Mr. F.B.M. Olijslager

Cameratoezicht en de AVG

Steeds vaker wordt cameratoezicht toegepast als middel om toezicht te houden op goederen, gebouwen en terreinen, voor toezicht op productieprocessen en om inbreuken op eigendomsrechten en ander onregelmatigheden vast te leggen als bewijsmateriaal. In dit artikel wordt aandacht besteed aan de juridische aspecten van cameratoezicht in de "private" context en de relatie met de Algemene Verordening Gegevensbescherming (AVG). Onder private context valt cameratoezicht door bedrijven (zoals fabrieken, winkels en horecaondernemingen), instellingen (zoals scholen, overheden en zorginstellingen), cameratoezicht op de werkplek door werkgevers en cameratoezicht door particulieren in en rond woningen Degene die verantwoordelijk is voor cameratoezicht wordt in dit artikel "rechthebbende" of "verwerkingsverantwoordelijke" genoemd. Dat kan een eigenaar van een pand of terrein zijn, maar ook de huurder.

Voor rechthebbenden van gebouwen en terreinen liggen verschillende overwegingen ten grondslag aan de keuze om camera's te gebruiken. Zo worden camera's gebruikt voor de gecontroleerde toegang tot gebouwen en terreinen in die zin dat het beeld op de monitor bepaalt of de receptiemedewerker wel of geen toegang verleent. Bij terrein of objectbewaking verschaffen camera's permanente informatie en geeft één persoon de mogelijkheid om snel grote terreindelen of meerdere objecten nagenoeg gelijktijdig te observeren. Incidenten en ongewenste situaties kunnen vroegtijdig worden ontdekt, waardoor de reactietijd aanzienlijk kan worden verkleind. In het geval van vermeende onregelmatigheden kunnen de vastgelegde beelden tevens als bewijs worden gebruikt. De technologische ontwikkelingen zorgen voor toepassingen waardoor het steeds aantrekkelijker wordt om cameratoezicht te gebruiken. Zo kan de toegang vrijwel zonder menselijk ingrijpen worden verleend als camera's zodanig geprogrammeerd zijn dat zij scannen, selecteren en toegang verlenen op basis van biometrische gelaatskenmerken of vooraf ingevoerde kentekens.

Algemene Verordening Gegevensbescherming

De Algemene Verordening Gegevensbescherming (AVG) geldt vanaf 25 mei 2018. De AVG is ook wel bekend onder de Engelse naam: General Data Protection Regulation (GDPR). De AVG wordt in Nederland aangevuld met de Uitvoeringswet AVG. In dit artikel wordt de structuur van de AVG verhelderd en worden de praktische consequenties van de AVG besproken in relatie tot cameratoezicht. De AVG bevat voorschriften van dwingend recht wat betekent dat contractuele bepalingen die afwijken van de AVG niet zijn toegestaan.

Toepasselijkheid AVG

De AVG richt zich op persoonsgegevens . Een persoonsgegeven kan direct of indirect identificerend zijn. Direct identificerende gegevens zijn gegevens als naam, een afbeelding of het BSN-nummer. Alleen of in combinatie met elkaar zijn ze dermate uniek en kenmerkend voor iemand dat hij met een vrij grote mate van zekerheid kan worden geïdentificeerd. Een voorbeeld van een indirect identificerend gegeven is het kenteken van een motorvoertuig. Via een aantal stappen kan het kenteken worden teruggebracht tot de persoon die als bestuurder optrad. Indien een camera-afbeelding niet scherp genoeg is, kan toch sprake zijn van een persoonsgegeven indien herleiding mogelijk is in combinatie met andere beschikbare gegevens. Als voorbeeld kan gedacht worden aan een gevelcamera bij een geldautomaat van een bank, waar met behulp van transactiegegevens alsnog de identiteit van

de vaag afgebeelde klant kan worden achterhaald. Als hiervoor te veel moeite moet worden gedaan is van een persoonsgegeven geen sprake.

De AVG is van toepassing indien persoonsgegevens geheel of gedeeltelijk geautomatiseerd worden verwerkt. Bij geautomatiseerde verwerking worden de gegevens op de harde schijf van een computer of op een bedrijfsserver opgeslagen. Via verschillende zoekmogelijkheden kunnen beeld, geluid en andere persoonsgegevens snel worden teruggevonden en met elkaar worden gecombineerd.

