Retningslinjer 3/2019 om brug af videoudstyr til behandling af personoplysninger

Version 2.0

Vedtaget den 29. januar 2020

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

Versionsoversigt

Version 2.1	26. februar 2020	Ændring af en materiel fejl
Version 2.0	29. januar 2020	Vedtagelse af retningslinjerne efter offentlig høring
Version 1.0	10. juli 2019	Vedtagelse af retningslinjerne til offentlig høring

Indholdsfortegnelse

Det Europæiske Databeskyttelsesråd har –

under henvisning til artikel 70, stk. 1, litra e), i Europa-Parlamentets og Rådets forordning 2016/679/EU af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (i det følgende benævnt "GDPR")

under henvisning til EØS-aftalen, særligt til dennes bilag XI og protokol 37, som ændret ved Det Blandede EØS-Udvalgs afgørelse nr. 154/2018 af 6. juli 2018[1]

under henvisning til artikel 12 og artikel 22 i forretningsordenen –

VEDTAGET FØLGENDE RETNINGSLINJER

1 INDLEDNING

1. Den intensive brug af videoudstyr påvirker borgernes adfærd. Omfattende indførelse af sådanne værktøjer på mange områder af folks liv vil lægge yderligere pres på den enkelte med henblik på at undgå opdagelse af, hvad mange kan opfatte som unormalt. Faktisk kan disse teknologier begrænse mulighederne for at bevæge sig anonymt og bruge tjenester anonymt og i det hele taget begrænse muligheden for at forblive ubemærket. Databeskyttelse har omfattende konsekvenser.

2. Uanset at enkeltpersoner måske føler sig veltilpas med videoovervågning, der er indført til et bestemt sikkerhedsformål, skal der f.eks. sikres garanti for at undgå ethvert misbrug til helt andre og – for den registrerede – uventede formål (f.eks. markedsføring, overvågning af ansattes præstationer mv.). Dertil kommer, at der nu bruges mange værktøjer til at udnytte de billeder, der tages, og omdanne traditionelle kameraer til intelligente kameraer. I kombination med disse værktøjer og teknikker øger den mængde data, der genereres med video, risiciene for sekundær anvendelse (uanset om denne har tilknytning eller ej til systemets oprindelige formål) og endda risiciene for misbrug. Der bør altid tages nøje hensyn til de generelle principper i GDPR (artikel 5) i forbindelse med videoovervågning.

3. Systemer til videoovervågning ændrer på mange måder, hvordan fagfolk fra den private og den offentlige sektor interagerer på private eller offentlige steder med det formål at øge sikkerheden, foretage publikumsanalyse, lave personaliseret reklame osv. Videoovervågning er blevet højeffektiv i takt med den stigende indførelse af intelligent videoanalyse. Disse teknikker kan være mere indgribende (f.eks. komplekse biometriske teknikker) eller mindre indgribende (f.eks. simple optællingsalgoritmer). At forblive anonym og beskytte retten til privatliv bliver generelt sværere. De databeskyttelsesspørgsmål, der rejser sig i den enkelte situation, kan være forskellige, hvilket også gælder den juridiske analyse, afhængigt af om den ene eller den anden af disse teknologier anvendes.

4. Ud over problemer vedrørende privatlivets fred er der også risici forbundet med eventuelle funktionsfejl i anordningerne og de skævvridninger, de kan medføre. Forskere melder om, at den software, der anvendes til ansigtsidentificering, -genkendelse eller -analyse, fungerer forskelligt alt

[1] Betegnelsen "medlemsstater" i denne udtalelse skal forstås som "EØS-medlemsstater".

efter alder, køn og etnicitet hos den person, som identificeres. Algoritmer, der baseres på forskellige demografiske faktorer, kan indebære skævvridninger med hensyn til ansigtsgenkendelse, hvilket kan forstærke fordomme i samfundet. Dataansvarlige skal derfor også sørge for, at biometrisk behandling af data, der stammer fra videoovervågning, regelmæssigt vurderes ud fra relevans, og at der stilles tilstrækkelige garantier.

5. Udgangspunktet bør ikke være, at videoovervågning er en nødvendighed, når der er andre måder at nå det underliggende mål på. Ellers risikerer vi, at de kulturelle normer ændres i retning af almindelig accept af manglende beskyttelse af privatlivets fred.

6. Disse retningslinjer har til formål at vejlede om, hvordan GDPR skal anvendes i forbindelse med behandling af personoplysninger med videoudstyr. Eksemplerne er ikke udtømmende, men det generelle ræsonnement kan anvendes på alle tænkelige anvendelsesområder.

2 ANVENDELSESOMRÅDE[2]

2.1 Personoplysninger

7. Systematisk, automatiseret overvågning af et bestemt område med optiske eller audiovisuelle midler, hovedsagelig for at beskytte ejendom eller den enkeltes liv og sundhed, er i vore dage blevet et vigtigt fænomen. Denne aktivitet fører til indsamling og opbevaring af billeder eller audiovisuelle oplysninger om alle personer, som begiver sig ind i det overvågede område, og som kan identificeres på deres udseende eller andre særlige elementer. Disse personers identitet kan fastslås på grundlag af disse oplysninger. Denne aktivitet giver desuden mulighed for yderligere behandling af personoplysninger om personers tilstedeværelse og adfærd i det pågældende område. Den eventuelle risiko for misbrug af disse data vokser i forhold til det overvågede områdes størrelse og antallet af personer, der hyppigt kommer i området. Dette afspejles i artikel 35, stk. 3, litra c), i GDPR, som kræver, at der foretages en konsekvensanalyse vedrørende databeskyttelse i tilfælde af en systematisk overvågning af et offentligt tilgængeligt område i stort omfang, samt i artikel 37, stk. 1, litra b), der pålægger den dataansvarlige og databehandleren at udpege en databeskyttelsesrådgiver, når den dataansvarliges eller databehandlerens kerneaktiviteter indebærer regelmæssig og systematisk overvågning af registrerede.

8. Forordningen finder dog ikke anvendelse på behandling af oplysninger, der ikke omhandler en person, f.eks. hvis en person direkte eller indirekte ikke kan identificeres.

> Eksempel: GDPR finder ikke anvendelse på falske kameraer (dvs. kameraer, der ikke fungerer som kamera og derfor ikke behandler personoplysninger). *I nogle medlemsstater kan dette dog være omfattet af anden lovgivning.*
>
> Eksempel: Optagelser fra stor højde falder kun ind under anvendelsesområdet for GDPR, hvis de behandlede data under de givne omstændigheder kan knyttes til en bestemt person.
>
> Eksempel: Et videokamera er indbygget i en bil for at give parkeringsassistance. Hvis kameraet er konstrueret eller indstillet på en måde, så det ikke indsamler oplysninger om en fysisk person (f.eks. nummerplader eller oplysninger, der kan identificere forbipasserende), finder GDPR ikke anvendelse.

9.

2.2 Anvendelse af retshåndhævelsesdirektivet (LED) (EU/2016/680)

10. Under direktiv EU/2016/680 falder navnlig kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod eller forebygge trusler mod den offentlige sikkerhed.

[2] Det Europæiske Databeskyttelsesråd bemærker, at hvor GDPR tillader det, kan der gælde særlige krav i national lovgivning.

