Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur

Versie 2.0

Vastgesteld op 29 januari 2020

Translations proofread by EDPB Members. This language version has not yet been proofread.

Versiegeschiedenis

Versie 2.1	26 februari 2020	Correctie van een schrijffout
Versie 2.0	29 januari 2020	Vaststelling van de richtsnoeren na openbare raadpleging
Versie 1.0	10 juli 2019	Vaststelling van de richtsnoeren voor openbare raadpleging

Inhoudsopgave

Het Europees Comité voor gegevensbescherming

Gezien artikel 70, lid 1, onder e), van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (hierna "de AVG"),

Gezien de EER-overeenkomst en met name bijlage XI en Protocol 37 daarvan, zoals gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018[1],

Gezien artikel 12 en artikel 22 van zijn reglement van orde,

HEEFT DE VOLGENDE RICHTSNOEREN VASTGESTELD

1 INLEIDING

1. Het intensieve gebruik van videoapparatuur heeft effect op het gedrag van burgers. Het wijdverbreide gebruik van dergelijke apparaten op allerlei gebieden van het leven zet burgers onder toenemende druk om gedragingen te vermijden die als afwijkend zouden kunnen worden gezien. De facto kunnen deze technologieën de mogelijkheden van anoniem verkeer en het anoniem gebruik van diensten beperken en in het algemeen de mogelijkheid beperken om onopgemerkt te blijven. De gevolgen hiervan voor gegevensbescherming zijn vérstrekkend.

2. Hoewel mensen bijvoorbeeld geen problemen hebben met videobewaking voor bepaalde beveiligingsdoeleinden, moeten er garanties worden geboden dat deze niet wordt misbruikt voor geheel andere en – voor de betrokkene – onverwachte doeleinden (zoals marketingdoeleinden, toezicht op de prestaties van de werknemers enz.). Daarnaast worden er steeds meer toepassingen gebruikt voor een bredere exploitatie van de verzamelde beelden en om van traditionele camera's slimme camera's te maken. De hoeveelheid met video gegenereerde gegevens, gecombineerd met deze toepassingen en technieken, vergroot het risico op secundair gebruik (al dan niet gerelateerd aan het oorspronkelijke doel van het systeem), maar ook het risico op misbruik. De algemene beginselen waarin de AVG (artikel 5) voorziet, moeten bij het gebruik van videobewaking altijd zorgvuldig in acht worden genomen.

3. Videobewakingssystemen veranderen in veel opzichten de manier waarop professionals uit de particuliere en publieke sector in particuliere of openbare ruimten met elkaar omgaan, met het oog op vergroting van de veiligheid, de uitvoering van doelgroepanalysen, het aanbieden van gepersonaliseerde reclame enz. Videobewaking levert steeds betere resultaten op door het toenemende gebruik van intelligente videoanalyse. Deze technieken kunnen ingrijpender (bv. complexe biometrische technologieën) of minder ingrijpend zijn (bv. eenvoudige telalgoritmen). Het wordt in het algemeen steeds moeilijker voor mensen om anoniem te blijven en hun privacy te

[1] Alle verwijzingen in dit advies naar "lidstaten" moeten worden gelezen als verwijzingen naar "EER-lidstaten".

bewaren. De problemen die dit oplevert voor de gegevensbescherming verschillen per geval, evenals de juridische afwegingen, afhankelijk van de verschillende technologieën die worden gebruikt.

4. Naast privacykwesties spelen er ook risico's die verband houden met de mogelijke storingen in deze apparaten en het vertekende beeld dat zij kunnen opleveren. Onderzoekers signaleren dat de software die wordt gebruikt voor gezichtsidentificatie, -herkenning en -analyse beter of slechter presteert afhankelijk van de leeftijd, het geslacht en de etnische kenmerken van de persoon die wordt geïdentificeerd. De algoritmen zouden op verschillende demografische kenmerken gebaseerd zijn, waardoor de vertekening die bij gezichtsherkenning plaatsvindt, de vooroordelen in de samenleving dreigt te versterken. Daarom moeten verwerkingsverantwoordelijken er ook voor zorgen dat regelmatig wordt beoordeeld of de verwerking van biometrische gegevens die afkomstig zijn van videobewaking, relevant is en voldoende waarborgen biedt.

5. Videobewaking is niet per definitie noodzakelijk als er andere middelen zijn om het beoogde doel te bereiken. We lopen anders risico op een cultuuromslag die leidt tot de algemene aanvaarding van een gebrek aan privacy.

6. Deze richtsnoeren zijn bedoeld als leidraad voor de toepassing van de AVG met betrekking tot de verwerking van persoonsgegevens door middel van videoapparatuur. De voorbeelden die hierin worden gegeven, zijn niet uitputtend. De algemene redenering is van toepassing op alle mogelijke gebieden waarop deze apparatuur kan worden gebruikt.

2 TOEPASSINGSGEBIED[2]

2.1 Persoonsgegevens

7. De stelselmatige en geautomatiseerde monitoring van specifieke ruimten met optische of audiovisuele middelen, meestal ter bescherming van gebouwen of het leven en de gezondheid van personen, is tegenwoordig een wijdverbreid verschijnsel. Hiermee worden afbeeldingen of audiovisuele informatie verzameld en opgeslagen over alle personen die de bewaakte ruimte betreden en die identificeerbaar zijn op basis van hun uiterlijk of andere specifieke kenmerken. Aan de hand van deze gegevens kan de identiteit van deze personen worden vastgesteld. Ook maakt het de verdere verwerking van persoonsgegevens mogelijk die betrekking hebben op de aanwezigheid en het gedrag van de personen in de betrokken ruimte. Het potentiële risico van misbruik van deze gegevens neemt toe naarmate de bewaakte ruimte en het aantal personen dat de ruimte bezoekt groter is. Met deze situatie wordt rekening gehouden in de algemene verordening gegevensbescherming, te weten in artikel 35, lid 3, onder c), dat voorschrijft dat er een gegevensbeschermingseffectbeoordeling moet worden uitgevoerd in geval van stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten, alsook in artikel 37, lid 1, onder b), dat voorschrijft dat verwerkers een functionaris voor gegevensbescherming moeten aanwijzen indien de verwerking vanwege de aard daarvan regelmatige en stelselmatige observatie op grote schaal van betrokkenen met zich meebrengt.

8. De verordening is echter niet van toepassing op de verwerking van gegevens die geen betrekking hebben op een persoon, bijvoorbeeld wanneer een persoon hiermee niet direct of indirect kan worden geïdentificeerd.

> Voorbeeld: De AVG is niet van toepassing op nepcamera's (d.w.z. camera's die niet als camera werken en dus geen persoonsgegevens verwerken). *Hiervoor kan in sommige lidstaten echter andere wetgeving gelden.*
>
> Voorbeeld: Opnamen van grote hoogte vallen alleen binnen de werkingssfeer van de AVG indien de verwerkte gegevens onder de gegeven omstandigheden in verband kunnen worden gebracht met een specifiek persoon.
>
> Voorbeeld: In een auto is een videocamera geïnstalleerd om hulp te bieden bij het parkeren. Als de camera zodanig is gebouwd of afgesteld dat hij geen gegevens over natuurlijke personen verzamelt (zoals kentekens of informatie waarmee voorbijgangers kunnen worden geïdentificeerd), is de AVG niet van toepassing.

9.

2.2 Toepassing van Richtlijn (EU) 2016/680 inzake rechtshandhaving

10. Richtlijn (EU) 2016/680 regelt met name de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

[2] Het EDPB wijst erop dat voor zover de AVG dit toelaat, er specifieke nationale voorschriften kunnen gelden.

2.3 Vrijstelling voor huishoudelijke activiteiten

11. Overeenkomstig artikel 2, lid 2, onder c), valt de verwerking van persoonsgegevens door een natuurlijke persoon in het kader van een zuiver persoonlijke of huishoudelijke activiteit, die ook een online-activiteit kan omvatten, buiten de werkingssfeer van de AVG.[3]

12. Deze bepaling – de zogenaamde vrijstelling voor huishoudelijke activiteiten – moet in het geval van videobewaking strikt worden uitgelegd. Volgens het Europees Hof van Justitie moet deze vrijstelling voor huishoudelijk gebruik "*derhalve aldus worden uitgelegd, dat zij uitsluitend betrekking heeft op activiteiten die tot het persoonlijke of gezinsleven van particulieren behoren, hetgeen klaarblijkelijk niet het geval is met de verwerking van persoonsgegevens die bestaat in hun openbaarmaking op internet waardoor die gegevens voor een onbepaald aantal personen toegankelijk worden gemaakt*".[4] Bovendien, voor zover het gebruik van een videobewakingssysteem dat voortdurend persoonsgegevens vastlegt en opslaat "*de openbare ruimte bestrijkt – zelfs gedeeltelijk – en hierdoor buiten de privésfeer geraakt van degene die door middel van dit systeem gegevens verwerkt, kan het niet worden beschouwd als een activiteit die met uitsluitend 'persoonlijke of huishoudelijke doeleinden' wordt verricht in de zin van artikel 3, lid 2, tweede streepje, van richtlijn 95/46*"[5].

13. Ook videoapparatuur die op het terrein van een particulier is geïnstalleerd, kan onder de vrijstelling voor huishoudelijk gebruik vallen. Dat zal afhangen van verschillende factoren, die allemaal in overweging moeten worden genomen om dit te bepalen. Naast de hierboven genoemde elementen die in de uitspraken van het Hof van Justitie zijn vastgesteld, moet de particulier die thuis gebruikmaakt van videobewaking, bekijken of hij een persoonlijke relatie heeft met de betrokkene, of de schaal en de frequentie van het cameratoezicht wijst op een bepaalde beroepsmatige activiteit van zijn kant en of het toezicht mogelijk negatieve gevolgen voor betrokkenen heeft. Als er sprake is van een van de bovengenoemde elementen, betekent dat niet noodzakelijkerwijs dat de verwerking niet onder de vrijstelling voor huishoudelijk gebruik valt. Om dat te bepalen, is een complete beoordeling nodig.

[3] Zie ook overweging 18.

[4] Arrest van het Hof van Justitie van de Europese Unie in zaak C-101/01, *Bodil Lindqvist*, 6 november 2003, punt 47.

[5] Arrest van het Europees Hof van Justitie in zaak C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 11 december 2014, punt 33.

Voorbeeld: Een toerist maakt video-opnamen, zowel met zijn mobiele telefoon als met een videocamera, om een beeldverslag van zijn vakantie te maken. Hij toont de beelden aan vrienden en familie, maar maakt ze niet toegankelijk voor een onbepaald aantal mensen. Dit valt onder de vrijstelling voor huishoudelijk gebruik.

Voorbeeld: Een mountainbiker wil haar afdaling opnemen met een actioncamera. Ze rijdt in een afgelegen gebied en is van plan om de opnamen alleen thuis voor zichzelf te gebruiken. Dit valt onder de vrijstelling voor huishoudelijk gebruik, ook al worden hierbij in beperkte mate persoonsgegevens verwerkt.

Voorbeeld: Iemand houdt met een videocamera toezicht op zijn eigen tuin. Het terrein is omheind en alleen de verwerkingsverantwoordelijke zelf en zijn gezin bevinden zich regelmatig in de tuin. Dit valt in principe onder de vrijstelling voor huishoudelijk gebruik, mits de videobewaking zich niet uitstrekt – zelfs niet gedeeltelijk – tot een openbare ruimte of een belendend privéterrein.

14.

3 RECHTMATIGHEID VAN DE VERWERKING

15. De doeleinden van verwerking moeten van te voren nauwkeurig worden bepaald (artikel 5, lid 1, onder b)). Videobewaking kan voor veel doeleinden dienen, bijvoorbeeld als hulp bij de bescherming van gebouwen en andere eigendommen, de bescherming van het leven en de lichamelijke integriteit van personen of het verzamelen van bewijsmateriaal voor civielrechtelijke vorderingen.[6] De doeleinden van het cameratoezicht moeten schriftelijk worden vastgelegd (artikel 5, lid 2) en afzonderlijk worden gespecificeerd voor elke gebruikte bewakingscamera. In het geval van meerdere camera's die door één verwerkingsverantwoordelijke voor hetzelfde doeleinde worden gebruikt, hoeft dit maar één keer te worden gedocumenteerd. Bovendien moeten de betrokkenen overeenkomstig artikel 13 worden geïnformeerd over de doeleinden van de verwerking (zie deel 7, "Transparantie en informatieverplichtingen"). De enkele vermelding dat de videobewaking dient voor "de veiligheid" of "uw veiligheid" is niet specifiek genoeg (artikel 5, lid 1, onder b)). Dat is bovendien in strijd met het beginsel dat persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is (zie artikel 5, lid 1, onder a)).

