingezet op basis van opsporingsbevoegdheid. Typische voorbeelden zijn camera's voor verkeersovertreding, camera's op plekken waar ernstige ordeverstoring worden verwacht, verborgen camera's voor opsporingsonderzoek, infraroodcamera's tegen hennepkwekers, enzovoorts.

Passende waarborgen

Door voorschriften uit de AVG en Richtlijn 2016/680 te volgen (beide weten zijn vooral een handboek als je door de wetgevingstaal heen leest), krijg je cameratoepassingen die met allerlei privacywaarborgen zijn omkleed.

Films of boeken zoals *1984*, *The Circle*, *Enemy of The State* en *Minority Rapport* of *Weapons of Math Destruction* zetten terecht aan het denken. Maar bij goede toepassing van de AVG en Richtlijn 2016/680 hoef je niet bang te zijn voor de scenario's die ze schetsen. Tenminste; we zijn nog in afwachting van de nieuwe EU-wet voor bescherming tegen algoritmes. Maar op basis van de AVG en Richtlijn 2016/680 komen we ook al een eind.

Als uitvloeisel van de AVG en Richtlijn 2016/680, is het vast beleid volgens het gemeentelijk privacybeleidskader, óók ten aanzien van cameratoepassingen:

1. dat er privacyrisico-analyses worden uitgevoerd (DPIA's);
2. er bijpassende beschermingsplannen worden opgesteld (procesplannen);
3. deze daadwerkelijke worden uitgevoerd (managementverantwoording);
4. op daadwerkelijke bescherming worden gecontroleerd (zo nodig zelfs audits)
5. en worden geëvalueerd op doelmatigheid en doeltreffendheid (behoorlijk bestuur).

De DPIA-fase is meteen ook het moment voor inspraak. Onbeschermde cameratoepassingen komen, als het goed is, dan ook niet voor.

3e aanbeveling

Besteed vooral aandacht aan de specifieke privacywaarborgen waarmee een cameratoepassing is omkleed.

Vergeet hierbij ook niet hoe het zit met de algemenere waarborgen: informatieverstrekking, waar mensen terecht voor uitoefening van rechten (recht op uitleg, inzage, correctie, …), het meldpunt datalekken en de FG-ombudsregeling bij klachten.

Verantwoordelijk

Degene die voor dit alles verantwoordelijk is, is degene met de uiteindelijke beslissings-bevoegdheid; de eigenaar. Hij moet niet alleen het waarom van een cameratoepassing kunnen uitleggen maar vooral ook hoe het precies geregeld is met de privacybescherming.

- Bij gemeentelijke camera's voor particulier gebruik ligt het eigenaarschap bij het dagelijks bestuur van de gemeenteorganisatie.
- In de bestuurlijke sfeer en waar Richtlijn 2016/680 speelt, ligt het eigenaarschap bij het verantwoordelijke bestuursorgaan, dus het college, de burgemeester of de raad.

De eigenaar wordt hierin bijgestaan door het management ('proceseigenaarschap'), het privacy-ondersteuningsteam, eventueel andere stafafdelingen en concerncontrol. Waar passend komt er zelfs een externe auditor aan te pas om te controleren of ook inderdaad volgens afspraak privacybeschermende maatregelen zijn genomen. Momenteel speelt dit in het kader van Richtlijn 2016/680 (de WPG-audits).

Toetsing aan de wet

De toetsing of bij een cameratoepassing de AVG of Richtlijn 2016/680 naar behoren zijn nageleefd, is uiteindelijk aan de FG – wat neerkomt op een keuring. Landelijk wordt gewerkt aan de mogelijkheid dat ook erkende expertisebureaus zulke keuringen mogen doen. Dat zou op termijn betekenen dat cameratoepassingen van een wettelijk certificaat en keurmerk kunnen worden voorzien.

Toetsing van een specifieke cameratoepassing heb ik voor uw gemeente nog niet gedaan. Maar om een indruk te geven, komt deze beoordeling van de Hilversumse druktemeter meest dicht in de buurt.