2.3 Undtagelse for familiemæssige aktiviteter

11. I henhold til artikel 2, stk. 2, litra c), finder GDPR ikke anvendelse for behandling af personoplysninger, som en fysisk person foretager som led i rent personlige eller familiemæssige aktiviteter, der også kan omfatte onlineaktivitet.[3]

12. Denne bestemmelse – den såkaldte familiemæssige undtagelse – skal fortolkes snævert i forbindelse med videoovervågning. Som Domstolen har fastslået, skal den såkaldte familiemæssige undtagelse skal "*fortolkes således, at den udelukkende vedrører de aktiviteter, der indgår i den enkelte borgers privatliv eller familieliv, hvilket åbenbart ikke er tilfældet med hensyn til behandling af personoplysninger, som består i, at de offentliggøres på internettet, hvorved disse oplysninger bliver tilgængelige for et ubestemt antal personer*".[4] Desuden gælder, at hvis et videoovervågningssystem, i det omfang det indebærer en konstant registrering og lagring af personoplysninger, og "*– om end kun delvist – derfor optager uden for det private rum, som den, der gennem overvågningen foretager behandlingen af disse oplysninger, befinder sig i, kan den ikke anses for en rent "personlig eller familiemæssig" aktivitet som omhandlet i artikel 3 stk. 2, andet led, i direktiv 95/46.*"[5]

13. Hvad angår videoudstyr, der anvendes i en privat persons lokaler, kan det være omfattet af undtagelsen vedrørende familiemæssige aktiviteter. Dette vil afhænge af flere faktorer, som alle skal tages i betragtning for at nå frem til en konklusion. Ud over de ovennævnte elementer, der er identificeret i Domstolens afgørelser, skal brugeren af videoovervågning i hjemmet tage i betragtning, om han har nogen form for personlig relation til den registrerede, om overvågningens omfang eller hyppighed tyder på nogen form for erhvervsmæssig aktivitet fra hans side, og om overvågningen har potentielle negative konsekvenser for de registrerede. Tilstedeværelsen af bare et enkelt af ovennævnte elementer tyder ikke nødvendigvis på, at behandlingen falder uden for anvendelsesområdet for den familiemæssige undtagelse. Der er derfor behov for en samlet vurdering for at fastslå dette.

> Eksempel: En turist optager videoer fra sin ferie både med sin mobiltelefon og et videokamera Han viser optagelserne til venner og familie, men gør dem ikke tilgængelige for et ubegrænset antal personer. Dette vil falde ind under den familiemæssige undtagelse.
>
> Eksempel: En mountainbiker vil optage sin tur ned ad bakke med et actionkamera. Hendes tur er i et afsides område, og hun har kun til hensigt anvende optagelserne til sin personlige underholdning hjemme. Dette falder ind under den familiemæssige undtagelse, selv om der til en vis grad er tale om behandling af personoplysninger.
>
> Eksempel: En person overvåger og optager sin egen have. Ejendommen er indhegnet, og kun den dataansvarlige selv og hans familie kommer regelmæssigt ind i haven. Dette falder ind under den familiemæssige undtagelse, forudsat at videoovervågningen ikke – heller ikke delvis – omfatter et offentligt område eller en naboejendom.

14.

[3] Jf. betragtning 18.

[4] Domstolens dom i sag C-101/01, *Bodil Lindqvist*-sagen, 6. november 2003, præmis 47

[5] Domstolens dom i sag C-212/13, *František Ryneš mod Úřad pro ochranu osobních údajů*, 11. december 2014, præmis 33.

3 LOVLIGHEDEN AF BEHANDLINGEN

15. Før anvendelse skal formålene med behandlingen specificeres nærmere (artikel 5, stk. 1, litra b)). Videoovervågning kan tjene mange formål, f.eks. beskyttelse af ejendom og andre aktiver, beskyttelse af personers liv og fysiske integritet, og indsamling af beviser vedrørende civilretlige søgsmål.[6] Sådanne overvågningsformål skal dokumenteres skriftligt (artikel 5, stk. 2) og skal specificeres for hvert overvågningskamera, der er i brug. Flere kameraer, som en enkelt dataansvarlig anvender til samme formål, kan dokumenteres samlet. Desuden skal de registrerede underrettes om formålet eller formålene med behandlingen i overensstemmelse med artikel 13 (*se afsnit 7, gennemsigtigheds- og oplysningspligt*). "Sikkerhed" eller "personers sikkerhed" som eneste begrundelse for videoovervågning er ikke tilstrækkelig specifikt (artikel 5, stk. 1, litra b)). Det er desuden i strid med princippet om, at personoplysninger skal behandles på lovlig, rimelig og gennemsigtig måde i forhold til den registrerede (jf. artikel 5, stk. 1, litra a)).

16. I princippet kan enhver juridisk begrundelse i henhold til artikel 6, stk. 1, være retsgrundlag for behandling af videoovervågningsdata. F.eks. finder artikel 6, stk. 1, litra c) anvendelse, hvis den nationale lovgivning fastsætter en forpligtelse til at foretage videoovervågning.[7] I praksis er de bestemmelser, der med størst sandsynlighed vil blive anvendt, imidlertid

- artikel 6, stk. 1, litra f) (legitim interesse)
- artikel 6, stk. 1, litra e) (nødvendigheden af at udføre en opgave i samfundets interesse eller under udøvelse af offentlig myndighed).

I særlige tilfælde kan den dataansvarlige anvende artikel 6, stk. 1, litra a) (samtykke) som retsgrundlag.

3.1 Legitim interesse, artikel 6, stk. 1, litra f)

17. Den retlige vurdering i artikel 6, stk. 1, litra f), bør baseres på følgende kriterier i overensstemmelse med betragtning 47.

3.1.1 Eksistensen af legitime interesser

18. Videoovervågning er lovlig, hvis den er nødvendig for at opfylde en dataansvarligs eller tredjemands legitime interesse, medmindre den registreredes grundlæggende rettigheder og friheder går forud herfor (artikel 6, stk. 1, litra f)). Legitime interesser, der forfølges af en dataansvarlig eller en tredjemand, kan være retlige[8], økonomiske eller immaterielle interesser.[9] Den dataansvarlige bør imidlertid tage hensyn til, at hvis den registrerede gør indsigelse mod overvågningen i henhold til artikel 21, kan den dataansvarlige kun foretage videoovervågning af den pågældende registrerede, hvis det er en *vægtig* legitim interesse, der går forud for den registreredes interesser, rettigheder og frihedsrettigheder, eller for at fastlægge, udøve eller forsvare retskrav.

---

[6] Reglerne om indsamling af bevismateriale med henblik på civilretlige søgsmål varierer fra medlemsstat til medlemsstat.

[7] Disse retningslinjer omfatter ikke analyse af eller går i detaljer med national lovgivning, som kan være forskellig fra medlemsstat til medlemsstat.

[8] Domstolens dom i sag C-13/16, *Rīgas satiksme*, 4. maj 2017

[9] jf. WP 217, artikel 29-Gruppen.

19. I en virkelig og farlig situation kan formålet om at beskytte ejendom mod indbrud, tyveri eller hærværk udgøre en legitim interesse hvad angår videoovervågning.

20. Den legitime interesse skal være reelt, og behovet skal være aktuelt (dvs. det må ikke være fiktivt eller spekulativt[10]. Der skal foreligge en reel nødsituation – som f.eks. skader eller tidligere alvorlige hændelser – før overvågningen iværksættes. På baggrund af princippet om ansvarlighed tilrådes dataansvarlige at dokumentere relevante hændelser (dato, karakter, økonomisk tab) og tilknyttede strafferetlige tiltaler. Sådanne dokumenterede hændelser kan være overbevisende vidnesbyrd om, at der foreligger en legitim interesse. Om der foreligger en legitim interesse, og om overvågning er nødvendig, bør tages op til fornyet overvejelse med regelmæssige mellemrum (f.eks. en gang om året, afhængigt af omstændighederne).