16. In beginsel kan elke rechtsgrond voorzien in artikel 6, lid 1, een rechtsgrondslag vormen voor de verwerking van gegevens die met videobewaking zijn verkregen. Artikel 6, lid 1, onder c), is bijvoorbeeld van toepassing wanneer het nationale recht voorziet in een verplichting om gebruik te maken van videobewaking.[7] In de praktijk zullen de volgende bepalingen echter waarschijnlijk het meest worden gebruikt:

- artikel 6, lid 1, onder f) (gerechtvaardigd belang);
- artikel 6, lid 1, onder e) (noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag).

In veeleer uitzonderlijke gevallen kan artikel 6, lid 1, onder a) (toestemming) door de verwerkingsverantwoordelijke als rechtsgrondslag worden gebruikt.

3.1 Gerechtvaardigd belang (artikel 6, lid 1, onder f))

17. De juridische beoordeling van artikel 6, lid 1, onder f), moet gebaseerd zijn op de volgende criteria, in overeenstemming met overweging 47.

3.1.1 Bestaan van gerechtvaardigde belangen

18. Videobewaking is rechtmatig indien deze noodzakelijk is voor de behartiging van een gerechtvaardigd belang van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene zwaarder wegen dan dat belang (artikel 6, lid 1, onder f)). De door een verwerkingsverantwoordelijke of een derde nagestreefde gerechtvaardigde belangen kunnen van juridische[8], economische of immateriële aard zijn.[9] De verwerkingsverantwoordelijke moet er echter rekening mee houden dat indien de betrokkene bezwaar maakt tegen de bewaking overeenkomstig artikel 21, de verwerkingsverantwoordelijke de

[6] De regels voor het verzamelen van bewijsmateriaal voor civielrechtelijke vorderingen verschillen per lidstaat.

[7] In deze richtsnoeren worden de aspecten van het nationale recht die per lidstaat kunnen verschillen niet geanalyseerd, noch uitgebreid besproken.

[8] Arrest van het Hof van Justitie van de Europese Unie in zaak C-13/16, *Rīgas satiksme*, 4 mei 2017.

[9] Zie WP217, Groep artikel 29.

videobewaking van die betrokkene alleen kan voortzetten als hij een *dwingend* gerechtvaardigd belang heeft dat zwaarder weegt dan de belangen, rechten en vrijheden van de betrokkene of dat verband houdt met de instelling, uitoefening of onderbouwing van een rechtsvordering.

19. In aantoonbaar gevaarlijke situaties kan de bescherming van eigendommen tegen inbraak, diefstal of vandalisme een belang zijn dat videobewaking rechtvaardigt.

20. Het gerechtvaardigde belang moet reëel zijn en betrekking hebben op een actueel probleem (d.w.z. het mag niet fictief of speculatief zijn)[10]. Alvorens over te gaan tot bewaking moet er sprake zijn van een daadwerkelijke noodsituatie, die bijvoorbeeld blijkt uit eerder gevallen van schade of ernstige incidenten. Gezien het verantwoordingsbeginsel doen verwerkingsverantwoordelijken er goed aan om alle relevante incidenten (inclusief datum, verloop, financiële schade) en de daarmee samenhangende strafrechtelijke procedures te documenteren. Deze gedocumenteerde incidenten kunnen sterke aanwijzingen voor het bestaan van een gerechtvaardigd belang vormen. Het bestaan van een gerechtvaardigd belang en de noodzaak van het toezicht moeten regelmatig opnieuw worden beoordeeld (bv. eenmaal per jaar, afhankelijk van de omstandigheden).

> Voorbeeld: Een winkelier wil een nieuwe winkel openen en wil een videobewakingssysteem installeren om vandalisme te voorkomen. Aan de hand van statistieken kan hij aantonen dat er in de nabije omgeving sprake is van een grote kans op vandalisme. Ook de ervaringen van andere winkels in de buurt zijn relevant. Het is niet nodig dat de betrokken verwerkingsverantwoordelijke zelf schade heeft geleden. Zolang schadegevallen in de buurt duiden op het gevaar van soortgelijke schade, kunnen zij een indicatie zijn van een gerechtvaardigd belang. Het volstaat echter niet om de nationale of algemene misdaadstatistieken te in te brengen zonder het betrokken gebied of de gevaren voor deze specifieke winkel te analyseren.

21.

22. Ook dreigend gevaar kan een gerechtvaardigd belang opleveren, bijvoorbeeld in het geval van banken of winkels die waardevolle artikelen verkopen (zoals juweliers), of in gebieden waarvan bekend is dat daar regelmatig vermogensdelicten plaatsvinden (bijvoorbeeld benzinestations).

23. In de AVG is ook duidelijk bepaald dat overheidsinstanties hun verwerking niet kunnen baseren op gerechtvaardigde belangen, wanneer deze plaatsvindt in het kader van de uitoefening van hun taken (artikel 6, lid 1, tweede zin).

3.1.2 Noodzaak van de verwerking

24. Persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (“minimale gegevensverwerking”), zie artikel 5, lid 1, onder c). Alvorens een systeem voor cameratoezicht te installeren, moet de verwerkingsverantwoordelijke altijd kritisch onderzoeken of deze maatregel ten eerste geschikt is om het gewenste doel te bereiken, en ten tweede of deze toereikend en noodzakelijk voor de beoogde doeleinden is. Maatregelen voor videobewaking moeten alleen worden gekozen indien het doel van de verwerking niet redelijkerwijs kan worden bereikt met andere middelen die minder ingrijpend zijn voor de fundamentele rechten en vrijheden van de betrokkene.

25. Als een verwerkingsverantwoordelijke beoogt om vermogensdelicten te voorkomen, zou hij in plaats van een videobewakingssysteem te installeren ook alternatieve veiligheidsmaatregelen kunnen

[10] Zie WP217, Groep artikel 29, blz. 24 e.v. Zie ook zaak C-708/18 van het HvJ, blz. 44.

nemen, zoals het plaatsen van een hekwerk, het organiseren van regelmatige patrouilles door beveiligingspersoneel, het installeren van een betere verlichting, het installeren van veiligheidssloten, inbraakbestendige ramen en deuren of het aanbrengen van anti-graffiticoating of -folies op muren. Deze maatregelen kunnen even doeltreffend tegen inbraak, diefstal en vandalisme zijn als videobewaking. De verwerkingsverantwoordelijke moet per geval beoordelen of dergelijke maatregelen een redelijke oplossing kunnen zijn.

26. Alvorens een camerasysteem te gebruiken, moet de verwerkingsverantwoordelijke beoordelen waar en wanneer de videobewaking strikt noodzakelijk is. Gewoonlijk is een bewakingssysteem dat zowel 's nachts als buiten de normale kantooruren wordt ingeschakeld voldoende om te voorzien in de behoefte van verwerkingsverantwoordelijken om eventuele gevaren voor hun eigendommen te voorkomen.

27. In het algemeen beperkt de noodzaak van videobewaking voor de bescherming van de bedrijfsgebouwen van verwerkingsverantwoordelijken zich tot de buitengrenzen van het betreffende terrein.[11] In bepaalde gevallen is de bewaking van het terrein zelf echter niet voldoende voor een doeltreffende bescherming. In specifieke gevallen kan het noodzakelijk zijn de videobewaking uit te breiden naar de directe omgeving van het terrein. In dit geval moet de verwerkingsverantwoordelijke fysieke en technische maatregelen overwegen, bijvoorbeeld het afschermen of pixeleren van niet-relevante gebieden.

> Voorbeeld: Een boekwinkel wil zijn pand tegen vandalisme beschermen. Doorgaans hoeven de camera's alleen het pand zelf te filmen, omdat het voor dat doel niet nodig is om de gebouwen of openbare ruimten in de omgeving van de boekwinkel in beeld te brengen.

28.

29. Ook de wijze waarop de opnamen worden bewaard, kan vragen oproepen over de noodzaak van verwerking. In sommige gevallen kan het noodzakelijk zijn "zwarte doos"-oplossingen te gebruiken, waarbij de beelden na een bepaalde bewaartermijn automatisch worden gewist en alleen in geval van incidenten toegankelijk zijn. In andere situaties is het wellicht helemaal niet nodig om het videomateriaal vast te leggen, maar kan in plaats daarvan beter gebruik worden gemaakt van realtime toezicht. De keuze tussen "zwarte doos"-oplossingen en realtime toezicht moet ook gebaseerd zijn op het beoogde doel. Als het doel van videobewaking bijvoorbeeld is om bewijsmateriaal te vergaren, zijn realtime methoden meestal niet geschikt. Soms kan realtime toezicht ook ingrijpender zijn dan het opslaan en automatisch verwijderen van materiaal na een beperkte periode (als iemand bijvoorbeeld voortdurend een monitor bekijkt, kan dit ingrijpender zijn dan wanneer er helemaal geen monitor is en al het materiaal rechtstreeks in een zwarte doos wordt opgeslagen). In dit verband moet rekening worden gehouden met het beginsel van minimale gegevensverwerking (artikel 5, lid 1, onder c)). Ook moet worden overwogen dat de verwerkingsverantwoordelijke in plaats van videobewaking beveiligingspersoneel zou kunnen inzetten, dat in staat is om onmiddellijk te reageren en in te grijpen.

3.1.3 Belangenafweging

30. Ervan uitgaande dat videobewaking noodzakelijk is om de gerechtvaardigde belangen van een verwerkingsverantwoordelijke te beschermen, mag een videobewakingssysteem alleen in gebruik worden genomen indien de belangen of de grondrechten en fundamentele vrijheden van de betrokkene niet zwaarder wegen dan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of die van een derde (bijvoorbeeld de bescherming van diens

[11] In sommige lidstaten kan dit ook gereguleerd zijn door nationale wetgeving.

eigendommen of fysieke integriteit). De verwerkingsverantwoordelijke moet beoordelen 1) in hoeverre het toezicht gevolgen heeft voor de belangen, grondrechten en vrijheden van personen en 2) of dit leidt tot schending van of negatieve gevolgen voor de rechten van betrokkenen. Het is immers verplicht om de belangen tegen elkaar af te wegen. De grondrechten en fundamentele vrijheden enerzijds en de gerechtvaardigde belangen van de verwerkingsverantwoordelijke anderzijds moeten zorgvuldig worden beoordeeld en tegen elkaar afgewogen.

Voorbeeld: Een particulier parkeerbedrijf beschikt over bewijzen dat er regelmatig diefstallen plaatsvinden in de op hun terrein geparkeerde auto's. Het parkeerterrein is een open ruimte en is gemakkelijk toegankelijk voor iedereen, maar is aan de buitenrand duidelijk afgebakend met borden en barrières. Het parkeerbedrijf heeft een gerechtvaardigd belang (het voorkomen van diefstal in de auto's van klanten) om het gebied te bewaken op de tijdstippen waarop zij problemen ondervinden. De betrokkenen worden gedurende beperkte tijd gemonitord, bevinden zich niet op het terrein voor recreatiedoeleinden en het is ook in hun eigen belang dat diefstal wordt voorkomen. Het gerechtvaardigde belang van de verwerkingsverantwoordelijke weegt in dit geval zwaarder dan het belang van de betrokkenen om niet te worden gemonitord.

Voorbeeld: Een restaurant besluit videocamera's in de toiletten te installeren om de hygiëne van de sanitaire voorzieningen te controleren. In dit geval wegen de rechten van de betrokkenen duidelijk zwaarder dan de belangen van de verwerkingsverantwoordelijke, zodat er geen camera's kunnen worden geïnstalleerd.

31.

3.1.3.1 Besluitneming per geval

32. Aangezien de afweging van belangen volgens de verordening verplicht is, moeten besluiten per geval worden genomen (zie artikel 6, lid 1, onder f)). De verwijzing naar abstracte situaties of het vergelijken van soortgelijke gevallen is niet voldoende. De verwerkingsverantwoordelijke moet de risico's van inbreuk op de rechten van de betrokkenen beoordelen; bepalend hierbij is de vraag hoe ingrijpend de inbreuk op de rechten en vrijheden van personen is.