Sergej Katus

_____

Mr. S.H. Katus
Functionaris gegevensbescherming
fg@pmpartners.nl
www.pmpartners.nl

Verdere toelichting

Hoever gaat het recht op privacy?

Privacy wordt vaak omschreven als het recht om met rust te worden gelaten. Maar dat is een ideaal. Juridisch bestaat dit recht niet – tenminste, niet letterlijk en ook niet zo absoluut. Het recht op privacy ligt dus genuanceerder.

Zonder hier een verhandeling over grondrechten te houden, merk je dat meteen al aan de juridische benaming van het recht op privacy: het recht op bescherming van de persoonlijke levenssfeer. Dat is vooral iets fysieks, maar hangt ook samen met informatieverwerking.

Om er beter gevoel bij te krijgen, is een gemakkelijke vuistregel dat de privacy van je woning absoluter is dan privacy op je werk of op straat.

In je woning moet je je ongezien kunnen terugtrekken of bezoek ontvangen, terwijl je op het werk en op straat weet dat je gezien wordt. Toch bestaan er ook de bevoegdheden om zelfs woningen te betreden, te observeren of af te luisteren als daar goede reden voor is. Dat is allemaal streng gereguleerd en dat is óók privacybescherming.

Als op straat een camera hangt, word je – afhankelijk van de werking van het camerasysteem – in principe ook door die camera 'gezien'. Of dat ook meteen een privacyprobleem is, hangt er maar vanaf.

Je privacyrisico

De AVG en Richtlijn 2016/680 'slaan aan' als met een camera beelden worden gemaakt waardoor de gemeente of een derde, jou zonder onevenredig veel moeite zal of kan identificeren. Zie voor dit criterium artikel 4.1, 25 en overweging 26 AVG. En artikel 3.1, 20 en overweging 21 Richtlijn 2016/680. Naar voormalig privacyrecht noemen we dit vaak 'herleidbaarheid'.

- Bij de ene cameratoepassing is de kans op identificatie theoretisch ('de Chinezen' – hoe groot is werkelijk de kans dat iemand in China zodanig geïnteresseerd is wie zich in het winkelgebied bevindt dat hij er geld, tijd en energie voor over heeft om je te identificeren, om daar vervolgens in te slagen?). Of zelfs 100% onmogelijk.

- Bij de andere cameratoepassing is de kans op identificatie reëel genoeg of is dat ook helemaal de bedoeling. Pas in deze categorie classificeren de beelden zich als 'persoonsgegevens'. Ze hebben betrekking op jou, zeggen iets over jou en je bent geïdentificeerd of identificeerbaar.

Toch is zelfs identificeerbaarheid nog niet meteen een privacyrisico. Dat wordt het pas als een cameratoepassing *niet* voldoet aan dé twee kerneisen in zowel de AVG als Richtlijn 2016/680: (a) dat de cameratoepassing rechtmatig is; en (b) met passende waarborgen is omkleed.

Pas als aan één of beide voorwaarden niet is voldaan, kun je spreken van schending van de privacywetgeving. Het privacyrisico is de waarschijnlijkheid dat je hierdoor schade ondervindt. Om dat risico te duiden, hanteert de gemeente het classificatiesysteem volgens de 'Schaal van Erg'. Zie hiervoor het gemeentelijk privacybeleid, en ook overweging 76 AVG / overweging 52 Richtlijn 2016/680.

Privacy by design

Een typisch risico van bewakingscamera's is dat beelden onjuist worden geïnterpreteerd, waardoor je ten onrechte met iets in verband wordt gebracht zoals een verdenking. Of dat je woning zonder geldige reden in de gaten gehouden wordt, wat werkelijk een inbreuk op je persoonlijke levenssfeer inhoudt. Want de privacy van je woning – zoals eerder aangegeven – telt immers extra zwaar.