> Eksempel: En butiksindehaver ønsker at åbne en ny butik og installere et videoovervågningssystem for at forebygge hærværk. Han kan ved hjælp af statistikker vise, at der er stor risiko for hærværk i nabolaget. Erfaringer fra nabobutikker er også nyttige. Det er ikke nødvendigt, at den pågældende dataansvarlige har lidt et tab, så længe skaderne i naboområdet tyder på en fare eller lignende og derfor kan være tegn på en legitim interesse. Det er imidlertid ikke tilstrækkeligt at fremlægge nationale eller generelle statistiske data over kriminalitet uden at analysere det pågældende område eller farerne for netop denne butik.

21.

22. Situationer med overhængende fare kan udgøre en legitim interesse, således for banker eller for butikker, der sælger kostbare varer (f.eks. juvelerer), eller områder, der er kendt som typiske gerningssteder for krænkelse af ejendomsret (f.eks. benzinstationer).

23. I GDPR hedder det også klart, at offentlige myndigheder ikke kan begrunde behandlingen med legitim interesse, så længe de udfører deres opgaver (artikel 6, stk. 1, 2. punktum).

3.1.2 Lovligheden af behandlingen

24. Personoplysninger skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles ("dataminimering"), jf. artikel 5, stk. 1, litra c). Den dataansvarlige skal altid foretage en kritisk undersøgelse af, om denne foranstaltning for det første er egnet til at nå det ønskede mål, og for det andet er hensigtsmæssig og nødvendig til formålet. Videoovervågning bør kun vælges, hvis formålet med behandlingen ikke med rimelighed kan opfyldes på anden måde, som er mindre indgribende i den registreredes grundlæggende rettigheder og frihedsrettigheder.

25. I den situation, hvor en dataansvarlig ønsker at forhindre formuerelaterede forbrydelser, kan han i stedet for at installere et videoovervågningssystem også træffe alternative sikkerhedsforanstaltninger såsom at indhegne ejendommen, indføre regelmæssig patruljering med sikkerhedspersonale, bruge portvagter, sørge for bedre belysning, installere sikkerhedslåse og manipulationssikre vinduer og døre, eller anvende antigraffiti-overfladebehandling eller -folie på murene. Sådanne foranstaltninger kan være lige så effektive som videoovervågningssystemer over for indbrud, tyveri og hærværk. Den dataansvarlige skal fra sag til sag vurdere, om sådanne foranstaltninger kan være en rimelig løsning.

26. Inden den dataansvarlige anvender et kamerasystem, er han forpligtet til at vurdere, hvor og hvornår videoovervågning er strengt nødvendig. Et overvågningssystem, der opererer både om natten og uden

[10] Jf. WP217, artikel 29-Gruppen, s. 24 ff. Jf. også Domstolens dom i sag C-708/18, s. 44.

for normal arbejdstid, vil sædvanligvis opfylde den dataansvarliges behov for at afværge farer for ejendommen.

27. Behovet for at anvende videoovervågning til at beskytte den dataansvarliges lokaler ophører sædvanligvis ved ejendommens skel.[11] Der er dog tilfælde, hvor overvågning af selve ejendommen ikke er tilstrækkelig til effektiv beskyttelse. I visse enkeltstående tilfælde kan det være nødvendigt at udvide videoovervågningen til ejendommens umiddelbare omgivelser. I denne forbindelse bør den dataansvarlige overveje fysiske og tekniske midler som at blokere eller pixelere ikke relevante områder.

> Eksempel: En boghandel vil beskytte sine lokaler mod hærværk. Sædvanligvis bør kameraerne kun filme selve lokalerne, da det til dette formål ikke er nødvendigt at se naboområder eller offentlige områder omkring boghandelens lokaler.

28.

29. Spørgsmål om behandlingens nødvendighed melder sig også i forbindelse med den måde, dokumentation opbevares på. I nogle tilfælde kan det være nødvendigt at anvende løsninger med sorte bokse, hvor optagelserne automatisk slettes efter en vis opbevaringsperiode og kun tilgås i forbindelse med en hændelse. I andre situationer er det måske slet ikke nødvendigt at opbevare videomaterialet, men mere hensigtsmæssigt i stedet at anvende løbende overvågning. Valget mellem løsninger med sorte bokse eller realtidsovervågning bør også baseres på det tilstræbte formål. Hvis formålet med videoovervågning f.eks. er at opbevare dokumentation, er metoder med realtidsovervågning sædvanligvis ikke egnede. Undertiden kan realtidsovervågning også være mere indgribende, end at materialet opbevares og efter en begrænset tidsramme automatisk slettes (hvis en person f.eks. til stadighed iagttager skærmen, kan det være mere indgribende, end hvis der slet ikke er nogen skærm, og materialet direkte overføres til en sort boks til opbevaring). Princippet om dataminimering skal ses i denne sammenhæng (artikel 5, stk. 1, litra c)). Man bør også være opmærksom på, at der er mulighed for, at den dataansvarlige i stedet for videoovervågning bruger sikkerhedspersonale, der er i stand til straks at reagere og gribe ind.

3.1.3 Afvejning af interesser

30. Når videoovervågning er nødvendig for at beskytte en dataansvarligs legitime interesser, må videoovervågningssystemet kun tages i brug, hvis den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder ikke går forud for den dataansvarliges eller en tredjeparts legitime interesser (f.eks. at beskytte ejendom eller fysisk integritet). Den dataansvarlige skal overveje 1), i hvilket omfang overvågningen påvirker enkeltpersoners interesser, grundlæggende rettigheder og frihedsrettigheder, og 2) om dette medfører krænkelse af eller negative konsekvenser for den registreredes rettigheder. At afveje interesserne er faktisk påbudt. Grundlæggende rettigheder og frihedsrettigheder på den ene side og den dataansvarliges legitime interesser på den anden side skal nøje vurderes og afvejes.

[11] Dette kan i nogle medlemsstater også være underlagt national lovgivning.

Eksempel: En privat parkeringsvirksomhed har dokumenteret, at der er gentagne problemer med tyverier fra de parkerede biler. Parkeringspladsen er et åbent område, der er let tilgængeligt for alle, men tydeligt markeret med skilte og afspærringer omkring området. Parkeringsvirksomheden har en legitim interesse (at forebygge tyveri fra kundernes biler) i at overvåge området i det tidsrum af dagen, hvor den oplever problemer. De registrerede overvåges inden for en begrænset tidsramme, de befinder sig ikke i området til rekreative formål, og det er også i deres egen interesse at forhindre tyverierne. Den dataansvarliges legitime interesse går i dette tilfælde forud for de registreredes interesse i ikke at blive overvåget.

Eksempel: En restaurant beslutter at installere videokameraer i toiletterne for at kontrollere, at de sanitære faciliteter er i orden. I dette tilfælde har de registreredes rettigheder klart forrang for den dataansvarliges interesser, og der kan følgelig ikke installeres kameraer på dette sted.

31.

3.1.3.1 Afgørelse i hvert enkelt tilfælde

32. Da interesseafvejning er påbudt i henhold til forordningen, skal afgørelsen træffes fra tilfælde til tilfælde (jf. artikel 6, stk. 1, litra f)). Henvisning til abstrakte situationer eller sammenligning med lignende tilfælde er ikke tilstrækkeligt. Den dataansvarlige skal vurdere risikoen for krænkelse af den registreredes rettigheder; her er det afgørende kriterium graden af indgriben i den enkeltes rettigheder og friheder.