33. De ingrijpendheid kan onder meer worden bepaald aan de hand van het soort informatie dat wordt verzameld (inhoud van de informatie), de reikwijdte ervan (informatiedichtheid, ruimtelijk en geografisch bereik), het aantal betrokkenen, hetzij in absolute aantallen, hetzij als percentage van de betrokken populatie, de concrete situatie, de feitelijke belangen van de groep betrokkenen en de beschikbare alternatieve middelen, alsook op basis van de aard en de reikwijdte van de gegevensbeoordeling.

34. Belangrijke afwegingsfactoren zijn de omvang van het bewaakte gebied en het aantal betrokkenen dat onder toezicht staat. Het gebruik van videobewaking in een afgelegen gebied (bijvoorbeeld om toezicht te houden op wilde flora en fauna of om kritieke infrastructuur te beschermen, zoals een particuliere radioantenne) moet anders worden beoordeeld dan videobewaking in een voetgangersgebied of een winkelcentrum.

Voorbeeld: Als er een dashcam wordt geïnstalleerd (bv. voor het verzamelen van bewijs in het geval van een ongeluk), is het belangrijk ervoor te zorgen dat de camera niet voortdurend het verkeer of de personen in de buurt van de weg filmt. Het belang bij video-opnamen als bewijs in het meer theoretische geval van een verkeersongeval kan anders geen rechtvaardiging vormen voor deze ernstige aantasting van de rechten van de betrokkenen.[11]

35.

3.1.3.2 Redelijke verwachtingen van betrokkenen

36. Volgens overweging 47 moet het bestaan van een gerechtvaardigd belang zorgvuldig worden beoordeeld. Hierbij moet rekening worden gehouden met de redelijke verwachtingen van de betrokkene op het moment en in het kader van de verwerking van zijn persoonsgegevens. In het geval van stelselmatige observatie kan de relatie tussen de betrokkene en de verwerkingsverantwoordelijke aanzienlijk variëren, wat de redelijke verwachtingen van de betrokkene kan beïnvloeden. De uitleg van het begrip "redelijke verwachtingen" mag niet alleen gebaseerd zijn op de subjectieve verwachtingen van de betrokkene. Het beslissende criterium moet veeleer zijn of een objectieve derde redelijkerwijs mocht verwachten dat hij in die specifieke situatie zou worden gemonitord.

37. Zo zal een werknemer op zijn of haar werkplek in de meeste gevallen niet door zijn of haar werkgever worden gecontroleerd.[12] Ook verwachten mensen niet dat zij worden geobserveerd in hun eigen tuin, in woonruimten of in onderzoeks- en behandelruimten. Vanuit diezelfde gedachte is het ook redelijk om te verwachten dat er geen cameratoezicht wordt gehouden in sanitaire voorzieningen of sauna's, aangezien de monitoring van deze ruimten een grove aantasting van de rechten van betrokkenen zou betekenen. De redelijke verwachting van betrokkenen is dat er in dat soort ruimten geen videobewaking plaatsvindt. De klant van een bank mag daarentegen wel verwachten dat hij/zij binnen de bank of bij de geldautomaat wordt geobserveerd.

38. Betrokkenen mogen ook verwachten dat zij niet worden gemonitord in openbaar toegankelijke gebieden, met name wanneer die gebieden doorgaans worden gebruikt voor ontspanning en recreatie, of waar mensen gaan zitten en/of elkaar treffen, zoals bankjes, tafels in restaurants, parken, bioscopen en fitnessvoorzieningen. Hier zullen de belangen of de rechten en vrijheden van de betrokkenen vaak zwaarder wegen dan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke.

> Voorbeeld: In toiletten verwachten betrokkenen dat zij niet worden geobserveerd. Videobewaking om ongevallen te voorkomen, is bijvoorbeeld niet evenredig.

39.

40. Borden die betrokkenen wijzen op de videobewaking zijn niet relevant bij de beoordeling van wat een betrokkene objectief kan verwachten. Dit betekent dat de winkelier er bijvoorbeeld niet van uit mag gaan dat klanten *objectief gezien* de redelijke verwachting hebben dat zij worden gecontroleerd, enkel omdat een bord bij de ingang klanten hierop wijst.

3.2 Verwerking die noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen (artikel 6, lid 1, onder e))

41. Op grond van artikel 6, lid 1, onder e) kunnen persoonsgegevens door middel van videobewaking worden verwerkt, indien dat nodig is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag.[13] Het kan zijn dat de uitoefening van het openbaar gezag een dergelijke verwerking niet toestaat, maar dat andere rechtsgrondslagen, zoals "gezondheid en veiligheid" voor de bescherming van bezoekers en werknemers beperkte

[12] Zie ook: Groep artikel 29, Advies 2/2017 over gegevensverwerking op het werk, WP 249, Brussel, 8 juni 2017.

[13] De rechtsgrond voor de bedoelde verwerking moet worden vastgesteld "bij Unierecht of lidstatelijk recht" en "is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend" (artikel 6, lid 3).

mogelijkheden voor verwerking kunnen bieden, rekening houdend met de verplichtingen van de AVG en de rechten van betrokkenen.

42. De lidstaten kunnen specifieke nationale wetgeving voor videobewaking handhaven of invoeren om de toepassing van de regels van de AVG aan te passen door specifiekere vereisten voor verwerking vast te stellen, zo lang dit in overeenstemming is met de beginselen die zijn vastgelegd in de AVG (bv. opslagbeperking, evenredigheid).

3.3 Toestemming (artikel 6, lid 1, onder a))

43. De toestemming moet worden gegeven door middel van een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting, zoals beschreven in de richtsnoeren inzake toestemming.[14]

44. Wat stelselmatige monitoring betreft, kan de toestemming van de betrokkene volgens artikel 7 (zie overweging 43) alleen in uitzonderlijke gevallen als rechtsgrondslag dienen. Het ligt in de aard van de technologie dat bij camerabewaking een onbekend aantal mensen tegelijk wordt gemonitord. De verwerkingsverantwoordelijke zal dus moeilijk kunnen aantonen dat de betrokkene van tevoren toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens (artikel 7, lid 1). Ook in het geval dat de betrokkene zijn toestemming intrekt, zal het voor de verwerkingsverantwoordelijke moeilijk zijn te bewijzen dat de persoonsgegevens niet langer worden verwerkt (artikel 7, lid 3).

> Voorbeeld: Atleten kunnen tijdens individuele oefeningen om monitoring verzoeken om hun techniek en prestaties te kunnen analyseren. Wanneer een sportclub daarentegen het initiatief neemt om een volledig team voor hetzelfde doel te monitoren, is de toestemming vaak niet geldig, aangezien de individuele sporters zich onder druk gezet kunnen voelen om toestemming te geven, doordat hun weigering een negatief effect op teamgenoten zou kunnen hebben.

45.

46. Als de verwerkingsverantwoordelijke toestemming als grondslag wil gebruiken, moet hij ervoor zorgen dat iedere betrokkene die het gebied betreedt dat onder videobewaking staat, hiervoor toestemming heeft gegeven. Deze toestemming moet voldoen aan de voorwaarden van artikel 7. Het betreden van een gemarkeerde bewaakte zone (mensen worden bijvoorbeeld verzocht om via een specifieke gang of een specifieke toegangspoort naar een bewaakte zone te gaan) vormt geen verklaring of ondubbelzinnige actieve handeling zoals vereist is voor toestemming, tenzij het voldoet aan de criteria van artikel 4 en 7 zoals beschreven in de richtsnoeren inzake toestemming.[15]

47. Gezien de onevenwichtige machtsverhouding tussen werkgevers en werknemers kunnen werkgevers zich in de meeste gevallen beter niet baseren op toestemming voor de verwerking van persoonsgegevens, aangezien deze waarschijnlijk niet vrijelijk gegeven is. In dit verband moet rekening worden gehouden met de richtsnoeren inzake toestemming.

48. In de wetgeving van lidstaten of in collectieve arbeidsovereenkomsten, waaronder “bedrijfsakkoorden”, kunnen nadere regels worden gesteld voor de verwerking van persoonsgegevens van werknemers in het kader van de arbeidsverhouding (zie artikel 88).

---

[14] Groep artikel 29 (artikel 29 WP) „Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679” (WP 259 rev. 01). – goedgekeurd door het Europees Comité voor gegevensbescherming (EDPB)

[15] Groep artikel 29 (WP 29), „Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679” (WP 259) – goedgekeurd door het Europees Comité voor gegevensbescherming (EDPB) – waarmee hierbij rekening moet worden gehouden.

4 VERSTREKKING VAN VIDEOBEELDEN AAN DERDEN

49. In beginsel zijn de algemene voorschriften van de AVG van toepassing op de verstrekking van video-opnamen aan derden.

4.1 Verstrekking van videobeelden aan derden in het algemeen

50. Verstrekking wordt in artikel 4, onder 2, gedefinieerd als doorzending (bv. individuele communicatie), verspreiden (bv. online publiceren) of het op andere wijze ter beschikking stellen. Het begrip "derde" wordt gedefinieerd in artikel 4, onder 10. Wanneer de verstrekking wordt gedaan aan derde landen of internationale organisaties, zijn de bijzondere bepalingen van artikel 44 e.v. eveneens van toepassing.

51. De openbaarmaking van persoonsgegevens is een afzonderlijke vorm van verwerking van persoonsgegevens, die de verwerkingsverantwoordelijke moet baseren op een van de rechtsgronden voorzien in artikel 6.

> Voorbeeld: Een verwerkingsverantwoordelijke die een opname in het internet wenst te uploaden, moet een beroep doen op een rechtsgrondslag voor die verwerking, bijvoorbeeld door het verkrijgen van toestemming van de betrokkene overeenkomstig artikel 6, lid 1, onder a).

52.

53. De doorgifte van videobeelden aan derden voor een ander doel dan waarvoor de gegevens zijn verzameld, is volgens de regels van artikel 6, lid 4, mogelijk.

> Voorbeeld: Bij een hefboom (op een parkeerterrein) wordt een camera geïnstalleerd voor het oplossen van schadegevallen. Er ontstaat schade en de opnamen worden aan een advocaat gegeven om de zaak af te handelen. In dit geval is het doel van de opname hetzelfde als dat voor de doorgifte.
>
> Voorbeeld: Bij een hefboom (op een parkeerterrein) wordt een camera geïnstalleerd voor het oplossen van schadegevallen. De opname wordt puur voor vermaak online gezet. In dit geval is er sprake van een ander doel dat niet verenigbaar is met het oorspronkelijke doel. Het is bovendien lastig om voor deze verwerking (publicatie) een rechtsgrondslag te vinden.

54.

55. Een ontvangende derde partij moet deze situatie zelf juridisch beoordelen, met name de rechtsgrondslag voor verwerking op grond van artikel 6 (zoals de ontvangst van het materiaal).

4.2 Verstrekking van videobeelden aan rechtshandhavingsinstanties

56. De verstrekking van video-opnamen aan rechtshandhavingsinstanties is ook een onafhankelijk proces, dat een afzonderlijke verantwoording door de verwerkingsverantwoordelijke vereist.

57. Volgens artikel 6, lid 1, onder c), is de verwerking rechtmatig wanneer de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust. Hoewel de toepasselijke politiewetgeving een zaak is die tot de exclusieve bevoegdheid van de lidstaten behoort, bestaan er doorgaans in elke lidstaat ook algemene regels die de overdracht van bewijsmateriaal aan rechtshandhavingsinstanties regelen. De verwerking door de verwerkingsverantwoordelijke die de gegevens overdraagt, wordt geregeld door de AVG. Als de verwerkingsverantwoordelijke overeenkomstig de nationale wetgeving verplicht is aan de rechtshandhaving (bv. onderzoek) mee te werken, is de rechtsgrondslag voor de overdracht van de gegevens de wettelijke verplichting voorzien in artikel 6, lid 1, onder c).

58. De doelbinding volgens artikel 6, lid 4, vormt dan vaak geen probleem, aangezien de verstrekking uitdrukkelijk is gebaseerd op het recht van de lidstaat. In dat geval is niet nodig de bijzondere overwegingen in acht te nemen die gepaard gaan met een verandering van het doel van de verwerking in de zin van de letters a) tot en met e).