Dit zijn maar twee voorbeelden. Of en met welke privacyrisico's rekening moet worden gehouden, valt alleen maar per cameratoepassing te beoordelen. Het is daarom wezenlijk om goede risico-analyses uit te voeren in de vorm van data protectie impact assessments (DPIA's). 'Met passende waarborgen omkleed', wil zeggen dat aan de hand van zo'n DPIA vervolgens in passende oplossingen is voorzien om de geconstateerde risico's tegen te gaan. De cameratoepassing voldoet dan aan de eisen van 'privacy by design' (zie artikel 25 AVG / artikel 20 Richtlijn 2016/680).

Privacy by design kan zo ver gaan dat een cameratoepassing in hoge mate anonimiteit garandeert. De camera's lijken op camera's maar ze zijn het eigenlijk niet. Bijvoorbeeld de camera van de slagboom van een parkeergelegenheid die bij het wegrijden automatisch open gaat. Als dat technisch zo is aangepakt dat het parkeersysteem uitsluitend werkt op basis van kentekenherkenning (de camera filtert al het andere weg), is dat een toonvoorbeeld van privacy by design. In het jargon moet ik eigenlijk spreken van 'sterke pseudonimisering' maar de strekking is dat je anoniem parkeert en wegrijdt – voor het systeem volstaat de wetenschap dat je betaald hebt.

Eigenaarschap

Alles staat of valt met 'goed eigenaarschap', dat wil zeggen de regievoering door de eigenaar op passende waarborgen en duurzame beheer ervan, en zijn vermogen om hierover verantwoording af te leggen. Wettelijk heet dat 'de verantwoordelijkheid/plicht van de verwerkingsverantwoordelijke'.

Zoals al aangegeven; het eigenaarschap voor verwerking van persoonsgegevens voor particuliere doelen ligt bij het dagelijks bestuur (degene die uiteindelijk beslist door vaststelling van doel en middelen). Het eigenaarschap in de bestuurlijke sfeer of bij opsporing, ligt bij het bestuursorgaan, de overheidsinstantie of autoriteit waaraan de taak is opgedragen. Zie artikel 4.7 en artikel 24 e.v. AVG, artikel 4.8 en 20 e.v. Richtlijn 2016/680, evenals de uitleg over expliciete en impliciete verwerkingsverantwoordelijkheid in EU-richtsnoeren 07/2020.

Eigenaarschap is naar zijn aard niet af te wentelen op een ander, omdat het onlosmakelijk verbonden is met het particuliere of publieke belang dat wordt nagestreefd, zoals bedrijfsveiligheid, goed werkgeverschap, milieubeheer, wonen, werken, sociale zaken, re-integratie enzovoorts. Specifiek toegepast op camera's, is het besluit om ze in te zetten, automatisch gekoppeld aan de verantwoordelijkheid om daar dan ook goed eigenaarschap over te betrachten. Vergeet niet dat het in de kern gaat om de bescherming van grondrechten – dus de bestuurlijke borging dát je bescherming van grondrechten duurzaam wordt gegarandeerd.

In de praktijk wordt eigenaarschap nog wel eens verward met operationele zeggenschap. Dat is problematisch omdat daardoor vaak het eigenaarschap waar het in deze handreiking over gaat, niet meer wordt gevoeld. Bij operationele zeggenschap gaat het er om wie in de uitvoering de gegevensverwerking aanstuurt, dus de manager. Of bij uitbesteding, de uitvoeringsorganisatie (vestiging 'verwerkerschap' – zie artikel 28 AVG / 22 Richtlijn 2016/680).

Het eigenaarschap waar het in deze notitie over gaat is het bestuurlijk eigenaarschap en de bestuurlijke regievoering (*good governance*). Sinds jaar en dag (TK 1997-1998, 25892, p. 57) ligt die

opdracht – naar gelang de bevoegdheidsverdeling – bij het college, de burgemeester of de raad. Onder de AVG en Richtlijn 2016/680 is dat des te meer het geval. Vandaar nu ook het recht van iedere gedupeerde op volledige schadevergoeding bij gebrekkig eigenaarschap volgens artikel 82 AVG / 56 Richtlijn 2016/680, en bestuurlijke boete c.q. bestraffing volgens artikel 83 AVG / 57 Richtlijn 2016/680.