33. Intensiteten kan bl.a. defineres ved den type oplysninger, der indsamles (oplysningernes indhold), deres omfang (informationsniveau, rumlige og geografiske udstrækning), antallet af berørte registrerede, enten som et konkret tal eller som andel af den pågældende befolkningsgruppe, den pågældende situation, de registreredes faktiske interesser, alternative midler samt datavurderingens art og omfang.

34. Vigtige afbalancerende faktorer kan være størrelsen af det overvågede område og antallet af registrerede, der overvåges. Brug af videoovervågning i et afsides område (f.eks. med henblik på at se vilde dyr eller planter eller beskytte kritisk infrastruktur såsom en privatejet radioantenne) skal vurderes anderledes end videoovervågning i en fodgængerzone eller et indkøbscenter.

Eksempel: Hvis der er installeret et bilkamera (f.eks. for at indsamle dokumentation i tilfælde af et uheld), er det vigtigt at sikre, at dette kamera ikke konstant optager trafikken eller personer ved vejen. Ellers kan interessen i at have videooptagelser som bevis, hvis et trafikuheld rent teoretisk skulle finde sted, ikke berettige dette alvorlige indgreb i registreredes rettigheder.[11]

35.

3.1.3.2 Registreredes rimelige forventninger

36. Ifølge betragtning 47 skal der foretages en omhyggelig vurdering af, om der foreligger en legitim interesse. Dette skal omfatte den registreredes rimelige forventninger på det pågældende tidspunkt i sammenhæng med den behandling af vedkommendes personoplysninger, der foretages. Ved systematisk overvågning kan relationen mellem den registrerede og den dataansvarlige være ret forskellig og kan have betydning for, hvilke rimelige forventninger den registrerede kan have. Fortolkningen af begrebet rimelige forventninger bør ikke alene baseres på de pågældende subjektive forventninger. Det afgørende kriterium skal snarere være, om en objektiv tredjemand med rimelighed kan forvente og konkludere at være underkastet overvågning i denne konkrete situation.

37. F.eks. forventer en arbejdstager som regel ikke at blive overvåget på arbejdsstedet af sin arbejdsgiver.[12] Man bør heller ikke kunne forvente at blive overvåget i sin egen have, i beboelsesområder eller i undersøgelses- og behandlingsrum. Tilsvarende er det ikke rimeligt at forvente overvågning i sanitære faciliteter eller en sauna – overvågning af sådanne områder er et stærkt indgreb i den registreredes rettigheder. De registreredes rimelige forventninger er, at der ikke er videoovervågning i sådanne omgivelser. På den anden side vil en bankkunde måske forvente at blive overvåget i banken eller ved pengeautomaten.

38. Registrerede kan også forvente at være fri for overvågning på offentlige områder, navnlig på områder, der typisk anvendes til rekreative formål og fritidsaktiviteter, og på steder, hvor enkeltpersoner opholder sig og/eller kommunikerer, som f.eks. i siddeområder, ved borde i restauranter, i parker, biografer og fitnesscentre. Her vil den registreredes interesser eller rettigheder og frihedsrettigheder ofte gå forud for den dataansvarliges legitime interesser.

> Eksempel: På toiletter forventer registrerede ikke at blive overvåget. Videoovervågning for f.eks. at forebygge ulykker er ikke forholdsmæssig.

39.

40. Skilte, der oplyser den registrerede om videoovervågningen, har ingen relevans i forbindelse med fastlæggelsen af, hvad en registreret objektivt kan forvente. Det betyder f.eks., at en butiksindehaver ikke kan forlade sig på, at kunderne *objektivt set* har rimelig forventning om at blive overvåget, blot fordi et skilt ved indgangen informerer den pågældende om overvågningen.

3.2 Behandlingen er nødvendig af hensyn til udførelse af en opgave, som er i samfundets interesse eller henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt (artikel 6, stk. 1, litra e)).

41. Persondata vil kunne behandles ved videoovervågning i henhold til artikel 6, stk. 1, litra e), hvis det er nødvendigt for at udføre en opgave i samfundets interesse eller under udøvelse af offentlig myndighed.[13] Udøvelse af offentlig myndighed tillader ikke nødvendigvis sådan behandling, men andre retsgrundlag såsom "sundhed og sikkerhed" til beskyttelse af besøgende og arbejdstagere kan give begrænset mulighed for behandling, når der samtidig tages hensyn til GDPR's regler om forpligtelser og registreredes rettigheder.

42. Medlemsstaterne kan opretholde eller indføre særlig national lovgivning om videoovervågning for at tilpasse anvendelsen af reglerne i GDPR ved at fastsætte mere præcise specifikke krav til behandling, når blot det er i overensstemmelse med principperne i GDPR (f.eks. begrænsning af opbevaring, proportionalitet).

[12] Se også: Artikel 29-Gruppen, udtalelse 2/2017 om databehandling på arbejdspladsen, WP249, vedtaget den 8. juni 2017.

[13] Grundlaget for behandlingen skal fremgå af EU-ret eller medlemsstatens ret og skal være "nødvendigt for udførelsen af en opgave i samfundets interesse eller henhørende under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt" (artikel 6, stk. 3).

3.3 Samtykke (artikel 6, stk. 1, litra a)

43. Samtykke skal være frivilligt, specifikt, informeret og utvetydigt som beskrevet i retningslinjerne for samtykke.[14]

44. Ved systematisk overvågning kan den registreredes samtykke kun undtagelsesvis anvendes som retsgrundlag i overensstemmelse med artikel 7 (jf. betragtning 43). Det ligger i overvågningens natur, at denne teknologi overvåger et ukendt antal mennesker på én gang. Den dataansvarlige vil næppe kunne bevise, at den registrerede har givet sit samtykke, inden dennes personoplysninger behandles (artikel 7, stk. 1). Hvis den registrerede trækker sit samtykke tilbage, vil det være vanskeligt for den dataansvarlige at bevise, at personoplysningerne ikke længere behandles (artikel 7, stk. 3).

> Eksempel: Idrætsudøvere kan anmode om overvågning under de enkelte øvelser for at analysere deres teknik og resultater. Hvis derimod en sportsklub tager initiativ til at overvåge et helt hold til samme formål, vil samtykket ofte ikke være gyldigt, da de enkelte idrætsudøvere kan føle sig presset til at give samtykke, for at deres afslag på samtykke ikke skal påvirke deres holdkammerater negativt.

45.

46. Hvis den dataansvarlige ønsker at påberåbe sig samtykket, er vedkommende forpligtet til sikre, at hver registreret, der begiver sig ind i det videoovervågede område, har givet samtykke. Dette samtykke skal opfylde betingelserne i artikel 7. Registrering af et afmærket overvåget område (hvor personer f.eks. anmodes om at benytte en bestemt gang eller port for at begive sig ind i et overvåget område), udgør ikke en sådan erklæring eller klar bekræftelse, som er nødvendig for samtykke, medmindre det opfylder kriterierne i artikel 4 og 7 som beskrevet i retningslinjerne for samtykke.[15]

47. I betragtning af den ulige magtbalance mellem arbejdsgivere og arbejdstagere bør arbejdsgivere i de fleste tilfælde ikke forlade sig på samtykket, når de behandler personoplysninger, da det næppe er givet frivilligt. Retningslinjerne for samtykke bør tages i betragtning i denne forbindelse.

48. Medlemsstaternes nationale lovgivning eller kollektive overenskomster kan indeholde særlige regler for behandling af arbejdstageres personoplysninger i arbejdsmæssig sammenhæng (jf. artikel 88).