Voorbeeld: De winkelier maakt video-opnamen bij de ingang van de winkel. Daarop is te zien hoe iemand de portefeuille van iemand anders steelt. De politie verzoekt de verwerkingsverantwoordelijke om hun het beeldmateriaal ter beschikking te stellen voor het onderzoek. In dat geval kan de winkelier zich voor de verwerking van de overgedragen gegevens baseren op de rechtsgrondslag van artikel 6, lid 1, onder c) (wettelijke verplichting), in combinatie met de toepasselijke nationale wetgeving.

59.

Voorbeeld: Om veiligheidsredenen wordt er in een winkel een camera geïnstalleerd. De winkelier vermoedt dat hij iets verdachts heeft opgenomen en besluit het materiaal naar de politie te sturen (zonder enige aanwijzing dat er een onderzoek loopt). In dit geval moet de winkelier beoordelen of aan de voorwaarden van artikel 6, lid 1, onder f), is voldaan, dat in dit soort gevallen veelal van toepassing is. Dit is doorgaans het geval wanneer de winkelier een redelijk vermoeden heeft dat er een misdrijf is gepleegd.

60.

61. De verwerking van persoonsgegevens door rechtshandhavingsinstanties valt niet onder de AVG (zie artikel 2, lid 2, onder d)), maar onder Richtlijn (EU) 2016/680 inzake rechtshandhaving.

5 VERWERKING VAN BIJZONDERE CATEGORIEËN PERSOONSGEGEVENS

62. Videobewakingssystemen verzamelen meestal enorme hoeveelheden persoonsgegevens die informatie van zeer persoonlijke aard aan het licht kunnen brengen, inclusief bijzondere categorieën van persoonsgegevens. Daarbij kan uit schijnbaar insignificante gegevens die oorspronkelijk met videocamera's werden verzameld, informatie worden afgeleid waarmee een ander doel wordt nagestreefd (bv. om een beeld te krijgen van iemands gewoonten). Videobewaking wordt echter niet altijd als verwerking van bijzondere categorieën persoonsgegevens aangemerkt.

> Voorbeeld: Videobeelden waarop iemand te zien is die een bril draagt of in een rolstoel zit, worden niet per se als bijzondere categorieën persoonsgegevens beschouwd.

63.

64. Als de videobeelden echter worden verwerkt om daaruit bijzondere categorieën gegevens af te leiden, is artikel 9 van toepassing.

> Voorbeeld: Politieke opvattingen kunnen bijvoorbeeld worden afgeleid uit beelden van identificeerbare betrokkenen die deelnemen aan een evenement, een staking enz. Dit valt onder artikel 9.
>
> Voorbeeld: Wanneer een ziekenhuis een videocamera installeert om de gezondheidstoestand van een patiënt te bewaken, wordt dit beschouwd als verwerking van bijzondere categorieën persoonsgegevens (artikel 9).

65.

66. Als algemene regel moet bij de installatie van een videobewakingssysteem het beginsel van minimale gegevensverwerking zorgvuldig in acht worden genomen. Daarom moet de verwerkingsverantwoordelijke zelfs in gevallen waarin artikel 9, lid 1, niet van toepassing is, proberen zoveel mogelijk te voorkomen dat er gevoelige (niet onder artikel 9 vallende) gegevens worden verzameld, ongeacht het doel daarvan.

> Voorbeeld: De videobewaking van een kerk valt niet per se onder artikel 9. De verwerkingsverantwoordelijke moet echter bij de beoordeling van de belangen van de betrokkene een bijzonder zorgvuldige afweging maken op grond van artikel 6, lid 1, onder f), waarbij hij rekening moet houden met de aard van de gegevens en het risico dat er andere (niet onder artikel 9 vallende) gevoelige gegevens worden verzameld.

67.

68. Indien een videobewakingssysteem wordt gebruikt om bijzondere categorieën gegevens te verwerken, moet de verwerkingsverantwoordelijke zowel aantonen dat er sprake is van een uitzondering voor de verwerking van bijzondere categorieën gegevens als bedoeld in artikel 9 (d.w.z. een uitzondering op de algemene regel dat bijzondere categorieën van gegevens niet mogen worden verwerkt) alsook van een van de rechtsgronden voorzien in artikel 6.

69. Zo zou bijvoorbeeld – in theorie en bij wijze van uitzondering – artikel 9, lid 2, onder c) kunnen worden toegepast ("*de verwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon*"), maar in dat geval zou de verwerkingsverantwoordelijke moeten aantonen dat de bewaking absoluut noodzakelijk is om iemands vitale belangen te

beschermen, alsook dat de "*betrokkene fysiek of juridisch niet in staat is zijn toestemming te verlenen*". Bovendien mag de verwerkingsverantwoordelijke het systeem niet om andere redenen gebruiken.

70. Het is belangrijk om hier op te merken dat waarschijnlijk geen van de in artikel 9 genoemde uitzonderingen kan worden gebruikt om de verwerking van bijzondere categorieën gegevens door middel van videobewaking te rechtvaardigen. Meer specifiek kunnen verwerkingsverantwoordelijken die deze gegevens verwerken in het kader van videobewaking zich niet beroepen op artikel 9, lid 2, onder e), dat de verwerking toestaat van persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt. Het enkele feit dat de betrokkene het gezichtsveld van de camera betreedt, betekent niet dat de betrokkene bijzondere categorieën van gegevens die op hem of haar betrekking hebben openbaar wil maken.

71. Voorts vereist de verwerking van bijzondere categorieën gegevens een verhoogde en voortdurende waakzaamheid ten aanzien van bepaalde verplichtingen; bijvoorbeeld een hoog beveiligingsniveau en de uitvoering van een gegevensbeschermingseffectbeoordeling, indien nodig.

> Voorbeeld: Een werkgever mag niet gebruikmaken van de video-opnamen van een demonstratie om de stakers te identificeren.

72.

5.1 Algemene overwegingen bij de verwerking van biometrische gegevens

73. Het gebruik van biometrische gegevens en met name gezichtsherkenning brengt verhoogde risico's met zich mee voor de rechten van betrokkenen. Het is essentieel dat het gebruik van dergelijke technologieën plaatsvindt met inachtneming van de beginselen van rechtmatigheid, noodzakelijkheid, evenredigheid en minimale gegevensverwerking, zoals uiteengezet in de AVG. Hoewel deze technologieën als bijzonder doeltreffend kunnen worden beschouwd, moeten verwerkingsverantwoordelijken eerst de gevolgen voor de grondrechten en fundamentele vrijheden beoordelen en bezien of er minder ingrijpende middelen voorhanden zijn om het gerechtvaardigde doel van de verwerking te bereiken.

74. Om als biometrische gegevens te worden aangemerkt zoals gedefinieerd in de AVG, moet de verwerking van ruwe gegevens, zoals de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon, gepaard gaan met een meting van deze kenmerken. Aangezien biometrische gegevens het resultaat zijn van dergelijke metingen, wordt in artikel 4, onder 14, van de AVG bepaald dat het hier gaat om persoonsgegevens *„[…] die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd […]*". De video-opnamen van een persoon kunnen echter op zichzelf niet als biometrische gegevens in de zin van artikel 9 worden beschouwd als deze niet met bepaalde technische middelen zijn verwerkt met het oog op diens identificatie. [16]

[16] Dit wordt bevestigd door overweging 51 van de AVG, waarin wordt gesteld: "*[…] De verwerking van foto's mag niet systematisch worden beschouwd als verwerking van bijzondere categorieën van persoonsgegevens, aangezien foto's alleen onder de definitie van biometrische gegevens vallen wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maken. […]*".

75. Om als verwerking van bijzondere categorieën persoonsgegevens (artikel 9) te kunnen worden beschouwd, is vereist dat biometrische gegevens worden verwerkt "met het oog op de unieke identificatie van een persoon".

76. Samenvattend moeten er gezien artikel 4, onder 14 en artikel 9 drie criteria in aanmerking worden genomen:

- **de aard van de gegevens:** gegevens betreffende de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon;
- **de middelen en wijze van verwerking:** gegevens "die het resultaat zijn van een specifieke technische verwerking";
- **het doel van de verwerking:** de gegevens moeten worden gebruikt voor de unieke identificatie van een natuurlijke persoon.

77. Het gebruik van videocamera's met functionaliteiten voor biometrische herkenning die door particuliere entiteiten voor eigen doeleinden (bv. marketing, statistieken, maar ook beveiliging) worden geïnstalleerd, zal in de meeste gevallen de uitdrukkelijke toestemming van alle betrokkenen vereisen (artikel 9, lid 2, onder a). Een andere passende uitzondering voorzien in artikel 9 zou echter ook van toepassing kunnen zijn.

Voorbeeld: Om haar dienstverlening te verbeteren, vervangt een particuliere onderneming de controlepunten voor de identificatie van passagiers op een luchthaven (bagage drop-off, boarden) door videosystemen, waarbij gebruik wordt gemaakt van gezichtsherkenning om de identiteit te verifiëren van passagiers die toestemming hebben verleend voor deze procedure. Aangezien deze verwerking onder artikel 9 valt, moeten de passagiers, die hiervoor van tevoren hun uitdrukkelijke en geïnformeerde toestemming hebben gegeven, bijvoorbeeld gebruikmaken van een automatische terminal om een gezichtstemplate te creëren en te registreren dat wordt gekoppeld aan hun instapkaart en hun identiteit. De controlepunten met gezichtsherkenning moeten duidelijk gescheiden zijn, bijvoorbeeld door het systeem in poortjes te installeren, zodat de biometrische templates van personen die hiervoor geen toestemming hebben gegeven niet worden vastgelegd. Alleen passagiers die hiervoor vooraf toestemming hebben gegeven en zich hebben laten registreren, kunnen gebruikmaken van het poortje met het biometrische systeem.

Voorbeeld: Een verwerkingsverantwoordelijke beheert de toegang tot zijn gebouw met behulp van gezichtsherkenningstechnologie. Mensen kunnen van deze manier van toegang alleen gebruikmaken als zij daarvoor van tevoren uitdrukkelijk geïnformeerde toestemming hebben gegeven (overeenkomstig artikel 9, lid 2, onder a)). Om te voorkomen dat opnamen worden gemaakt van iemand die hiervoor geen toestemming heeft gegeven, mag de gezichtsherkenning pas worden toegepast wanneer de betrokkene deze zelf activeert, bijvoorbeeld door op een knop te drukken. Om de rechtmatigheid van de verwerking te waarborgen, moet de verwerkingsverantwoordelijke altijd een alternatieve toegangswijze bieden om in het gebouw te komen waarbij geen biometrische gegevens worden verwerkt, bijvoorbeeld met badges of sleutels.

78.

79. In dit soort gevallen, waarbij biometrische templates worden aangemaakt, moeten de verwerkingsverantwoordelijken ervoor zorgen dat, zodra de betrokkene al of niet is herkend, alle templates die ter plaatse zijn gecreëerd (met de uitdrukkelijke en geïnformeerde toestemming van de

betrokkene) om te worden vergeleken met de templates die de betrokkene tijdens het registratieproces heeft laten aanmaken, onmiddellijk en veilig worden gewist. De bij registratie gecreëerde templates mogen alleen worden bewaard om het doel van de verwerking te kunnen verwezenlijken en mogen niet worden opgeslagen of gearchiveerd.

80. Wanneer het doel van de verwerking bijvoorbeeld echter is om een categorie personen te onderscheiden van een andere categorie, maar niet om iemand op unieke wijze te identificeren, valt de verwerking niet onder artikel 9.

> Voorbeeld: Een winkelier wil graag zijn reclame personaliseren op basis van de gender- en leeftijdskenmerken van de klanten die met een videobewakingssysteem worden vastgesteld. Indien dat systeem geen biometrische templates genereert om personen op unieke wijze te identificeren, maar die fysieke kenmerken alleen detecteert om iemand in een categorie in te delen, valt de verwerking niet onder artikel 9 (mits er geen andere soorten bijzondere categorieën gegevens worden verwerkt).

81.