Wanner is de AVG niet van toepassing?

De volgende vormen van cameratoezicht vallen niet onder de AVG:
1. Cameratoezicht dat alleen het actuele moment registreert, niet opneemt en als het ware het verlengde oog van de gebruiker is (slechts monitoren)[1];
2. Camerasystemen waarbij de opnamen niet herleidbaar zijn tot individuele natuurlijke personen (bijvoorbeeld bij gebruik van een camera die alleen een zeer lage kwaliteit infraroodbeelden registreert).
3. Cameratoezicht voor uitsluitend persoonlijke of huishoudelijke doeleinden.[2]

Vaak is wel sprake van de vastlegging van persoonsgegevens. Indien een afbeelding niet scherp genoeg is, kan toch sprake zijn van een persoonsgegeven indien herleiding tot individuele personen mogelijk is in combinatie met andere beschikbare gegevens. Denk daarbij bijvoorbeeld een camera bij de toegang van bedrijven, waar met behulp van het toegangsbeheersingssysteem alsnog de identiteit van de vaag afgebeelde persoon kan worden achterhaald. Als hiervoor te veel moeite moet worden gedaan is van een persoonsgegeven geen sprake.

Voorbeelden cameratoezicht voor persoonlijk en huishoudelijk gebruik
- Een woningeigenaar hangt een camera op in zijn woning ter beveiliging van zijn gezin en eigendommen. De camera filmt alleen het interieur van de woning.
- Een woningeigenaar hangt een camera op in zijn tuin ter beveiliging van zijn gezin en eigendommen. De camera filmt alleen de tuin en niet de openbare weg.
- Een persoon bevestigt een camera aan zijn jas (een zogenoemde ‘bodycam’) en wil daarmee de omgeving voor zichzelf filmen wanneer hij op straat loopt. Op deze beelden zullen ook andere mensen in beeld worden gebracht. Er is sprake van uitsluitend persoonlijk of huishoudelijk gebruik, als deze persoon de camerabeelden niet verder verstrekt worden aan derden (dis niet publiceren).

Geen sprake van persoonlijk en huishoudelijk gebruik
- Een particulier zet camerabeelden waarop andere mensen staan op YouTube of Twitter.
- Een woningeigenaar hangt een camera op in zijn woning ter beveiliging van zijn gezin en eigendommen. De woningeigenaar heeft een kapsalon aan huis. De camera zal ook de klanten

[1] De Autoriteit Persoonsgegevens heeft een afwijkende mening dan de auteur van dit hoofdstuk. De Autoriteit Persoonsgegevens stelt op blz. 16 en 17 van de Beleidsregels Cameratoezicht. “Bij digitale camera’s worden intern geheugen en een digitale processor gebruikt om de beeldgegevens op te slaan en door te zetten tussen verschillende componenten van het systeem. Dus wordt dat dit proces – hoe tijdelijk ook van karakter – altijd wordt beschouwd als een verwerking in de zin van de AVG. Het actief gebruik van opnamefunctionaliteiten is niet relevant om te bepalen of er sprake zal zijn van een verwerking in de zin van de AVG. Dit betekent dat er bij het gebruik van een digitale camera altijd een verwerking van persoonsgegevens plaatsvindt, ook als beelden niet actief worden vastgelegd. Daarmee is het live uitkijken middels een digitale camera een verwerking van persoonsgegevens en is de AVG van toepassing.” De auteur van dit handboek is het daarmee niet eens. Alle artikelen van de AVG suggereren beeldopslag. Vergelijk art. art. 5 lid 1 onder e AVG over het bepalen van de bewaarduur; art. 6 lid 4 AVG over verder verwerken(dan moet er wel iets zijn dat verder verwerkt kan worden) en art. 13 AVG over het informeren van betrokkene in verband met de uitoefening van diens rechten uit art. 15 AVG (rectificatie en verwijdering’. Al deze artikelen impliceren dat er reproduceerbare beeldopslag is.