[14] Artikel 29-Gruppens (Art 29 WP) retningslinjer for samtykke i henhold til forordning 2016/679 (WP 259 rev. 01). – godkendt af Det Europæiske Databeskyttelsesråd

[15] Artikel 29-Gruppens (Artikel 29 WP): retningslinjer for samtykke i henhold til forordning 2016/679 (WP 259) – godkendt af Det Europæiske Databeskyttelsesråd – som bør tages i betragtning

4 VIDEREGIVELSE AF VIDEOMATERIALE TIL TREDJEPARTER

49. Principielt finder de generelle bestemmelser i GDPR anvendelse på videregivelse af videooptagelser til tredjeparter.

4.1 Videregivelse af videomateriale til tredjeparter generelt

50. Videregivelse er i artikel 4, stk. 2, defineret som transmission (f.eks. individuel meddelelse), formidling (f.eks. offentliggørelse online) eller anden form for overladelse. Tredjeparter er defineret i artikel 4, stk. 10. For offentliggørelse af oplysninger til tredjelande eller internationale organisationer finder de særlige bestemmelser i artikel 44 ff. også anvendelse.

51. Enhver videregivelse af personoplysninger er en særskilt form for behandling af personoplysninger, som den dataansvarlige skal have hjemmel til i artikel 6.

> Eksempel: En dataansvarlig, der ønsker at uploade en optagelse til internettet, skal have et retsgrundlag for denne behandling, f.eks. i form af et samtykke indhentet fra den registrerede i henhold til artikel 6, stk. 1, litra a).

52.

53. Overførsel af en videooptagelse til tredjemand til andet formål end det, personoplysningerne er indsamlet til, er mulig efter reglerne i artikel 6, stk. 4.

> Eksempel: Der er installeret videoovervågning af en bom (ved et parkeringsanlæg) med henblik på at opklare skader. Der opstår en skade, og optagelsen overføres til en advokat med henblik på retsforfølgning. I dette tilfælde er formålet med optagelsen det samme som med overførslen.
>
> Eksempel: Der er installeret videoovervågning af en bom (ved et parkeringsanlæg) med henblik på at opklare skader. Optagelsen offentliggøres online til ren underholdningsbrug. I dette tilfælde er formålet ændret og er ikke foreneligt med det oprindelige formål. Det ville desuden være problematisk at finde frem til et retsgrundlag for denne behandling (offentliggørelse).

54.

55. En tredjepartsmodtager vil skulle foretage sin egen retlige analyse, navnlig ved at identificere retsgrundlaget i henhold til artikel 6 for sin behandling (f.eks. at modtage materialet).

4.2 Videregivelse af videomateriale til retshåndhævende myndigheder

56. Videregivelsen af videooptagelser til retshåndhævende organer er også en uafhængig proces, som kræver særskilt begrundelse fra den dataansvarlige.

57. Behandlingen er lovlig i henhold til artikel 6, stk. 1, litra c), hvis den er nødvendig for at overholde en retlig forpligtelse, som den dataansvarlige er underkastet. Den gældende strafferetlige lovgivning er udelukkende under medlemsstaternes kontrol, men der er sandsynligvis i alle medlemsstater generelle regler for overførsel af bevismateriale til retshåndhævende myndigheder. Den behandling, der foretages af den dataansvarlige, som overfører dataene, er reguleret ved GDPR. Hvis den dataansvarlige i henhold til national lovgivning skal samarbejde med de retshåndhævende myndigheder (f.eks. med henblik på efterforskning), er retsgrundlaget for udlevering af oplysningerne den retlige forpligtelse i henhold til artikel 6, stk. 1, litra c).

58. Formålsbegrænsningen i artikel 6, stk. 4, er da ofte uproblematisk, da videregivelsen udtrykkeligt henhører under medlemsstaternes nationale ret. Det er derfor ikke nødvendigt at tage hensyn til de særlige krav vedrørende en ændring af formålet i den litra a)-e) anvendte forstand.

Eksempel: En butiksindehaver foretager optagelser ved indgangen. Optagelserne viser en person, der stjæler en tegnebog fra en anden person. Politiet anmoder den dataansvarlige om at udlevere materialet af hensyn til efterforskningen. I så fald kan butiksejeren anvende det retsgrundlag for overførslen, der er omhandlet i artikel 6, stk. 1, litra c) (retlig forpligtelse), sammen med den relevante nationale lovgivning.

59.

Eksempel: Et kamera er installeret i en butik af sikkerhedsmæssige grunde. Butiksejeren mener, at have fundet noget mistænkeligt i sine optagelser og beslutter at sende materialet til politiet (uden tegn på, at der foregår en undersøgelse af nogen art). I så fald skal butiksejeren vurdere, om betingelserne – som regel i artikel 6, stk. 1, litra f) – er opfyldt. Dette vil normalt være tilfældet, hvis butiksejeren har begrundet mistanke om, at der er begået en kriminel handling.

60.

61. De retshåndhævende myndigheders egen behandling af personoplysninger følger ikke GDPR (jf. artikel 2, stk. 2, litra d)), men i stedet retshåndhævelsesdirektivet ((EU) 2016/680).

5 BEHANDLING AF SÆRLIGE KATEGORIER AF OPLYSNINGER

62. Videoovervågningssystemer indsamler sædvanligvis store mængder af personoplysninger, der kan afsløre oplysninger af meget personlig art, også særlige kategorier af oplysninger. Tilsyneladende uvæsentlige oplysninger, der oprindeligt blev indsamlet via video, kan således bruges til at udlede andre oplysninger til opfyldelse af andre formål (f.eks. at kortlægge en persons vaner). Videoovervågning anses imidlertid ikke altid for at være behandling af særlige kategorier af personoplysninger.

63. Eksempel: Videooptagelser, der viser en registreret, der bruger briller eller kørestol, anses ikke i sig selv for at være særlige kategorier af personoplysninger.

64. Hvis videooptagelserne derimod behandles for at udlede særlige kategorier af oplysninger, finder artikel 9 anvendelse.

65. Eksempel: Der kan afledes politiske holdninger af billeder, der f.eks. viser identificerbare registrerede deltage i et arrangement, en strejke osv. Dette falder ind under artikel 9.

Eksempel: Et hospital, der installerer et videokamera for at kunne overvåge en patients helbred, vil blive anset for at behandle særlige kategorier af personoplysninger (artikel 9).

66. Sædvanligvis bør der tages nøje hensyn til princippet om dataminimering, når der installeres et videoovervågningssystem. Selv i tilfælde, hvor artikel 9, stk. 1, ikke finder anvendelse, bør den dataansvarlige derfor altid søge at minimere risikoen for optagelser, der afslører andre følsomme oplysninger (ud over artikel 9), uanset formålet.

67. Eksempel: Videoovervågning, der viser en kirke, falder ikke i sig selv ind under artikel 9. Den dataansvarlige skal imidlertid foretage en særlig omhyggelig vurdering i henhold til artikel 6, stk. 1, litra f), under hensyntagen til oplysningernes karakter og risikoen for at optage andre følsomme oplysninger (ud over artikel 9), når han vurderer den registreredes interesser.

68. Hvis et videoovervågningssystem anvendes til at behandle særlige kategorier af oplysninger, skal den dataansvarlige identificere både en undtagelse for behandling af særlige kategorier af oplysninger i henhold til artikel 9 (dvs. en undtagelse fra den generelle regel om, at man ikke bør behandle særlige kategorier af oplysninger) og et retsgrundlag i henhold til artikel 6.

69. F.eks. kan artikel 9, stk. 2, litra c) ("[...] *behandling er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser* […]") – i teorien eller undtagelsesvis – anvendes, men den dataansvarlige skal begrunde det som absolut nødvendigt for at beskytte en persons vitale interesser, og bevise, at denne registrerede "[...] *fysisk eller juridisk ikke er i stand til at give sit samtykke*." Desuden må den dataansvarlige ikke anvende systemet af nogen anden grund.