82. Artikel 9 is echter wel van toepassing als de verwerkingsverantwoordelijke biometrische gegevens opslaat (meestal in de vorm van templates die worden gecreëerd door de essentiële gelaatstrekken te bepalen op basis van ruwe biometrische gegevens (bv. gezichtsmetingen aan de hand van een beeld)) om iemand op unieke wijze te identificeren. Indien een verwerkingsverantwoordelijke een betrokkene wil detecteren als hij of zij een ruimte opnieuw betreedt of een andere ruimte betreedt (bijvoorbeeld om gepersonaliseerde reclame te kunnen blijven projecteren), is het doel om een natuurlijke persoon op unieke wijze te identificeren, wat betekent dat de verwerking van meet af aan onder artikel 9 valt. Dit is onder meer het geval als een verwerkingsverantwoordelijke de gegenereerde templates opslaat om op informatieborden op verschillende plaatsen in de winkel meer gepersonaliseerde reclame aan te bieden. Aangezien het systeem gebruikmaakt van fysieke kenmerken om specifieke personen te detecteren die weer in het gezichtsveld van de camera komen (zoals de bezoekers van een winkel) en hen te volgen, vormt dit een biometrische identificatiemethode omdat deze gericht is op herkenning door het gebruik van specifieke technische verwerking.

> Voorbeeld: Een winkelier heeft in zijn winkel een systeem voor gezichtsherkenning geïnstalleerd om zijn reclame voor klanten te personaliseren. De verwerkingsverantwoordelijke moet de uitdrukkelijke en geïnformeerde toestemming van alle betrokkenen verkrijgen voordat hij dit biometrische systeem mag gebruiken en reclame op maat kan bieden. Het systeem zou onrechtmatig zijn als het bezoekers of voorbijgangers filmt die niet hebben ingestemd met het aanmaken van hun biometrische template, ook al wordt die template zo snel mogelijk weer verwijderd. Deze tijdelijke templates zijn namelijk biometrische gegevens die worden verwerkt om iemand eenduidig te identificeren die mogelijk geen gerichte reclame wenst te ontvangen.

83.

84. Het Europees Comité voor gegevensbescherming merkt op dat sommige biometrische systemen in een ongecontroleerde omgeving worden geïnstalleerd[17], wat betekent dat het systeem automatisch de gezichten vastlegt van iedereen die door het gezichtsveld van de camera loopt, met inbegrip van mensen die niet hebben toegestemd in deze toepassingen waarmee biometrische templates worden

[17] Dit betekent dat het biometrische apparaat is geïnstalleerd in een openbaar toegankelijke ruimte en kan worden gebruikt voor iedereen die langsloopt, in tegenstelling tot biometrische systemen in gecontroleerde omgevingen die alleen kunnen worden gebruikt met toestemming van de betrokkene.

gecreëerd. Deze templates worden vergeleken met de templates van betrokkenen die vooraf, tijdens een registratieproces, toestemming hebben gegeven voor het aanmaken daarvan (d.w.z. gebruikers van een biometrisch apparaat), zodat de verwerkingsverantwoordelijke kan vaststellen of de betreffende persoon al dan niet een gebruiker van een biometrisch apparaat is. In deze gevallen is het systeem vaak zodanig ontworpen dat het de in een databank opgenomen personen die moeten worden herkend, kan onderscheiden van personen die zich niet hebben geregistreerd. Aangezien het doel is om natuurlijke personen op een unieke manier te identificeren, moet voor iedereen die door de camera wordt gefilmd nog steeds een van de uitzonderingen van artikel 9, lid 2, AVG gelden.

Voorbeeld: Een hotel maakt gebruik van videobewaking, zodat de hotelmanager automatisch wordt gewaarschuwd dat er een VIP is gearriveerd wanneer het gezicht van de gast wordt herkend. Deze VIP's hebben voordat zij werden opgenomen in een daartoe gecreëerde databank uitdrukkelijke toestemming voor het gebruik van gezichtsherkenning gegeven. Deze systemen voor de verwerking voor biometrische gegevens zijn onrechtmatig, tenzij alle andere gasten die worden gemonitord (met het oog op de identificatie van VIP's) toestemming hebben gegeven voor de verwerking overeenkomstig artikel 9, lid 2, onder a), AVG.

Voorbeeld: Een verwerkingsverantwoordelijke installeert een videobewakingssysteem met gezichtsherkenning bij de ingang van de door hem beheerde concertzaal. De verwerkingsverantwoordelijke moet hiervoor duidelijk gescheiden ingangen creëren: één met het biometrisch systeem en één zonder (waar bijvoorbeeld alleen het toegangskaartje wordt gescand). De ingang die is uitgerust met biometrische apparatuur moet dusdanig ingericht en toegankelijk zijn dat het systeem geen biometrische templates kan verzamelen van toeschouwers die hiervoor geen toestemming hebben gegeven.

85.

86. Wanneer er toestemming vereist is volgens artikel 9 AVG, mag de verwerkingsverantwoordelijke bovendien de toegang tot zijn diensten niet afhankelijk stellen van de instemming met de biometrische verwerking. Met andere woorden, de verwerkingsverantwoordelijke moet een alternatieve oplossing zonder biometrische verwerking bieden die geen beperkingen of extra kosten voor de betrokkene met zich meebrengt, met name wanneer de biometrische verwerking voor authenticatiedoeleinden wordt gebruikt. Deze alternatieve oplossing is ook nodig voor personen die niet voldoen aan de minimumvereisten van het biometrische systeem (registratie of lezen van de biometrische gegevens niet mogelijk, handicap waardoor het systeem moeilijk te gebruiken is, enz.); ook moet er, rekening houdend met de mogelijke niet-beschikbaarheid van het biometrische apparaat (bijvoorbeeld door een storing) een "back-up-oplossing" worden geboden om de continuïteit van de aangeboden dienst te waarborgen, die evenwel alleen bij wijze van uitzondering mag worden gebruikt. In uitzonderlijke gevallen kan er sprake zijn van een situatie waarin de verwerking van biometrische gegevens de kernactiviteit is van een dienst die wordt aangeboden op basis van een contract, bijvoorbeeld een museum dat een tentoonstelling organiseert over het gebruik van een apparaat voor gezichtsherkenning. In dat geval kunnen betrokkenen de verwerking van hun biometrische gegevens niet weigeren indien zij aan de tentoonstelling willen deelnemen. In dat geval is de krachtens artikel 9 vereiste toestemming nog steeds geldig indien aan de vereisten van artikel 7 is voldaan.

5.2 Voorgestelde maatregelen om de risico's bij de verwerking van biometrische gegevens tot een minimum te beperken

87. In overeenstemming met het beginsel van minimale gegevensverwerking moeten verwerkingsverantwoordelijken ervoor zorgen dat gegevens die uit een digitaal beeld worden afgeleid om een template te creëren, evenredig zijn en alleen de informatie bevatten die voor het

gespecificeerde doel vereist is, zodat eventuele verdere verwerking wordt voorkomen. Er moeten maatregelen worden genomen om te waarborgen dat templates niet naar andere biometrische systemen kunnen worden overgedragen.

88. Voor identificatie en authenticatie/verificatie moet het template waarschijnlijk worden opgeslagen met het oog op vergelijking in een later stadium. De verwerkingsverantwoordelijke moet beoordelen wat de meest geschikte locatie voor de opslag van de gegevens is. In een gecontroleerde omgeving (gescheiden gangen of controlepunten) moeten de templates worden opgeslagen op een afzonderlijk apparaat van de gebruiker dat onder zijn of haar exclusieve controle staat (een smartphone of identiteitskaart) of – indien vereist voor specifieke doeleinden en gezien objectieve behoeften – in versleutelde vorm opgeslagen in een gecentraliseerde databank waarbij de geheime sleutel uitsluitend in handen is van de gebruiker om ongeoorloofde toegang tot de template of de opslaglocatie te voorkomen. Indien de verwerkingsverantwoordelijke de toegang tot de templates niet kan vermijden, moet hij passende maatregelen nemen om de beveiliging van de opgeslagen gegevens te waarborgen. Dit kan onder meer door versleuteling van de template met behulp van een cryptografisch algoritme.

89. De verwerkingsverantwoordelijke moet in elk geval alle nodige voorzorgsmaatregelen nemen om de beschikbaarheid, integriteit en vertrouwelijkheid van de verwerkte gegevens te waarborgen. Hiertoe moet de verwerkingsverantwoordelijke met name de volgende maatregelen nemen: compartimentering van de gegevens tijdens verzending en opslag, opslag van biometrische templates en ruwe gegevens of identiteitsgegevens in afzonderlijke databanken, versleuteling van biometrische gegevens, en met name biometrische templates, en vaststelling van een beleid voor versleuteling en sleutelbeheer, geïntegreerde organisatorische en technische maatregelen voor de opsporing van fraude, koppeling van de gegevens aan een integriteitscode (bijvoorbeeld handtekening of hash) en het verbieden van externe toegang tot de biometrische gegevens. Deze maatregelen zullen gelijke tred moeten houden met de technologische ontwikkelingen.

90. Verwerkingsverantwoordelijken moeten bovendien overgaan tot verwijdering van de ruwe gegevens (gezichtsopnamen, spraaksignalen, bewegingspatronen enz.), waarbij zij de effectiviteit van de verwijdering moeten waarborgen. Als er niet langer een rechtmatige grondslag voor de verwerking bestaat, moeten de ruwe gegevens worden gewist. Voor zover biometrische templates het resultaat zijn van dergelijke gegevens kan de creatie van databanken namelijk als een even grote, zo niet grotere bedreiging worden beschouwd (het is immers niet altijd gemakkelijk om een biometrische template te lezen zonder kennis van de wijze van programmering, terwijl ruwe gegevens de bouwstenen van de template vormen). In het geval dat de verwerkingsverantwoordelijke dergelijke gegevens moet bewaren, moet hij de mogelijkheden onderzoeken van ruistoevoeging (bv. met watermerken), waardoor het aanmaken van templates onmogelijk wordt gemaakt. De verwerkingsverantwoordelijke moet de biometrische gegevens en de templates ook wissen in geval van ongeoorloofde toegang tot de terminal die de gegevens leest en vergelijkt of tot de opslagserver. Ook moeten gegevens worden gewist die aan het einde van de levensduur van het biometrische apparaat niet langer bruikbaar zijn voor verdere verwerking.

6 RECHTEN VAN DE BETROKKENE

91. Vanwege de aard van de gegevensverwerking bij gebruik van videobewaking moeten sommige van de rechten van betrokkenen uit hoofde van de AVG verder worden verduidelijkt. Hoewel dit hoofdstuk niet uitputtend is, zijn alle rechten uit hoofde van de AVG van toepassing op de verwerking van persoonsgegevens door middel van videobewaking.

6.1 Recht op inzage

92. Betrokkenen hebben het recht om door de verwerkingsverantwoordelijke bevestiging te krijgen of hun persoonsgegevens al of niet worden verwerkt. In het geval van videobewaking betekent dit dat als er op geen enkele wijze gegevens zijn opgeslagen of overgedragen, de verwerkingsverantwoordelijke na het moment van realtime toezicht alleen kan meedelen dat er geen persoonsgegevens meer worden verwerkt (afgezien van de algemene informatieverplichtingen op grond van artikel 13; zie deel 7 ,*Transparantie en informatieverplichtingen*). Als er op het moment van het verzoek echter nog steeds gegevens worden verwerkt (d.w.z. als de gegevens op een andere manier worden opgeslagen of continu worden verwerkt), moet de betrokkene hiertoe inzage krijgen en moet hem/haar de informatie voorzien in artikel 15 worden verstrekt.

93. In bepaalde gevallen geldt echter een aantal beperkingen met betrekking tot het recht van inzage.

- Artikel 15, lid 4, AVG: de inzage mag geen afbreuk doen aan de rechten van anderen

94. Aangezien op een video-opname een onbepaald aantal betrokkenen kan zijn vastgelegd, kan het bekijken van de opname leiden tot een verdere verwerking van de persoonsgegevens van andere betrokkenen. Als de betrokkene een kopie van het materiaal wenst te ontvangen (artikel 15, lid 3), kan dit afbreuk doen aan de rechten en vrijheden van andere betrokkenen die in het materiaal zijn opgenomen. Om dat te voorkomen, moet de verwerkingsverantwoordelijke rekening houden met het feit dat hij in sommige gevallen video-opnamen waarop ook andere betrokkenen kunnen worden geïdentificeerd, vanwege hun ingrijpende aard niet ter beschikking kan stellen. De bescherming van de rechten van derden mag echter niet worden gebruikt als een excuus om legitieme verzoeken om inzage van betrokkenen te weigeren. De verwerkingsverantwoordelijke moet in die gevallen technische maatregelen treffen om aan het verzoek om inzage te voldoen (bijvoorbeeld door de beelden deels af te schermen of vager te maken). Verwerkingsverantwoordelijken zijn echter niet verplicht dat soort technische maatregelen toe te passen indien zij binnen de in artikel 12, lid 3, gestelde termijn op andere wijze aan een verzoek uit hoofde van artikel 15 kunnen voldoen.