[2] In december 2014 heeft het Hof van Justitie een uitspraak gedaan over de uitzondering persoonlijk en huishoudelijk gebruik. De ging over de vraag of uitzondering wel/niet van toepassing is als sprake is van het doorlopend vastleggen van (gedeelten) van openbare ruimte met een vaste/statische camera voor het doeleinde: beveiliging van personen, gebouwen, terreinen, zaken en productieprocessen. Voor het deel openbare ruimte dat gefilmd wordt voor beveiligingsdoeleinden, heeft het Hof van Justitie bepaald dat geen sprake is van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden, en daarmee is de AVG dus onverkort van toepassing.

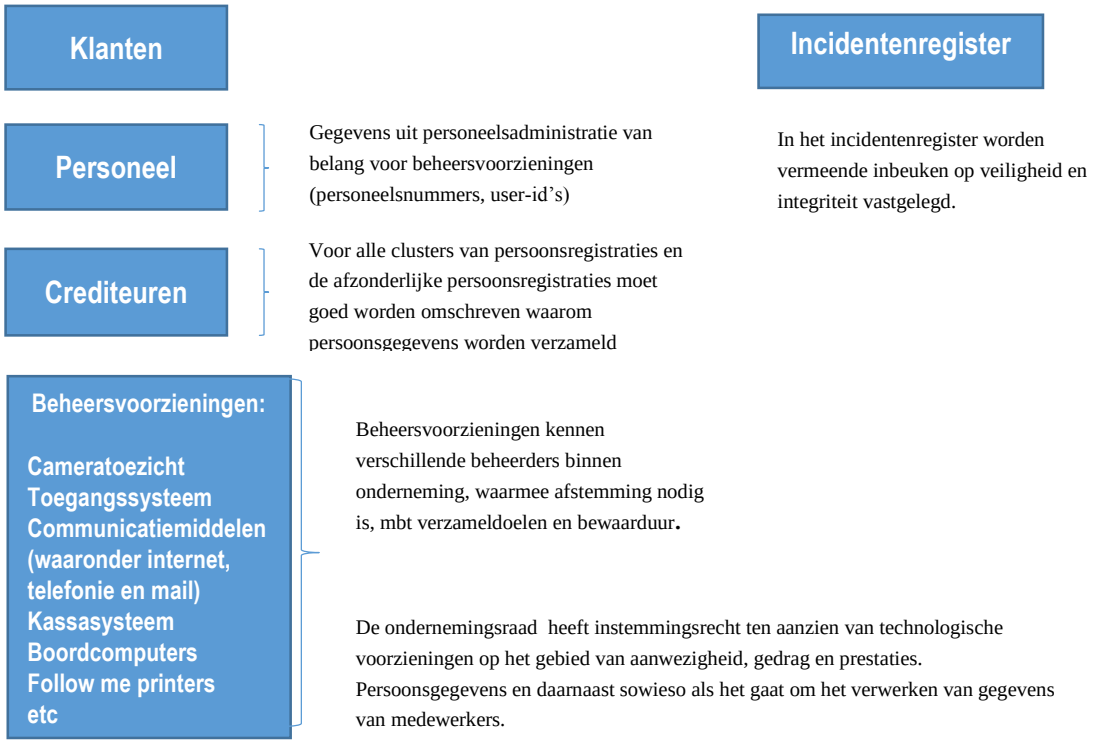
van de kapsalon filmen. Daarmee raakt het cameratoezicht buiten de privésfeer van de woningeigenaar.

Verwerkingsregister
Artikel 30 AVG bevat de verplichting voor de "verwerkingsverantwoordelijke" om een register bij te houden van alle categorieën van verwerkingen van persoonsgegevens die onder zijn verantwoordelijkheid plaatsvinden. De verwerkingsverantwoordelijke is vaak tevens de rechthebbende, namelijk degene die doel en middelen bepaalt die gebruik worden voor het verwerken van persoonsgegevens. Iedere onderneming of instelling heeft een aantal logische clusters van gegevensverwerkingen (ook wel persoonsregistraties genoemd) die onder de reikwijdte van de AVG vallen.