70. Det er her vigtigt at bemærke, at ingen af de undtagelser, der er nævnt i artikel 9, kan forventes af kunne anvendes som begrundelse for at behandle særlige kategorier af oplysninger gennem videoovervågning. Mere konkret kan dataansvarlige, der behandler disse oplysninger i forbindelse med videoovervågning, ikke påberåbe sig artikel 9, stk. 2, litra e), som vedrører behandling af personoplysninger, der åbenbart er offentliggjort af den registrerede. Alene at den registrerede

begiver sig inden for kameraets rækkevidde, er ikke ensbetydende med, at han har til hensigt at offentliggøre særlige kategorier af oplysninger vedrørende sig selv.

71. Ydermere kræver behandling af særlige kategorier af oplysninger øget og vedholdende årvågenhed over for visse forpligtelser, f.eks. en høj grad af konsekvensanalyse vedrørende sikkerhed og databeskyttelse, hvor det er nødvendigt.

> Eksempel: En arbejdsgiver må ikke anvende videoovervågningsoptagelser af en demonstration til at identificere strejkende.

72.

5.1 Generelle hensyn ved behandling af biometriske data

73. Anvendelse af biometriske data, navnlig ansigtsgenkendelse, indebærer øget risiko for de registreredes rettigheder. Det er afgørende, at anvendelsen af sådanne teknologier sker under behørig hensyntagen til principperne om lovmedholdelighed, nødvendighed, proportionalitet og dataminimering som fastlagt i GDPR. Skønt anvendelsen af disse teknologier kan blive opfattet som specielt effektivt, skal dataansvarlige først og fremmest vurdere konsekvenserne for grundlæggende rettigheder og frihedsrettigheder og overveje mindre indgribende midler til at opfylde deres legitime formål med behandlingen.

74. For at dataene skal kunne betragtes som biometriske data som defineret i GDPR, skal behandlingen af rådata såsom fysiske, fysiologiske eller adfærdsmæssige karakteristika for en fysisk person indebære en måling af sådanne karakteristika. Da biometriske data er et resultat af sådanne målinger, hedder det i artikel 4, stk. 14, i GDPR, at det er *"[...] personoplysninger, der som følge af specifik teknisk behandling vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika muliggør eller bekræfter en entydig identifikation af vedkommende [...]"*. Videooptagelser af en person kan derimod ikke i sig selv anses for biometriske data i henhold til artikel 9, hvis de ikke er blevet specifikt teknisk behandlet som bidrag til at identificere en person. [16]

75. For at det kan betragtes som behandling af særlige kategorier af personoplysninger (artikel 9), skal biometriske oplysninger behandles "med det formål entydigt at identificere en fysisk person".

76. Sammenfattende skal der på baggrund af artikel 4, stk. 14 og stk. 9, tages hensyn til tre kriterier:

- **Dataenes art:** data vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika
- **Behandlingens midler og metoder**: personoplysninger, "der som følge af specifik teknisk behandling..."
- **Formålet med behandlingen:** dataene skal anvendes til entydig identifikation af en fysisk person.

77. Brug af videoovervågning, herunder funktioner til biometrisk genkendelse, der installeres af private parter til egen brug (f.eks. markedsføring, statistiske formål eller endda sikkerhed), vil i de fleste

[16] Betragtning 51 i GDPR støtter denne analyse med udsagnet om, at " [...] *Behandling af fotografier bør ikke systematisk anses for at være behandling af særlige kategorier af personoplysninger, eftersom de kun vil være omfattet af definitionen af biometriske data, når de behandles ved en specifik teknisk fremgangsmåde, der muliggør entydig identifikation eller autentifikation af en fysisk person. […]*".

tilfælde kræve udtrykkeligt samtykke fra alle registrerede (artikel 9, stk. 2, litra a)), dog kan en anden relevant undtagelse i artikel 9 også finde anvendelse.

> Eksempel: For at forbedre sin service erstatter en privat virksomhed kontrolpunkter til identifikation af passagerer i en lufthavn (bagageindlevering, boarding) med videoovervågningssystemer, der ved hjælp af teknikker til ansigtsgenkendelse verificerer identiteten af de passagerer, der har valgt at samtykke i en sådan procedure. Eftersom behandlingen falder ind under artikel 9, skal passagerer, der i forvejen har givet udtrykkeligt og informeret samtykke, registrere sig ved f.eks. en automatisk terminal for at oprette og registrere deres ansigtsskabelon, som er knyttet til deres boardingpas og identitet. Kontrolpunkterne med ansigtsgenkendelse skal være tydeligt adskilt, f.eks. skal systemet installeres i en portal, således at det ikke optager biometriske skabeloner af dem, der ikke har givet samtykke. Kun passagerer, der tidligere har givet samtykke og er fortsat med registreringen, anvender portalen med det biometriske system.
>
> Eksempel: En dataansvarlig styrer adgangen til sin bygning ved hjælp af en metode til ansigtsgenkendelse. Folk kan kun benytte denne adgangsvej, hvis de på forhånd har givet udtrykkeligt informeret samtykke hertil (jf. artikel 9, stk. 2, litra a)). For at sikre, at systemet ikke indfanger nogen, der ikke tidligere har givet deres samtykke, bør metoden til ansigtsgenkendelse imidlertid udløses af den registrerede selv, f.eks. ved tryk på en knap. For at sikre, at behandlingen er lovlig, skal den dataansvarlige altid tilbyde en alternativ måde at få adgang til bygningen på uden biometrisk behandling, f.eks. badges eller nøgler.

78.

79. I tilfælde som disse, hvor der genereres biometriske skabeloner, skal de dataansvarlige sikre, at når der er opnået et resultat med match eller ingen match, sletter man øjeblikkeligt og sikkert alle de mellemliggende skabeloner, der er oprettet i farten (med den registreredes udtrykkelige informerede samtykke) for at sammenligne dem med dem, den registrerede har oprettet på tilmeldingstidspunktet. De skabeloner, der er oprettet med henblik på tilmeldingen, bør kun opbevares for at opfylde formålet med behandlingen, og bør ikke opbevares eller arkiveres.

80. Når derimod formålet med behandlingen f.eks. er at skelne den ene kategori af personer fra den anden, men ikke at identificere nogen entydigt, falder behandlingen ikke ind under artikel 9.

> Eksempel: En butiksindehaver ønsker at tilpasse sin reklame på grundlag af kunders køns- og aldersbestemte karakteristika, som optages med et videoovervågningssystem. Hvis systemet ikke genererer biometriske skabeloner for entydigt at identificere personer, men i stedet detekterer disse fysiske egenskaber blot for at klassificere personen, falder behandlingen ikke ind under artikel 9 (når blot der ikke behandles andre typer af særlige kategorier af oplysninger).

81.

82. Artikel 9 finder dog anvendelse, hvis den dataansvarlige opbevarer biometriske oplysninger for entydigt at identificere en person (oftest via skabeloner oprettet ved at udlede hovedkarakteristika af rå biometriske data, f.eks. ansigtsmålinger af et billede). Hvis en dataansvarlig (f.eks. med henblik på fortsat skræddersyet reklame) ønsker at detektere en registreret, der vender tilbage til området eller begiver sig ind i et andet område, vil formålet være at identificere en fysisk person entydigt, hvilket vil betyde, at dette fra begyndelsen falder ind under artikel 9. Dette kan være tilfældet, hvis en dataansvarlig opbevarer dannede skabeloner for at foretage mere skræddersyet reklame på reklametavler forskellige steder i butikken. Da systemet anvender fysiske egenskaber til at opdage og

spore bestemte personer, der kommer tilbage inden for kameraets rækkevidde (f.eks. besøgende i et indkøbscenter) og spore dem, vil det udgøre en biometrisk identifikationsmetode, fordi det tilsigter genkendelse gennem specifik teknisk behandling.