Artikel 151c-camera's

Camera's zijn er in soorten en maten. Uit het voorgaande komt naar voren dat er pas iets zinnigs over camera's valt te zeggen als zowel de eigenschappen als het eigenaarschap voldoende duidelijk zijn – waarbij het vooral gaat om de vraag hoe camerabeelden nou eigenlijk worden verwerkt, en waar ze verder nog terecht komen.

De meest spannende camera's die een gemeente mag inzetten, zijn de camera's volgens artikel 151c Gemeentewet. Het lijken politiecamera's omdat ook de politie er aan te pas komt, maar zijn dat juist *niet* omdat ze onder gemeentelijk gezag staan (en daarmee ook *uitsluitend* onder gemeentelijk gezag, zie artikel 29 AVG / 23 Richtlijn 2016/680). Ze zijn specifiek bedoeld voor situaties waarin ernstige verstoring de openbare orde speelt of dreigt te spelen in de vorm van overlast, geweld of criminaliteit. Logischerwijs zijn ze ook in te zetten voor de bewaking van de publieke veiligheid bij evenementen (discretionaire bevoegdheid).

Hoe dan ook, artikel 151c-camera's zijn geen opsporingsmiddel maar zijn in eerste instantie instrumenteel voor de handhaving van de openbare orde, en dat is een bestuurlijke taak (artikel 172 Gemeentewet). Tegelijk legitimeert artikel 151c dat beelden ook voor opsporing en vervolging mogen worden gebruikt. Daarmee worden de werelden van de AVG en Richtlijn 2016/680 aan elkaar gekoppeld – alleen dan wel volgens een specifiek protocol.

- Groen gemarkeerd de stappen van het protocol
- Blauw gemarkeerd hoe rechtmatige inzet van artikel 151c-camera's ontstaat
- Geel gemarkeerd waaruit blijkt wie de eigenaar is (de verwerkingsverantwoordelijke, zie hiervoor)
- **In vet** overige wettelijke privacywaarborgen

> *Artikel 151c Gemeentewet*
>
> *1. De raad kan bij verordening de burgemeester de bevoegdheid verlenen om, indien dat in het belang van de handhaving van de openbare orde noodzakelijk is, te besluiten om **voor een bepaalde duur** camera's in te zetten ten behoeve van het toezicht op een openbare plaats (…).*
>
> *2. De burgemeester besluit (…):*
>
> *a. **binnen welk gebied**, bestaande uit openbare plaatsen of andere voor een ieder toegankelijke plaatsen (…) camera's worden ingezet;*
>
> *b. **voor welke duur** de gebiedsaanwijzing plaatsvindt.*
>
> *3. De burgemeester stelt, **na overleg met de officier** van justitie in het [driehoeksoverleg], (…), de **periode** vast waarin (…) daadwerkelijk gebruik van de camera's plaatsvindt en de met de camera's gemaakte beelden in elk geval rechtstreeks worden bekeken.*
>
> *4. De burgemeester bedient zich bij de uitvoering (…) van de **onder zijn gezag staande politie**.*
>
> *5. De burgemeester **trekt het besluit (…) in zodra** de inzet van camera's **niet langer noodzakelijk** is (…).*
>
> *6. De aanwezigheid van camera's als bedoeld in het eerste lid is **op duidelijke wijze kenbaar** voor een ieder die het gebied (…) betreedt.*
>
> *7. Met de camera's worden **uitsluitend beelden** gemaakt **van een openbare plaats** (…).*

> *8. Ten behoeve van de handhaving van de openbare orde worden in het kader van het toezicht [op een openbare plaats] (…) gegevens verwerkt.*
> *9. De verwerking van [deze] gegevens (…) is een verwerking als bedoeld in [Richtlijn 2016/680], met dien verstande dat (…)* ***vastgelegde beelden na*** *ten hoogste* ***vier weken*** *worden* ***vernietigd*** *[tenzij] (…) er concrete aanleiding bestaat te vermoeden dat die gegevens noodzakelijk zijn voor de opsporing van een strafbaar feit, [en deze] ten behoeve van de opsporing (…) worden verwerkt.*
> *(…)*