In het "verwerkingsregister" moeten per persoonsregistratie de volgende gegevens worden opgenomen:

- De verwerkingsdoeleinden (waarom worden persoonsgegevens verzameld);
- een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens die worden verwerkt;
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist en
- indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen

De gegevens in het verwerkingsregister vormen de basis voor reglementen of protocollen die met de ondernemingsraad worden besproken in het kader van het instemmingsrecht voor het verwerken van gegevens van medewerkers van de onderneming. Ook vormt het verwerkingsregister de basis voor het privacystatement dat veel bedrijven en instellingen op hun website plaatsen.
Cameratoezicht valt onder het cluster "beheersvoorzieningen". Bij het woord "beheer" kan gedacht worden aan risicobeheer of kostenbeheer.



Object van bescherming
Het object van bescherming in de AVG is de "verwerking van persoonsgegevens". Dit is het gehele proces dat een persoonsgegeven doormaakt vanaf het moment van verzamelen tot en met het moment van vernietigen. De AVG noemt onder meer het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken en verstrekken van persoonsgegevens.

Materiële normen van de AVG: doelbepaling en doelbinding
Een essentieel beginsel is de doelbepaling. In feite begint het proces van gegevensverwerking daarmee. Persoonsgegevens mogen alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt (art. 5 lid 1 onder a AVG). Dit laatste wordt doelbinding genoemd.
Het woord "doeleinden" is in meervoudsvorm gesteld. Het kan gaan om een hoofddoelstelling en meerdere neven- of subdoelstellingen. Het kunnen ook meerdere naast elkaar staande doelen zijn. De doelen mogen niet te ruim en niet te vaag gesteld zijn. De omschrijving van het doel of de doelen blijkt doorgaans uit de documentatie die de verwerkingsverantwoordelijke moet aanhouden (het verwerkingsregister) en waarvoor vaak de Functionaris voor de gegevensverwerking kan worden benaderd.
De doelbepaling is niet alleen belangrijk voor het verzamelen van persoonsgegevens, maar ook voor het verwerken daarvan (waaronder het opvragen, raadplegen en verstrekken van persoonsgegevens aan anderen wordt verstaan).

Het bepalen van de doeleinden
De doeleinden waarvoor persoonsgegevens verwerkt worden doorgaans te algemeen geformuleerd. Vaak komt men niet verder dan algemene termen als “bewaken van eigendommen”. Met focust zich niet op de vraag waarom persoonsgegevens “verzameld worden” en waarom persoonsgegevens bewaard moeten worden. Daardoor kan op een later moment onduidelijk zijn of persoonsgegevens aan bepaalde personen verstrekt mogen worden.

Die algemene doelen (waarom wil je cameratoezicht?) moeten verder gespecificeerd worden naar doelen waarvoor camerabeelden worden verzameld. In algemene zin zullen de doelen waarvoor camerabeelden binnen bedrijven en instellingen worden verzameld betrekking hebben op:
1. het reconstrueren van voorvallen die een inbreuk hebben gemaakt op rechten en belangen van e organisatie, haar medewerkers (in ruime zin) en derden (waaronder bezoekers en leveranciers.
2. het verlenen van toegang tot gebouwen en terreinen (gecontroleerde toegang);
3. het onderzoeken van vermeende integriteitsschendingen en/of overtreding van gedragsregels en/of wettelijke voorschriften
4. de controle op (verstoringen van) productieprocessen;
5. het beoordelen van alarmsignalen en zo nodig inroepen van de hulp van anderen (alarmverificatie).

Aan wie mogen camerabeelden worden verstrekt?
Op basis van de hiervoor geformuleerde doelen voor het verzamelen van camerabeelden (reproduceerbare beeldopslag) is verenigbaar dat de camerabeelden kunnen worden bekeken en beoordeeld door dan wel verstrekt worden aan:
1. Personen die belast zijn met toegangsverlening en toegangsbeheer (de receptie op basis van verzameldoel 2);
2. Medewerkers van de bedrijfsbeveiligingsdienst dan wel de ingehuurde beveiligingsmedewerkers (op basis van de verzameldoelen 1, 2 en 5).
3. Fraudeonderzoekers en/of integriteitsonderzoekers van het bedrijf of instelling (op basis van verzameldoelen 1 en 3);
4. Leidinggevenden van medewerkers betrokken bij incidenten en/of andere onregelmatigheden, met het oog op de afhandeling van het incident en/of andere onregelmatigheden, alsook degene die bij afhandeling van het voorval noodzakelijkerwijs zijn betrokken. Onder leidinggevende

wordt mede begrepen formele werkgevers van ingeschakelde derden.