> Eksempel: En butiksejer har installeret et system til ansigtsgenkendelse i sin butik for at målrette sin reklame mod enkeltpersoner. Den dataansvarlige skal indhente udtrykkeligt og informeret samtykke fra alle registrerede, inden han anvender dette biometriske system og leverer målrettet reklame. Systemet ville være ulovligt, hvis det optager besøgende eller forbipasserende, som ikke har givet samtykke til oprettelsen af deres biometriske skabelon, selvom skabelonen slettes hurtigst muligt. Disse midlertidige skabeloner udgør faktisk biometriske data, der behandles med henblik på entydigt at identificere en person, som måske ikke ønsker at modtage målrettet reklame.

83.

84. Det Europæiske Databeskyttelsesråd bemærker, at nogle biometriske systemer er installeret i ukontrollerede miljøer[17], hvilket vil sige, at systemet i forbifarten optager ansigterne på alle, der kommer inden for kameraets rækkevidde – også personer, der ikke har givet samtykke til det biometriske udstyr – og dermed opretter biometriske skabeloner. Disse skabeloner sammenlignes med dem, der er oprettet af registrerede, som har givet forudgående samtykke i forbindelse med en tilmeldingsproces (dvs. brugere af biometrisk udstyr), med henblik på, at den dataansvarlige kan fastslå, om de pågældende er en brugere af biometrisk udstyr eller ej. I dette tilfælde er systemet ofte udformet med henblik på at skelne personer, det søger at genkende i en database, fra dem, der ikke er tilmeldt. Da formålet er entydigt at identificere fysiske personer, behøves der stadig en undtagelse i henhold til artikel 9, stk. 2, i GDPR, for alle, der optages af kameraet.

> Eksempel: Et hotel bruger videoovervågning til automatisk at advisere hotelejeren om, at der er ankommet en VIP, når gæstens ansigt genkendes. Disse VIP'er har på forhånd givet udtrykkelig tilladelse til at anvende ansigtsgenkendelse, inden de er blevet registreret i en database, der er oprettet til formålet. Sådanne systemer til behandling af biometriske data ville være ulovlige, hvis ikke alle andre gæster, der overvåges (for at identificere VIP'erne), har givet samtykke til behandlingen i henhold til artikel 9, stk. 2, litra a), i GDPR.
>
> Eksempel: En dataansvarlig installerer et videoovervågningssystem med ansigtsgenkendelse ved indgangen til den koncertsal, som han administrerer. Den dataansvarlige skal oprette klart adskilte indgange: én med et biometrisk system og én uden (hvor man i stedet f.eks. scanner en billet). De indgange, der er udstyret med biometriske anordninger, skal være installeret og tilgængeliggjort på en måde, der forhindrer, at systemet optager biometriske skabeloner af publikumsmedlemmer, der ikke har givet samtykke.

85.

86. Endelig gælder, at når der kræves samtykke i henhold til artikel 9 i GDPR, må den dataansvarlige ikke gøre adgangen til sine tjenester betinget af, at den biometriske behandling accepteres. Med andre ord, og navnlig når den biometriske behandling anvendes til autentificeringsformål, skal den dataansvarlige tilbyde en alternativ løsning, der ikke omfatter biometrisk behandling – uden begrænsninger eller ekstra omkostninger for den registrerede. Denne alternative løsning er også nødvendig for personer,

[17] Det betyder, at det biometriske udstyr er placeret i et område, der er tilgængeligt for offentligheden og er i stand til at dække alle, der passerer forbi, modsat et kontrolleret miljø med biometriske systemer, der kun kan anvendes ved samtykke fra den pågældende.

der ikke opfylder kravene til det biometriske udstyr (registrering eller aflæsning af de biometriske data umulig, handicap vanskeliggør dets anvendelse mv.), og hvis det biometriske udstyr ikke er tilgængelig (f.eks. ved en fejl i anordningen). I de tilfælde skal der anvendes en "alternativ løsning" for at sikre kontinuiteten i den påtænkte tjeneste, som dog begrænses til ekstraordinær anvendelse. I særlige tilfælde kan der foreligge en situation, hvor behandling af biometriske data er den centrale aktivitet i en tjenesteydelseskontrakt, f.eks. hvis et museum arrangerer en udstilling, hvor man demonstrerer anvendelsen af et system til ansigtsgenkendelse. I det tilfælde vil de registrerede ikke kunne afvise behandlingen af biometriske data, hvis de ønsker at besøge udstillingen. Det samtykke, der kræves i henhold til artikel 9, er i så fald stadig gyldigt, hvis kravene i artikel 7 er opfyldt.

5.2 Foreslåede foranstaltninger til minimering af risici ved behandling af biometriske data

87. I overensstemmelse med princippet om dataminimering skal de dataansvarlige sikre, at oplysninger uddraget af et digitalt billede for at oprette en skabelon ikke har for stort et omfang og kun indeholder de oplysninger, der er nødvendige for det angivne formål, og dermed undgå en eventuel viderebehandling. Der bør træffes foranstaltninger for at sikre, at skabeloner ikke kan overføres på tværs af biometriske systemer.

88. Identifikation og autentifikation/verifikation vil sandsynligvis kræve, at skabelonen opbevares til brug ved senere sammenligning. Den dataansvarlige skal overveje det bedst egnede sted til opbevaring af oplysningerne. I et kontrolleret miljø (afgrænsede gange og kontrolsteder) skal skabeloner opbevares på en særlig anordning, der opbevares af brugere og udelukkende kontrolleres af dem selv (på en smartphone eller et id-kort), eller – når det er nødvendigt til særlige formål og i tilstedeværelse af objektive behov – opbevares i en central database i krypteret form med en nøgle/et password, der udelukkende er i hænderne på den pågældende person, for at forhindre uautoriseret adgang til skabelonen eller opbevaringsstedet. Hvis den dataansvarlige ikke kan undgå at få adgang til skabelonerne, skal han tage passende skridt til at garantere sikkerheden af de opbevarede oplysninger. Dette kan bestå i at kryptere skabelonen med en kryptografisk algoritme.

89. Under alle omstændigheder træffer den dataansvarlige alle nødvendige forholdsregler for at bevare tilgængeligheden, integriteten og fortroligheden af de behandlede oplysninger. Med henblik herpå træffer den dataansvarlige navnlig følgende foranstaltninger: at opdele data under transmission og opbevaring, opbevare biometriske skabeloner og rådata eller identitetsdata i særskilte databaser, kryptere biometriske data, navnlig biometriske skabeloner og fastlægge en politik for kryptering og nøglestyring, integrere en organisatorisk og teknisk foranstaltning for at afsløre svig, tilknytte en integritetskode til dataene (f.eks. signatur eller hash) og forhindre enhver ekstern adgang til de biometriske data. Sådanne foranstaltninger må udvikles i takt med de tekniske fremskridt.