- Artikel 11, lid 2, AVG: de verwerkingsverantwoordelijke is niet in staat de betrokkene te identificeren

95. Als in de videobeelden niet op persoonsgegevens kan worden gezocht (zodat de verwerkingsverantwoordelijke waarschijnlijk een grote hoeveelheid beeldmateriaal moet gaan bekijken om de betrokkene in kwestie te vinden), is de verwerkingsverantwoordelijke mogelijk niet in staat de betrokkene te identificeren.

96. Om die redenen moet de betrokkene zich niet alleen persoonlijk of met een identiteitsdocument identificeren, maar in zijn verzoek aan de verwerkingsverantwoordelijke ook specificeren wanneer — binnen een redelijk tijdvak gezien de hoeveelheid gefilmde betrokkenen — hij of zij zich in het door de camera bestreken gebied bevond. De verwerkingsverantwoordelijke moet de betrokkene van tevoren laten weten welke informatie hij nodig heeft om aan het verzoek te

kunnen voldoen. Indien de verwerkingsverantwoordelijke kan aantonen dat hij niet in staat is om de betrokkene te identificeren, moet hij de betrokkene daarvan zo mogelijk in kennis stellen. In een dergelijke situatie moet de verwerkingsverantwoordelijke de betrokkene in zijn antwoord informatie verstrekken over het exacte door de camera's bestreken gebied, welke camera's op dat moment in gebruik waren enz., zodat de betrokkene volledig inzicht krijgt in welke persoonsgegevens van hem/haar zijn verwerkt.

Voorbeeld: Als een betrokkene een kopie opvraagt van zijn of haar persoonsgegevens die zijn verwerkt door middel van videobewaking bij de ingang van een winkelcentrum met 30 000 bezoekers per dag, moet de betrokkene aangeven binnen welk tijdvak van ongeveer een uur hij of zij zich in het bewaakte gebied bevond. Indien de verwerkingsverantwoordelijke het betreffende materiaal nog steeds verwerkt, moet hij een kopie van de videobeelden verstrekken. Als andere betrokkenen in hetzelfde materiaal kunnen worden geïdentificeerd, moet dat deel van het materiaal worden geanonimiseerd (bijvoorbeeld door de kopie of delen daarvan vaag weer te geven) voordat de kopie wordt verstrekt aan de betrokkene die het verzoek heeft ingediend.

Voorbeeld: Als de verwerkingsverantwoordelijke automatisch alle beelden uiterlijk na bijvoorbeeld twee dagen wist, kan de hij de informatie na die twee dagen niet aan de betrokkene verstrekken. Indien de verwerkingsverantwoordelijke na die twee dagen een verzoek om inzage ontvangt, moet de betrokkene daarvan in kennis worden gesteld.

97.

- Artikel 12 AVG: buitensporige verzoeken

98. In geval van buitensporige of kennelijk ongegronde verzoeken van een betrokkene kan de verwerkingsverantwoordelijke een redelijke vergoeding in rekening brengen overeenkomstig artikel 12, lid 5, onder a), AVG, of weigeren aan het verzoek gevolg te geven (artikel 12, lid 5, onder b), AVG). De verwerkingsverantwoordelijke moet kunnen aantonen dat het verzoek kennelijk ongegrond of buitensporig is.

6.2 Recht op gegevenswissing en recht van bezwaar

6.2.1 Recht op gegevenswissing (recht op vergetelheid)

99. Indien de verwerkingsverantwoordelijke doorgaat met persoonsgegevensverwerking die verder gaat dan realtime toezicht (bv. opslag), kan de betrokkene uit hoofde van artikel 17 AVG verzoeken om de persoonsgegevens te wissen.

100. Desgevraagd is de verwerkingsverantwoordelijke verplicht om persoonsgegevens onverwijld te wissen indien een van de in artikel 17, lid 1, AVG vermelde omstandigheden (en geen van de in artikel 17, lid 3, AVG genoemde uitzonderingen) van toepassing is. De verplichting om persoonsgegevens te wissen is onder meer van toepassing wanneer deze niet langer nodig zijn voor het doel waarvoor zij oorspronkelijk waren opgeslagen of wanneer de verwerking onrechtmatig is (zie ook deel 8, "Opslagtermijnen en verplichting tot het wissen van gegevens"). Persoonsgegevens moeten verder, afhankelijk van de rechtsgrond voor de verwerking, worden gewist:

- *bij verwerking op basis van toestemming* wanneer de toestemming wordt ingetrokken (en er geen andere rechtsgrond voor de verwerking bestaat);
- *bij verwerking op basis van gerechtvaardigde belangen:*

- wanneer de betrokkene het recht van bezwaar uitoefent (zie punt 6.2.2) en er geen dwingende gerechtvaardigde gronden voor de verwerking bestaan; of
- in het geval van direct marketing (inclusief profilering), wanneer de betrokkene bezwaar maakt tegen de verwerking.

101. Indien de verwerkingsverantwoordelijke de videobeelden openbaar heeft gemaakt (bv. door uitzending of streaming ervan op internet), moeten er redelijke maatregelen worden genomen om de andere verwerkingsverantwoordelijken (die nu de betrokken persoonsgegevens verwerken) in kennis te stellen van het verzoek van de betrokkene overeenkomstig artikel 17, lid 2, AVG. De redelijke maatregelen moeten technische maatregelen omvatten, waarbij rekening wordt gehouden met de beschikbare technologie en de uitvoeringskosten. Voor zover mogelijk moet de verwerkingsverantwoordelijke overeenkomstig artikel 19 AVG na het wissen van persoonsgegevens iedereen aan wie de persoonsgegevens eerder werden verstrekt daarvan in kennis stellen.

102. Naast de verplichting van de verwerkingsverantwoordelijke om persoonsgegevens op verzoek van de betrokkene te wissen, is de verwerkingsverantwoordelijke krachtens de algemene beginselen van de AVG verplicht om de hoeveelheid opgeslagen persoonsgegevens te beperken (zie deel 8).

103. In het geval van videobewaking is het nuttig erop te wijzen dat wanneer beelden bijvoorbeeld worden vervaagd waardoor het niet meer mogelijk is om de persoonsgegevens terug te halen, deze als gewist worden beschouwd volgens de AVG.

> Voorbeeld: Een avondwinkel heeft problemen met vandalisme, met name aan de buitenkant, en maakt daarom gebruik van videocamera's bij de ingang, die direct aan de muur zijn bevestigd. Een voorbijganger verzoekt onmiddellijk om zijn persoonsgegevens te laten wissen. De verwerkingsverantwoordelijke is verplicht om onverwijld en uiterlijk binnen een maand op het verzoek te reageren. Aangezien de beelden in kwestie niet langer beantwoorden aan het doel waarvoor zij aanvankelijk waren opgeslagen (er was in de periode waarin de betrokkene langsliep geen sprake meer van vandalisme), bestond er ten tijde van het verzoek geen gerechtvaardigd belang voor het opslaan van de gegevens dat zwaarder woog dan de belangen van de betrokkene. De verwerkingsverantwoordelijke moet de persoonsgegevens derhalve wissen.

104.

6.2.2 Recht van bezwaar

105. In het geval van videobewaking die wordt uitgevoerd op basis van gerechtvaardigde belangen (artikel 6, lid 1, onder f), AVG) of die noodzakelijk is voor de vervulling van een taak van algemeen belang (artikel 6, lid 1, onder e), AVG) heeft de betrokkene overeenkomstig artikel 21 AVG te allen tijde het recht om vanwege met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van zijn persoonsgegevens. Tenzij de verwerkingsverantwoordelijke dwingende gerechtvaardigde gronden aanvoert die zwaarder wegen dan de rechten en belangen van de betrokkene, moet de verwerking van de gegevens van degene die bezwaar maakt vervolgens worden gestaakt. De verwerkingsverantwoordelijke is verplicht om onverwijld en uiterlijk binnen een maand op de verzoeken van de betrokkene te reageren.

106. In het geval van videobewaking kan dit bezwaar worden gemaakt bij het betreden, tijdens de aanwezigheid in of na het verlaten van het bewaakte gebied. In de praktijk betekent dit dat, tenzij de verwerkingsverantwoordelijke dwingende gerechtvaardigde gronden kan aanvoeren, het cameratoezicht op een gebied waarin natuurlijke personen kunnen worden geïdentificeerd, alleen rechtmatig is indien:

(1) de verwerkingsverantwoordelijke op verzoek in staat is om de camera onmiddellijk de verwerking van persoonsgegevens te laten staken; of

(2) de toegang tot het bewaakte gebied zodanig beperkt is dat de verwerkingsverantwoordelijke kan waarborgen dat de betrokkene voordat hij de ruimte betreedt goedkeuring voor verwerking geeft; daarnaast betreft het een ruimte die de betrokkene als burger niet mag betreden.

107. Deze richtsnoeren beogen niet vast te stellen wat als een *dwingend* gerechtvaardigd belang wordt beschouwd (artikel 21 AVG).

108. Wanneer wordt gebruikgemaakt van videobewaking voor direct marketing, heeft de betrokkene het recht om op discretionaire basis bezwaar te maken tegen de verwerking, aangezien het recht van bezwaar in dit geval absoluut is (artikel 21, lid 2 en 3, AVG).

> Voorbeeld: Een bedrijf ondervindt veiligheidsproblemen bij de openbaar toegankelijke ingang en maakt gebruik van videobewaking op grond van gerechtvaardigde belangen, met als doel de personen die zich onrechtmatig toegang verschaffen te onderscheppen. Een bezoeker maakt bezwaar tegen de verwerking van zijn of haar gegevens met het videobewakingssysteem om redenen die verband houden met zijn of haar specifieke situatie. De onderneming wijst het verzoek echter af met het argument dat het opgeslagen materiaal nodig is voor een lopend intern onderzoek, zodat er zwaarwegende gerechtvaardigde gronden bestaan om door te gaan met de verwerking van de persoonsgegevens.

109.

7 TRANSPARANTIE EN INFORMATIEVERPLICHTINGEN[18]

110. In de Europese wetgeving inzake gegevensbescherming ligt al geruime tijd besloten dat betrokkenen moeten weten dat er wordt gebruikgemaakt van videobewaking. Zij moeten nauwkeurig worden geïnformeerd over de plaatsen die onder bewaking staan.[19] In de AVG staan de algemene transparantie- en informatieverplichtingen beschreven in artikel 12 en volgende. De "richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679" (WP 260) van de Groep artikel 29, die op 25 mei 2018 door het EDPB werden goedgekeurd, verschaffen hierover nadere details. Volgens WP 260, punt 26, is artikel 13 AVG van toepassing wanneer persoonsgegevens worden verzameld "[…] bij een betrokkene door middel van waarneming (bv. met behulp van geautomatiseerde gegevensverzamelingsapparaten of gegevens verzamelende software zoals camera's […].".

111. Gezien de hoeveelheid informatie die aan de betrokkene moet worden verstrekt, kunnen verwerkingsverantwoordelijken een gelaagde aanpak volgen wanneer zij ervoor kiezen om een combinatie van methoden te gebruiken om transparantie te waarborgen (WP 260, punt 35; WP 89, blz. 22). Wat videobewaking betreft, moet de belangrijkste informatie op het waarschuwingsbord zelf (eerste laag) worden weergegeven, terwijl de andere verplichte gegevens met andere middelen (tweede laag) kunnen worden verstrekt.

7.1 Eerste laag met informatie (waarschuwingsbord)

112. De eerste laag heeft betrekking op de primaire wijze waarop de verwerkingsverantwoordelijke voor het eerst contact legt met een betrokkene. In dit stadium kunnen verwerkingsverantwoordelijken een waarschuwingsbord gebruiken waarop de relevante informatie vermeld staat. Die informatie kan in combinatie met een icoon worden verstrekt, teneinde op goed zichtbare, begrijpelijke en duidelijk leesbare vorm een nuttig overzicht van de voorgenomen verwerking te bieden (artikel 12, lid 7, AVG). Het formaat van de informatie moet aan elke locatie worden aangepast (WP 89, blz. 22).