Het eigenaarschap van de burgemeester eindigt wanneer alle beelden ook weer zijn vernietigd. Bezien vanuit de AVG, is het gebruik van openbare orde-beelden voor opsporingsonderzoek een vorm van verdere verwerking in de zin van artikel 6.4 AVG. De politiemensen die het feitelijke werk doen, leent de burgemeester in. Volgens het gemeentelijk beleidskader wijst hij voor de dagelijks aansturing daarvoor een manager aan die onder zijn gezag staat ('proceseigenaar').

Bij het delen van de beelden met het OM (en wellicht ook met de politie in het kader van breder opsporingsonderzoek), ontstaat aan verkrijgingszijde automatisch nieuw eigenaarschap. De burgemeester is bij rechtmatige verstrekking niet meer verantwoordelijk voor wat er verder nog met de beelden wordt gedaan.

Voor opsporingsonderzoek en rechtmatige verstrekking is vereist dat de beelden iets zeggen over strafbare feiten. Want pas onder die voorwaarde kan er sprake zijn van een verwerking in de zin van Richtlijn 2016/680. Wat dat betreft, behoeft het 9e lid van artikel 151c enige nuancering.

Zolang 151c-camera's uitsluitend het normale leven registreren, zijn de beelden nooit Richtlijn 2026/680-beelden. Weliswaar worden ze bekeken door de politie, maar dan enkel met de pet op als ordehandhaver – niet anders dan wat een agent ziet als hij/zij door de straat loopt (surveillance). 151c-camera's zijn daarom primair *toezicht*camera's. Bij een zorgvuldige aanpak, zijn goedwillende passanten die in beeld komen niet bij voorbaat verdacht.

De FG heeft tot taak om te adviseren over en toe te zien op de naleving van de AVG, Richtlijn 2016/680, gerelateerde wet- en regelgeving en het gegevensbeschermings-beleid van de gemeente. Dit doet hij in onafhankelijkheid en in samenwerking met de Autoriteit Persoonsgegevens. Hij let in het bijzonder op de risico's voor de rechten en vrijheden van personen.

FG's zijn aangewezen op grond van hun professionele kwaliteiten, in het bijzonder hun deskundigheid op het gebied van het gegevensbeschermingsrecht en de praktijk. Dit FG-advies vloeit dan ook voort uit toepassing van het EU-publiekrecht - met name het EU Handvest Grondrechten, de AVG en Richtlijn 2016/680 en de richtsnoeren van het EU-comité voor interpretatiecoördinatie, de EDPB. Voor herziening is ruimte bij valide argumenten binnen hetzelfde stramien.

Met Nederlandse wet- en regelgeving is rekening gehouden, met voorrang aan het Unierecht bij onduidelijkheid, dubbelzinnigheid of tegenstrijdigheid. Ook opvattingen en advies van anderen zijn meegenomen (dank daarvoor!), voor zover dat past binnen de bedoeling, het systeem en de bewoording van de AVG en Richtlijn 2016/680. Ook de uitspraak van de Rechtbank Rotterdam van 1 maart 2022 (ROT 20/4974) is meegewogen, alleen paste de rechter niet het Unierecht toe. Want zoals uitgelegd; 'operationele regie' is niet het criterium en de korpschef is geen gezagsdrager volgens de Gemeentewet. Per definitie is hij niet de verwerkingsverantwoordelijke.

Dit advies is een FG-aanwijzing in de zin van overweging 77 AVG.

#LeesdeAVGbeter

Privacy
Management
Partners
Coöperatie UA
adres
Vondellaan 58
3521 GH Utrecht
telefoon
+31 85 401 38 66
e-mail
info@pmpartners.nl
website
www.pmpartners.nl