5. Videotoezichtcentrales (op basis van verzameldoel 5)

Wat als de doeleinden te algemeen geformuleerd zijn?
Een voorbeeld kan dat verduidelijken. Als in het verwerkingsregister niet expliciet vermeld is, dat persoonsgegevens (tevens) verzameld worden voor "het onderzoeken van vermeende integriteitsschendingen door medewerkers en/of overtreding van wettelijke voorschriften" mogen geen camerabeelden verstrekt worden aan integriteitsonderzoekers van de organisatie of aan de door de organisatie ingeschakelde externe onderzoekers. Die verstrekking is immers onverenigbaar met de doeleinden waarvoor de gegevens verzameld zijn. De verstrekking past niet! In de AVG zijn geen bepalingen opgenomen die een dergelijke verstrekking wel mogelijk maken. Indien dat toch gebeurt kan in een ontslagzaak bepleit worden dat de gegevens onrechtmatig zijn verkregen. Het is dan aan de rechter om te bepalen of het belang van de feitenvaststelling zwaarder weegt dat de schending van de AVG. Organisaties moeten ervoor zorgen dat zij niet afhankelijk zijn van het ongewisse oordeel van de rechter.

Bewaarduur camerabeelden
Met name over de bewaartermijn heerst onduidelijkheid. De bewaartermijn van camerabeelden is gekoppeld aan het doel waarvoor camerabeelden verzameld worden. Als de camerabeelden niet langer nodig zijn voor de verwezenlijking van het doel of de doelen van de verwerking moeten ze vernietigd worden (art. art. 5 lid 1 onder e AVG). Indien het doel van het cameratoezicht beperkt is tot het vastleggen van incidenten gedurende een bepaalde periode en zich in die bepaalde periode geen incidenten hebben voorgedaan is er geen reden om de beelden lang te bewaren. Na de vooraf bepaalde duur moeten de opgenomen beelden vernietigd worden. Per cameratoepassing kan de bewaarduur verschillen. Dit wordt vastgelegd in het verwerkingsregister.
Een wijdverbreid misverstand is dat camerabeelden niet langer dan 4 weken bewaard mogen worden. De ervaring bij overvallen bijvoorbeeld leert bijvoorbeeld dat criminelen vaak meerdere keren een object afleggen voordat zij toeslaan. Een wat langere bewaartermijn verhoogt de kans dat de politie de daders alsnog kan pakken en is vanuit dit doel te rechtvaardigen.
Indien een incident heeft plaatsgevonden kunnen de beelden worden bewaard zolang zij nodig zijn voor een vervolgactie op het incident. Daarbij is te denken aan opsporing en vervolging of een privaatrechtelijke procedure. De camerabeelden worden dan opgenomen in het incidentenregister van de organisatie.

Rechtmatige verwerkingsgrondslag
Indien camerabeelden zijn opgeslagen, betekent dat niet zonder meer dat de camerabeelden verwerkt (lees bekijken, analyseren en verstrekken) mogen worden. Er moet ook een rechtmatige grondslag zijn voor de verwerking. Deze grondslagen zijn limitatief in de AVG opgenomen. Voor cameratoezicht zijn de belangrijkste verwerkingsgrondslagen dat:

a) de gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen waaraan de verwerkingsverantwoordelijke onderworpen is (art. 6 lid 1 onder c AVG)

Daarbij kan gedacht worden aan de plicht om camerabeelden te verstrekken aan handhavingsinstellingen (toezichthouders of opsporingsambtenaren) die deze gegevens nodig hebben voor hun werk (artikel 126nda van het Wetboek van Strafvordering voor opsporingsambtenaren en artikel 5:17 Algemene wet bestuursrecht voor toezichthouders).

b) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen (art. 6 lid 1 onder d AVG);

Toelichting:
Deze verwerkingsgrondslag wordt toegepast indien moet worden vastgesteld of nog personen in een gebouw zijn na een calamiteit (vermiste personen)

c) de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de onderzochte persoon, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert (art. 6 lid 1 onder f AVG).