7.1.1 Plaatsing van het waarschuwingsbord

113. De informatie moet zo zijn aangebracht dat de betrokkene gemakkelijk inzicht krijgt in de omstandigheden van het toezicht voordat hij het bewaakte gebied betreedt (ongeveer op ooghoogte). Het is niet nodig de plaats van de camera aan te geven zolang er geen twijfel bestaat over welke zones worden bewaakt en de omstandigheden waarin de bewaking plaatsvindt voor iedereen duidelijk zijn (WP 89, blz. 22). De betrokkene moet kunnen inschatten welk gebied door de camera wordt bestreken, zodat hij of zij de bewaking kan vermijden of zijn of haar gedrag waar nodig kan aanpassen.

7.1.2 Inhoud van de eerste laag

114. De eerste laag met informatie (waarschuwingsbord) moet over het algemeen de belangrijkste informatie bevatten, bv. details over het doel van de verwerking, de identiteit van de verwerkingsverantwoordelijke en het bestaan van de rechten van de betrokkene, samen met informatie over de belangrijkste gevolgen van de verwerking.[20] Hierop kunnen bijvoorbeeld de gerechtvaardigde belangen worden vermeld die door de verwerkingsverantwoordelijke (of een derde) worden nagestreefd, of de contactgegevens van de functionaris voor gegevensbescherming (indien

[18] Hiervoor kunnen in de nationale wetgeving specifieke voorschriften gelden.

[19] Zie WP 89, Advies 4/2004 van de Groep artikel 29 over de verwerking van persoonsgegevens met videobewaking.

[20] Zie WP 260, punt 38.

van toepassing). Het bord moet ook verwijzen naar de meer gedetailleerde tweede laag met informatie en waar en hoe deze te vinden is.

115. Daarnaast moet het bord ook alle informatie bevatten die voor de betrokkene onverwacht zou kunnen zijn (WP 260, punt 38). Een voorbeeld hiervan is de doorgifte aan derden, met name wanneer deze zich buiten de EU bevinden, of de opslagperiode. Als deze informatie niet wordt vermeld, moet de betrokkene erop kunnen vertrouwen dat er uitsluitend sprake is van realtime toezicht (zonder dat er gegevens worden opgenomen of doorgegeven aan derden).

116.

7.2 Tweede laag met informatie

117. De tweede laag met informatie moet ook beschikbaar worden gesteld op een plaats die gemakkelijk toegankelijk is voor de betrokkene, bijvoorbeeld in de vorm van een complete brochure die op een centrale locatie verkrijgbaar is (bv. informatiebalie, receptie of kassa) of worden weergegeven op een gemakkelijk leesbare poster. Zoals eerder aangegeven, moet het eerste waarschuwingsbord met de eerste informatielaag duidelijk naar de tweede laag verwijzen. Bovendien is het het beste als de eerste informatielaag een verwijzing bevat naar een digitale bron met een tweede laag met informatie (bv. QR-code of een internetadres). De informatie moet echter ook in niet-digitale vorm gemakkelijk toegankelijk zijn. Het moet mogelijk zijn om toegang te krijgen tot de informatie van de tweede laag zonder het bewaakte gebied te betreden, met name als de informatie digitaal wordt verstrekt (bijvoorbeeld door middel van een link). Een andere geschikte manier zou een telefoonnummer kunnen zijn dat de betrokkene kan bellen. Ongeacht de manier waarop deze wordt verstrekt, moet de informatie alle gegevens bevatten die verplicht zijn op grond van artikel 13 AVG.

118. Ter aanvulling en ondersteuning van deze mogelijkheden bevordert het EDPB het gebruik van technologische middelen bij de verstrekking van informatie aan betrokkenen. Hiervoor kan worden gebruikgemaakt van camera's met geolokalisering of informatie worden opgenomen in apps of websites met kaarten, zodat betrokkenen enerzijds gemakkelijk de videobronnen kunnen identificeren

en specificeren met het oog op de uitoefening van hun rechten, en anderzijds meer gedetailleerde informatie over de verwerking kunnen verkrijgen.

Voorbeeld: Een winkelier houdt cameratoezicht op zijn winkel. Om aan artikel 13 te voldoen, is het voldoende om een waarschuwingsbord op een goed zichtbare plaats bij de ingang van de winkel aan te brengen, die de eerste laag met informatie bevat. Daarnaast moet hij in de winkel aanvullende schriftelijke informatie beschikbaar stellen bij de kassa of een andere centraal gelegen, gemakkelijk toegankelijke plaats in de winkel.

119.

8 OPSLAGTERMIJNEN EN DE VERPLICHTING TOT WISSEN

120. Persoonsgegevens mogen niet langer worden opgeslagen dan nodig is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt (artikel 5, lid 1, onder c) en e), AVG). In sommige lidstaten kunnen er specifieke bepalingen gelden voor de opslagtermijnen met betrekking tot videobewaking overeenkomstig artikel 6, lid 2, AVG.

121. De periode waarbinnen persoonsgegevens worden opgeslagen, moet beperkt worden gehouden. In het algemeen bestaan de gerechtvaardigde doeleinden bij videobewaking uit de bescherming van gebouwen of het verzamelen van bewijsmateriaal. Gewoonlijk kan schade die optreedt, binnen een of twee dagen worden vastgesteld. Om gemakkelijker te kunnen aantonen dat de regels voor gegevensbescherming worden nageleefd, is het in het belang van de verwerkingsverantwoordelijke om van tevoren organisatorische maatregelen te treffen (bv. door waar nodig iemand aan te stellen die verantwoordelijk is voor het screenen en het veiligstellen van videomateriaal). Gelet op de beginselen van artikel 5, lid 1, onder c) en e), AVG, te weten minimale gegevensverwerking en opslagbeperking, moeten persoonsgegevens in de meeste gevallen (bv. wanneer zij dienen voor het opsporen van vandalisme) na enkele dagen worden gewist, idealiter automatisch. Hoe langer de opslagtermijn (met name wanneer deze langer is dan 72 uur), des te beter moeten de legitimiteit van het doel en de noodzaak van opslag worden onderbouwd. Als de verwerkingsverantwoordelijke de videobewaking niet alleen gebruikt voor het toezicht op zijn gebouwen, maar ook van plan is de gegevens op te slaan, moet hij/zij garanderen dat de opslag daadwerkelijk noodzakelijk is voor het beoogde doel. Is dit het geval, dan moet de opslagtermijn duidelijk en afzonderlijk voor elk specifiek doeleinde worden vastgesteld. Het is de verantwoordelijkheid van de verwerkingsverantwoordelijke om de opslagtermijn vast te stellen in overeenstemming met de beginselen van noodzakelijkheid en evenredigheid en om de naleving van de bepalingen van AVG aan te tonen.

> Voorbeeld: De eigenaar van een kleine winkel weet gewoonlijk nog dezelfde dag of er vandalisme heeft plaatsgevonden. Bijgevolg is een standaard opslagtermijn van 24 uur voldoende. Als de winkel in het weekend gesloten is of langer dicht is wegens vakantie kan dit echter reden zijn voor een langere opslagperiode. Als er schade wordt geconstateerd, zal hij de gegevens mogelijk voor een langere periode moeten opslaan om gerechtelijke stappen tegen de dader te kunnen ondernemen.

122.

9 TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

123. Zoals bepaald in artikel 32, lid 1, AVG moet de verwerking van persoonsgegevens bij videobewaking niet alleen wettelijk toegestaan zijn, maar moeten de verwerkingsverantwoordelijken en verwerkers ook de beveiliging daarvan afdoende waarborgen. De getroffen **organisatorische en technische maatregelen moeten in verhouding staan tot de risico's voor de rechten en vrijheden van natuurlijke personen** als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot videobewakingsgegevens, hetzij per ongeluk, hetzij onrechtmatig. Overeenkomst artikel 24 en 25 AVG moeten verwerkingsverantwoordelijken ook technische en organisatorische maatregelen nemen om te waarborgen dat alle beginselen van gegevensbescherming tijdens de verwerking in acht worden genomen, en dat betrokkenen over de middelen beschikken om hun rechten voorzien in de artikelen 15 tot en met 22 van de AVG te kunnen uitoefenen. Verwerkingsverantwoordelijken moeten een intern kader en beleid vaststellen om deze uitvoering te

waarborgen, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, inclusief, waar nodig, de uitvoering van gegevensbeschermingseffectbeoordelingen.

9.1 Overzicht van een videobewakingssysteem

124. Een systeem voor videobewaking (video surveillance system, VSS)[21] bestaat uit analoge en digitale apparatuur en software voor het opnemen van beelden van een plaats, het verwerken van deze beelden en het weergeven ervan aan de gebruiker. De componenten ervan zijn te verdelen in de volgende categorieën:

- Video-omgeving: beeldopnamen, interconnecties en beeldverwerking:
  - het doel van de beeldopnamen is het genereren van een beeld van de werkelijkheid in zodanige vorm dat het door de rest van het systeem kan worden gebruikt;
  - de interconnecties omvatten alle vormen van verzending van gegevens binnen de video-omgeving, d.w.z. verbindingen en communicatie. Voorbeelden van verbindingen zijn kabels, digitale netwerken en draadloze verzending. De communicatie omvat alle videosignalen en controlegegevens, die zowel digitaal als analoog kunnen zijn;
  - de beeldverwerking omvat de analyse, opslag en presentatie van een beeld of een reeks beelden.
- Vanuit het oogpunt van systeembeheer heeft een VSS de volgende logische functies:
  - gegevensbeheer en activiteitenbeheer, met inbegrip van de uitvoering van gebruikersopdrachten en door het systeem gegenereerde activiteiten (alarmprocedures, waarschuwingen aan gebruikers);
  - interfaces met andere systemen, waaronder verbindingen met andere beveiligingssystemen (toegangscontrole, brandalarm) en andersoortige systemen (systemen voor gebouwbeheer, automatische kentekenherkenning).
- De beveiliging van systemen voor videobewaking heeft betrekking op de vertrouwelijkheid, integriteit en beschikbaarheid van het systeem en de gegevens:
  - de systeembeveiliging omvat de fysieke beveiliging van alle systeemonderdelen en de controle op de toegang tot het VSS;
  - de gegevensbeveiliging omvat het voorkomen van verlies of manipulatie van gegevens.

[21] De AVG geeft hier geen definitie van, maar een technische beschrijving kan bijvoorbeeld worden gevonden in EN 62676-1-1: 2014 Videobewakingssystemen voor gebruik in beveiligingstoepassingen – Deel 1-1: Systeemeisen.

125.

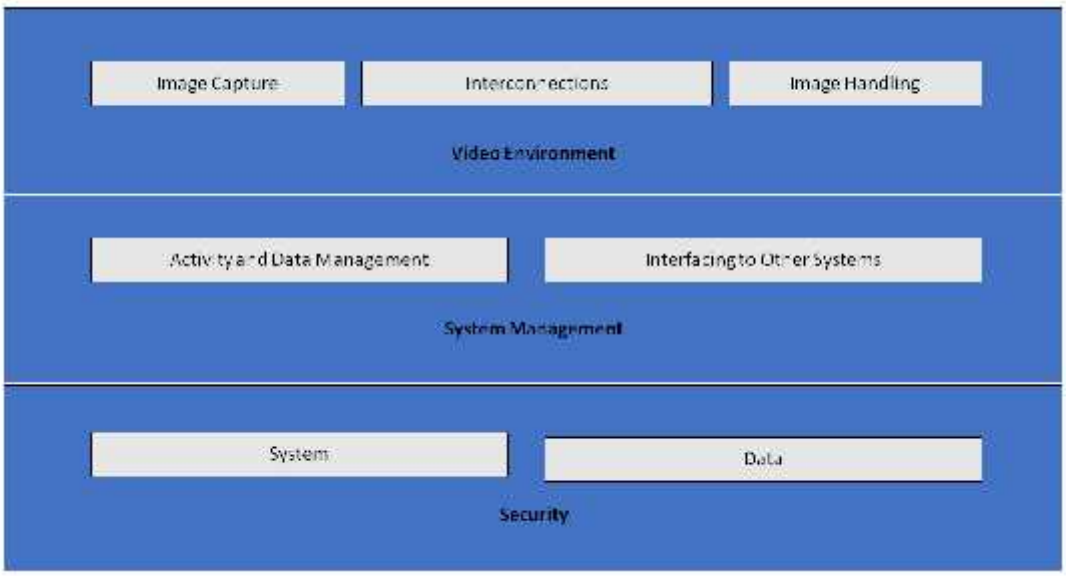

Image Capture	Beeldopnamen
Interconnections	Interconnecties
Image Handling	Beeldverwerking
Video Environment	Video-omgeving
Activity and Data Management	Activiteiten- en gegevensbeheer
Interfacing to Other Systems	Koppeling aan andere systemen
System Management	Systeembeheer
System	Systeem
Data	Gegevens
Security	Beveiliging