Toelichting:
Deze verwerkingsgrondslag is doorgaans van toepassing op het verwerken van camerabeelden in relatie tot de hiervoor geformuleerde doeleinden waarvoor reproduceerbaar beeldmateriaal nodig is. Deze verwerkingsgrondslag speelt ook een rol in het bepalen of een deel van de openbare weg in beeld moet worden gebracht omdat dat nodig geacht wordt om de private belangen te behartigen. Een voorbeeld kan dit verduidelijken.

Stel dat een onbevoegde het terrein heeft betreden en eigendommen van de rechthebbende heeft weggenomen. Als alleen het eigen terrein in beeld gebracht wordt, kan bij de analyse van het incident niet vastgesteld worden of die onbevoegde de weggenomen spullen in de kofferbak van diens auto heeft gelegd, als die auto geparkeerd staat op de openbare weg die parallel loopt aan de afscheiding van het terrein. Het is voor het identificeren van de dief verdedigbaar dat een klein deel van de openbare weg in beeld gebracht wordt. Bij die afweging om dat te doen moet rekening worden gehouden met mensen die gebruik maken van die openbare weg omdat zij zich daar in principe onbespied mogen wanen. Tot hoever mag de cameratoepassing pendelen? Is het ook nodig om de woningen aan de overzijde van de straat in beeld te brengen? Dit zijn vragen die in het licht van deze verwerkingsgrondslag beantwoord moeten worden.

Beveiligingsplicht en datalekken
Artikel 32 AVG bepaalt dat de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Hierbij houdt de verantwoordelijke rekening met de beschikbare technologie en de uitvoeringskosten en met de aard, context, omvang en doeleinden van de verwerking. Technische maatregelen zijn de logistieke en fysieke maatregelen in en rondom het camerasysteem (zoals toegangsbeperking, gebruik en back ups). Organisatorische maatregelen zijn maatregelen voor de inrichting van de organisatie en voor het verwerken van persoonsgegevens (zoals de al dan niet toekenning van verantwoordelijkheden en bevoegdheden).
In zijn algemeenheid kan gesteld worden dat, naarmate de aard van de gegevens een gevoeliger karakter heeft of wanneer het lekken een grotere bedreiging van de privacy betekent, zwaardere eisen worden gesteld aan de beveiliging. Leidraad voor de beveiliging van persoonsgegevens zijn de richtsnoeren “Beveiliging van Persoonsgegevens” van de Autoriteit Persoonsgegevens en de best practice ISO 27002.

Artikel 33 en 34 AVG bevatten bepalingen over het melden van datalekken. Artikel 33 AVG ziet op de melding van het datalek aan de toezichthoudende autoriteit. Het eerste lid omschrijft de meldplicht nader. Een inbreuk in verband met persoonsgegevens moet altijd gemeld worden, tenzij het niet waarschijnlijk is dat de inbreuk een risico
inhoudt voor de rechten en vrijheden van natuurlijke personen. De melding dient uiterlijk 72 uur nadat de verwerkingsverantwoordelijke er kennis van heeft genomen plaats te vinden. Het tweede, derde en vierde lid bevatten nadere vereisten aan de melding. Het vijfde lid bevat de verplichting tot documentatie van het datalek door de verwerkingsverantwoordelijke zelf.

Artikel 34 AVG bevat de verplichting om inbreuken te melden aan de betrokkene
zelf. Op grond van het eerste lid dient de melding onverwijld te geschieden. Het tweede lid stelt nadere inhoudelijke eisen aan de mededeling. Het derde lid bevat de uitzonderingen op het eerste lid. Een melding is niet vereist wanneer de gegevens versleuteld zijn of op een andere wijze onbegrijpelijk zijn gemaakt, de verantwoordelijke achteraf maatregelen heeft genomen om het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen, wanneer het groot aantal betrokken gevallen betreft, waardoor de melding onevenredig veel moeite zou kosten en waarbij een openbare mededeling kan volstaan, of wanneer melding afbreuk zou doen aan een zwaarwegend

belang.
De melding stelt betrokkene in staat de nodige voorzorgsmaatregelen te treffen. Een datalek wordt geacht negatieve gevolgen voor betrokkene te hebben wanneer die inbreuk kan leiden tot aantasting van diens reputatie. De kennisgeving dient de aard van het datalek te vermelden alsmede aanbevelingen hoe betrokkene mogelijke negatieve gevolgen kan beperken.