Figuur 1– Videobewakingssysteem

9.2 Gegevensbescherming door ontwerp en door standaardinstellingen

126. Zoals aangegeven in artikel 25 AVG moeten verwerkingsverantwoordelijken passende technische en organisatorische maatregelen treffen zodra zij het plan opvatten om gebruik te maken van videobewaking, dus voordat zij beginnen met het verzamelen en verwerken van videobeelden. Deze beginselen benadrukken de noodzaak van ingebouwde technologieën ter bevordering van de privacy, standaardinstellingen die de gegevensverwerking tot een minimum beperken en het ter beschikking stellen van de noodzakelijke hulpmiddelen om een zo groot mogelijke bescherming van persoonsgegevens mogelijk te maken.[22]

127. Verwerkingsverantwoordelijken moeten waarborgen voor de bescherming van gegevens en de persoonlijke levenssfeer niet alleen in de technologische ontwerpspecificaties, maar ook in hun organisatorische praktijken inbouwen. Wat de organisatorische praktijken betreft, moet de verwerkingsverantwoordelijke een passend beheerskader alsook beleid en procedures voor videobewaking vaststellen en de handhaving daarvan waarborgen. Vanuit technisch oogpunt moeten de specificaties en het ontwerp van het systeem eisen bevatten voor de verwerking van

[22] WP 168, advies over “De toekomst van privacy”, gezamenlijke bijdrage van de Groep gegevensbescherming artikel 29 en de Groep politie en justitie aan de raadpleging van de Europese Commissie over het rechtskader voor het grondrecht op bescherming van persoonsgegevens (goedgekeurd op 1 december 2009).

persoonsgegevens overeenkomstig de beginselen van artikel 5 AVG (rechtmatigheid van de verwerking, doelbinding, opslagbeperking, minimale gegevensverwerking door standaardinstellingen in de zin van artikel 25, lid 2, AVG, integriteit en vertrouwelijkheid, verantwoordingsplicht enz.). Wanneer een verwerkingsverantwoordelijke een commercieel videobewakingssysteem wil aanschaffen, moet hij deze eisen opnemen in de aankoopspecificatie. De verwerkingsverantwoordelijke moet waarborgen dat aan deze eisen wordt voldaan door deze op alle onderdelen van het systeem en alle daarmee verwerkte gegevens toe te passen, gedurende hun gehele levenscyclus.

9.3 Concrete voorbeelden van relevante maatregelen

128. De meeste maatregelen die kunnen worden gebruikt om videobewaking te beveiligen, met name wanneer hierbij wordt gebruikgemaakt van digitale apparatuur en software, zullen niet verschillen van de maatregelen die in andere IT-systemen worden gebruikt. Ongeacht de gekozen oplossing moet de verwerkingsverantwoordelijke alle onderdelen van het videobewakingssysteem en de gegevens in alle fasen afdoende beschermen, d.w.z. zowel tijdens de opslag (*gegevens in rusttoestand*), de verzending (*gegevens in transit*) en de verwerking (*gegevens in gebruik*). Om deze reden is het noodzakelijk dat verwerkingsverantwoordelijken en verwerkers organisatorische en technische maatregelen combineren.

129. Bij de keuze van technische oplossingen moet de verwerkingsverantwoordelijke privacyvriendelijke technologieën mede in overweging nemen omdat deze de veiligheid ten goede komen. Voorbeelden van dergelijke technologieën zijn systemen die het mogelijk maken om delen van het beeld die niet van belang zijn voor de bewaking af te schermen of vager te maken, of om de beelden van derden weg te laten wanneer er video-opnamen aan betrokkenen worden verstrekt.[23] Anderzijds mogen de gekozen oplossingen geen functionaliteiten bieden die niet noodzakelijk zijn (bv. onbeperkte bewegingsmogelijkheden van camera's, zoomfunctie, radioverzending, analysefuncties en geluidsopnamen). De aanwezige, maar niet noodzakelijke functies moeten worden uitgeschakeld.

130. Over dit onderwerp is veel vakinformatie beschikbaar, waaronder internationale normen en technische specificaties betreffende de fysieke beveiliging van multimediasystemen[24] en de beveiliging van algemene IT-systemen[25]. Daarom wordt in dit deel slechts een beknopt overzicht van dit onderwerp gegeven.

9.3.1 Organisatorische maatregelen

131. Naast een mogelijk vereiste gegevensbeschermingseffectbeoordeling (zie deel 10) moeten verwerkingsverantwoordelijken bij het bepalen van hun eigen beleid en procedures voor videobewaking de volgende aspecten in overweging nemen:

- wie verantwoordelijk is voor het beheer en het gebruik van het videobewakingssysteem;
- het doel en toepassingsgebied van het videobewakingsproject;

[23] Het gebruik van dergelijke technologieën kan in sommige gevallen zelfs verplicht zijn om te voldoen aan artikel 5, lid 1, onder c). Zij kunnen hoe dan ook dienen als voorbeelden van beste praktijken.

[24] IEC TS 62045 – Multimediabeveiliging – Richtsnoer voor de privacybescherming van in- en uitgeschakelde apparatuur en systemen.

[25] ISO/IEC 27000 – Reeks over informatiebeveiligingsbeheersystemen.

- gepaste en verboden videobewaking (waar en wanneer videobewaking is toegestaan en waar en wanneer niet, bv. het gebruik van verborgen camera's of van camera's die ook geluid opnemen)[26].
- transparantiemaatregelen als bedoeld in deel 7, "Transparantie en informatieverplichtingen";
- hoe en hoe lang de video's worden opgenomen, met inbegrip van de opslag van video-opnamen in verband met beveiligingsincidenten;
- wie een passende opleiding moet krijgen, en wanneer;
- wie toegang heeft tot de video-opnamen en voor welke doeleinden;
- operationele procedures (bv. door wie en waar worden de videobeelden gemonitord; wat te doen in geval van inbreuken in verband met persoonsgegevens);
- welke procedures externe partijen moeten volgen voor het opvragen van video-opnamen, alsook de procedures voor het weigeren of toewijzen van dergelijke verzoeken;
- procedures voor de aankoop, installatie en onderhoud van videobewakingssystemen;
- procedures voor het beheer en de correctie van incidenten.

9.3.2 Technische maatregelen

132. **Systeembeveiliging** betekent de **fysieke beveiliging** van alle systeemonderdelen, alsook systeemintegriteit, d.w.z. **bescherming en bestendigheid tegen opzettelijke en onopzettelijke inbreuken op de normale activiteiten** en **toegangscontrole**. Gegevensbeveiliging betekent **vertrouwelijkheid** (gegevens zijn alleen toegankelijk voor aan wie toegang wordt verleend), **integriteit** (preventie van gegevensverlies of manipulatie) en **beschikbaarheid** (gegevens kunnen worden geraadpleegd wanneer dat nodig is).

133. **Fysieke beveiliging** is een essentieel onderdeel van gegevensbescherming en vormt de eerste verdedigingslinie, omdat de VSS-apparatuur hiermee wordt beschermd tegen diefstal, vandalisme, natuurrampen, door de mens veroorzaakte rampen en onopzettelijke beschadiging (bv. door overspanning, extreme temperaturen of gemorste koffie). In het geval van analoge systemen speelt fysieke beveiliging een centrale rol bij de bescherming daarvan.

134. **Systeem- en gegevensbeveiliging**, d.w.z. bescherming tegen opzettelijke en onopzettelijke inbreuken op de normale werking ervan, omvat onder meer:

- bescherming van de volledige VSS-infrastructuur (waaronder op afstand bestuurde camera's, de bekabeling en stroomvoorziening) tegen fysieke manipulatie en diefstal;
- beveiliging van de verzending van beelden met tegen onderschepping beveiligde communicatiekanalen;
- gegevensversleuteling;
- gebruik van op hardware en software gebaseerde oplossingen, zoals firewalls, antivirus- of inbraakdetectiesystemen tegen cyberaanvallen;
- detectie van storingen in onderdelen, software en interconnecties;
- de manieren om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot het systeem te herstellen.

135. **Toegangscontrole** zorgt ervoor dat alleen daartoe gemachtigde personen toegang hebben tot het systeem en de gegevens, terwijl anderen de toegang wordt belet. Mogelijke maatregelen ter ondersteuning van de fysieke en logische toegangscontrole zijn:

[26] Dit kan afhangen van de nationale wetgeving en van brancheregels.

- waarborgen dat alle locaties waar videobewaking plaatsvindt en waar videobeelden worden opgeslagen, beveiligd zijn tegen de ongecontroleerde toegang van derden;
- monitors zodanig plaatsen (met name als ze zich in open ruimten bevinden, zoals een receptie) dat alleen daartoe gemachtigde medewerkers deze kunnen bekijken;
- vaststelling en handhaving van procedures voor het verlenen, wijzigen en intrekken van rechten voor fysieke en logische toegang;
- methoden en middelen voor de authenticatie en autorisatie van gebruikers, inclusief bijvoorbeeld de lengte van de wachtwoorden en de frequentie waarmee deze worden gewijzigd;
- de door gebruikers uitgevoerde acties (zowel met betrekking tot het systeem als de gegevens) worden geregistreerd en regelmatig beoordeeld;
- voortdurende monitoring en opsporing van toegangsfouten; geconstateerde tekortkomingen worden zo spoedig mogelijk gecorrigeerd.

10 GEGEVENSBESCHERMINGSEFFECTBEOORDELING

136. Volgens artikel 35, lid 1, AVG zijn verwerkingsverantwoordelijken verplicht om gegevensbeschermingseffectbeoordelingen uit te voeren wanneer een soort gegevensverwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Artikel 35, lid 3, onder c), AVG bepaalt dat verwerkingsverantwoordelijken verplicht zijn om gegevensbeschermingseffectbeoordelingen uit te voeren als de verwerking een stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten behelst. Bovendien is volgens artikel 35, lid 3, onder b), AVG een gegevensbeschermingseffectbeoordeling ook vereist wanneer de verwerkingsverantwoordelijke voornemens is op grote schaal bijzondere categorieën persoonsgegevens te verwerken.

137. De richtsnoeren voor gegevensbeschermingseffectbeoordelingen[27] bieden nadere adviezen en meer gedetailleerde voorbeelden die van belang zijn voor videobewaking (bv. over het "gebruik van een camerasysteem om het rijgedrag op snelwegen te controleren"). Volgens artikel 35, lid 4, AVG moet elke toezichthoudende autoriteit een lijst publiceren van de soorten verwerkingen waarvoor in het desbetreffende land een gegevensbeschermingseffectbeoordeling verplicht is. De lijsten zijn doorgaans te vinden op de websites van deze autoriteiten. Gezien de doeleinden waar videobewaking doorgaans voor wordt gebruikt (bescherming van personen en gebouwen, opsporing, preventie en beheersing van strafbare feiten, verzamelen van bewijzen en biometrische identificatie van verdachten), is het redelijk om aan te nemen dat voor veel gevallen van videobewaking een gegevensbeschermingseffectbeoordeling vereist is. Verwerkingsverantwoordelijken moeten deze documenten derhalve zorgvuldig raadplegen om te bepalen of een dergelijke beoordeling vereist is, en zo ja, deze vervolgens uitvoeren. Het resultaat van de uitgevoerde gegevensbeschermingseffectbeoordeling is bepalend voor de gegevensbeschermingsmaatregelen die de verwerkingsverantwoordelijke besluit uit te voeren.

138. Het is ook belangrijk om op te merken dat indien uit de resultaten van de gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico met zich meebrengt, ondanks de door de verwerkingsverantwoordelijke geplande veiligheidsmaatregelen, er voorafgaand aan de verwerking overleg moet worden gevoerd met de betrokken toezichthoudende autoriteit. Nadere bijzonderheden over dit voorafgaand overleg zijn te vinden in artikel 36.

Voor het Europees Comité voor gegevensbescherming

De voorzitter

(Andrea Jelinek)

[27] WP 248, rev.01, Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of de verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679. – goedgekeurd door het Europees Comité voor gegevensbescherming (EDPB)