Cameratoezicht moet kenbaar worden gemaakt
Een belangrijk adagium van de AVG is transparantie. Iemand kan zijn rechten (inzage, rectificatie, verwijdering en afscherming) slechts gebruiken maken indien hij op de hoogte is van het feit dat over hem gegevens zijn vastgelegd.
Voor cameratoezicht betekent dit dat de camera's duidelijk moeten zichtbaar zijn of dat een overduidelijke aankondiging gedaan wordt dat camera's geplaatst zijn. Het kenbaar maken van cameratoezicht is ook verplicht op basis van het Wetboek van strafrecht waarover later in dit hoofdstuk meer.
Indien iemand op de hoogte is van de aanwezigheid van camera's heeft hij in beginsel de mogelijkheid zich aan het cameratoezicht te onttrekken. Als iemand dat niet doet kan gesteld worden dat hij zijn persoonsgegevens bewust ter beschikking heeft gesteld (aldus de Memorie van Toelichting bij de eerdere Wet bescherming persoonsgegevens op blz. 156).

Art. 13 AVG schrijft voor dat bepaalde mededelingen moeten worden gedaan aan iemand die zelf gegevens heeft verstrekt die worden vastgelegd. De AVG noemt:

- de identiteit en de contactgegevens van de voor de verwerking verantwoordelijk
- de contactgegevens van de FG (indien aanwezig)
- de doeleinden waarvoor de gegevens worden verzameld
- de ontvangers of categorieën van ontvangers van de gegevens
- de rechtsgrondslag voor de verwerking van de persoonsgegevens en een toelichting daarop, alsmede
- facultatief de bewaartermijn van de gegevens.

Het is het meest efficiënt als deze mededelingen gedaan worden op de website van de organisatie (art. 12 lid 1 AVG). Iemand die op de hoogte wordt gesteld van de verwerking van zijn persoonsgegevens kan daartegen bezwaar maken. Bezwaar aantekenen leidt tot een hernieuwde afweging van de verwerkingsverantwoordelijke of het verwerken van de persoonsgegevens van de betrokkene wel echt noodzakelijk is voor het doel van de verwerking. Voor het maken van bezwaar zijn geen vormvoorschriften gegeven. Dat betekent dat de visueel geobserveerde waarvan beelden zijn vastgelegd zowel mondeling als schriftelijk zijn bezwaren kenbaar kan maken. Het heroverwegingsbesluit moet binnen vier weken genomen worden.

Data Privacy Impact Assessment

Voorafgaand aan de gebruik van cameratoezicht voor private doelen kan het noodzakelijk zijn dat een data privacy impact assessment (DPIA) wordt uitgevoerd. Een DPIA (artikel 35 AVG) is een proces dat bedoeld is om de verwerking van persoonsgegevens te beschrijven die waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, de noodzaak en evenredigheid ervan te beoordelen en de daaraan verbonden risico's voor de rechten en vrijheden van natuurlijke personen in te schatten en maatregelen te nemen om de risico’s te beheersen.

De autoriteit Persoonsgegevens heeft bepaald dat een DPIA moet worden uitgevoerd als een werkgever structureel of gedurende een langere periode cameratoezicht wil inzetten om diefstal en fraude door werknemers te bestrijden. Ook als een werkgever op incidentele basis een verborgen camera (heimelijk cameratoezicht) wil inzetten is een DPIA verplicht.

Handhaving AVG
De Autoriteit Persoonsgegevens is belast met het toezicht op de naleving van de AVG. Zij kan ambtshalve onderzoeken instellen. Zij kan dit ook op verzoek van een belanghebbende doen. Om hun

toezichttaken te kunnen uitoefenen hebben de medewerkers van de Autoriteit Persoonsgegevens toegang tot alle plaatsen en kunnen ze van een ieder medewerking vorderen. De verplichting om mee te werken kan afgedwongen worden met toepassing van een last onder dwangsom. In twijfelgevallen kan de Autoriteit Persoonsgegevens om advies gevraagd worden.
Het adres van de Autoriteit Persoonsgegevens is postbus 93374, 2509 AJ 's-Gravenhage. De Autoriteit Persoonsgegevens is telefonisch te bereiken onder nummer 070-3811300.