90. Desuden bør de dataansvarlige slette rådata (ansigtsbilleder, talesignaler, gangart osv.) og sikre, at denne sletning er effektiv. Er der ikke længere lovligt grundlag for behandlingen, skal rådata slettes. I det omfang de biometriske skabeloner er afledt af sådanne data, kan oprettelsen af databaser anses for at være en lige så stor eller endnu større trussel (eftersom en biometrisk skabelon ikke nødvendigvis er let at læse uden at vide, hvordan den er programmeret, hvorimod rådata kan være byggesten i enhver skabelon). Er den dataansvarlige nødt til at opbevare sådanne data, skal metoder til additiv støj (f.eks. vandmærkning) undersøges, hvilket vil gøre det umuligt at genoprette skabelonen. Den dataansvarlige skal også slette biometriske data og skabeloner i tilfælde af uautoriseret adgang til terminalen for sammenligning og aflæsning eller til opbevaringsserveren, og slette alle data, der ikke er brug for til den videre behandling ved udløb af det biometriske udstyrs levetid.

6 DEN REGISTREREDES RETTIGHEDER

91. På grund af karakteren af databehandlingen ved videoovervågning er det nødvendigt at forklare nogle af de registreredes rettigheder i henhold til GDPR nærmere. Dette kapitel er imidlertid ikke udtømmende – alle rettigheder i henhold til GDPR finder anvendelse ved behandling af personoplysninger fra videoovervågning.

6.1 Ret til indsigt

92. En registreret har ret til at få den dataansvarlige til at bekræfte, om den registreredes personoplysninger behandles eller ej. For videoovervågning betyder dette, at hvis der ikke på nogen måde opbevares eller overføres data, efter at den løbende overvågning har fundet sted, vil den dataansvarlige kun kunne oplyse, at der ikke længere behandles persondata (foruden de almindelige oplysningsforpligtelser i henhold til artikel 13, jf. *afsnit 7 – gennemsigtigheds- og oplysningspligt*). Hvis der imidlertid stadig behandles data på tidspunktet for anmodningen (dvs. ved fortsat at opbevare dataene eller på anden måde), bør den registrerede få indsigt og information i overensstemmelse med artikel 15.

93. I nogle tilfælde kan der dog gælde en række begrænsninger vedrørende retten til indsigt.

- Artikel 15, stk. 4, i GDPR: krænkning af andres rettigheder

94. I betragtning af at ethvert antal registrerede kan optages i samme videosekvens, vil en screening yderligere medføre behandling af personoplysninger for andre registrerede. Ønsker den registrerede at modtage en kopi af materialet (artikel 15, stk. 3), kan dette tænkes at krænke rettigheder og frihedsrettigheder for andre registrerede i materialet. For at forhindre dette bør den dataansvarlige tage hensyn til, at den dataansvarlige på grund af videooptagelsernes indgribende karakter i nogle tilfælde ikke bør udlevere videooptagelser, hvor der kan identificeres andre registrerede. Beskyttelsen af tredjeparters rettigheder bør dog ikke bruges som en undskyldning for at afvise legitime krav om indsigt for enkeltpersoner; den dataansvarlige bør i sådanne tilfælde gennemføre tekniske foranstaltninger til opfyldelse af anmodningen om indsigt (f.eks. billedredigering såsom maskering eller kodning). Dataansvarlige er dog ikke forpligtet til at gennemføre sådanne tekniske foranstaltninger, hvis de på anden måde kan sikre sig at kunne reagere på en anmodning i henhold til artikel 15 inden for den frist, der er fastlagt i artikel 12, stk. 3.

- Artikel 11, stk. 2, i GDPR: Den dataansvarlige kan ikke identificere den registrerede

95. Hvis videooptagelserne ikke er søgbare for personoplysninger (dvs. den dataansvarlige må antages at skulle gennemgå en stor mængde opbevaret materiale for at finde den pågældende registrerede), kan den dataansvarlige være ude af stand til at identificere den registrerede.

96. Af disse grunde bør den registrerede (ud over at identificere sig selv med identifikationsdokument eller personligt) i sin anmodning til den dataansvarlige specificere, hvornår – inden for en rimelig tidsramme i forhold til antallet af registrerede – vedkommende har begivet sig ind i det overvågede område. Den dataansvarlige bør på forhånd underrette den registrerede om, hvilke oplysninger der er nødvendige, for at den dataansvarlige kan efterkomme anmodningen. Kan den dataansvarlige påvise at være ude af stand til at identificere den registrerede, skal den dataansvarlige om muligt underrette den registrerede herom. I en sådan situation bør den dataansvarlige i sit svar til den registrerede oplyse om det nøjagtige overvågede område,

verifikation af kameraer, der er blevet anvendt, osv., således at den registrerede har fuld indsigt i, hvilke personoplysninger om ham/hende der kan være blevet behandlet.

> Eksempel: Hvis en registreret anmoder om en kopi af sine personoplysninger, der er behandlet via videoovervågning ved indgangen til et indkøbscenter med 30 000 daglige besøgende, bør den registrerede angive, hvornår vedkommende er kommet gennem det overvågede område inden for en tidsramme på ca. en time. Hvis den dataansvarlige stadig behandler materialet, bør der udleveres en kopi af videooptagelserne. Hvis der kan identificeres andre registrerede i samme materiale, skal denne del af materialet anonymiseres (f.eks. ved at udviske kopien eller dele heraf), inden der udleveres en kopi til den registrerede, som har indgivet anmodningen.
>
> Eksempel: Hvis den dataansvarlige automatisk sletter alle optagelser inden for f.eks. 2 dage, er den dataansvarlige ikke i stand til at udlevere optagelser til den registrerede efter 2 dage. Hvis den dataansvarlige modtager en anmodning efter de 2 dage, skal den registrerede underrettes herom.

97.

) Artikel 12 i GDPR, overdrevne anmodninger

98. I tilfælde af overdrevne eller åbenbart grundløse anmodninger fra en registreret kan den dataansvarlige enten opkræve et rimeligt gebyr i overensstemmelse med artikel 12, stk. 5, litra a), i GDPR, eller nægte at efterkomme anmodningen (artikel 12, stk. 5, litra b), i GDPR). Den dataansvarlige skal være i stand til at påvise, at anmodningen er åbenbart grundløs eller overdreven.

6.2 Ret til sletning og ret til indsigelse

6.2.1 Ret til sletning (ret til at blive glemt)

99. Hvis den dataansvarlige fortsætter med at behandle personoplysninger ud over løbende overvågning (f.eks. opbevaring), kan den registrerede anmode om, at personoplysningerne slettes i henhold til artikel 17 i GDPR.

100. På anmodning er den dataansvarlige forpligtet til at slette personoplysningerne uden unødig forsinkelse, hvis en af omstændighederne i artikel 17, stk. 1, i GDPR foreligger (og ingen af undtagelserne i artikel 17, stk. 3, i GDPR). Dette gælder således forpligtelsen til at slette personoplysninger, når de ikke længere er nødvendige til det formål, hvortil de oprindeligt blev opbevaret, eller når behandlingen er ulovlig (se også *afsnit 8 – opbevaringsperioder og pligt til sletning*). Afhængigt af behandlingens retsgrundlag bør personoplysninger desuden slettes

- for *samtykke*, hvis samtykket trækkes tilbage (og der ikke er andet retsgrundlag for behandlingen)
- for *legitim interesse*:
    - når den registrerede gør brug af sin ret til at gøre indsigelse (se *afsnit 6.2.2*), og der ikke er tvingende legitime grunde til behandlingen, eller
    - i tilfælde af direkte markedsføring (herunder profilering), når som helst den registrerede gør indsigelse mod behandlingen.

101. Hvis den dataansvarlige har offentliggjort videooptagelserne (f.eks. ved radio- og TV-spredning eller streaming online), skal der tages rimelige skridt til at informere andre dataansvarlige (som nu behandler de pågældende personoplysninger) om anmodningen i henhold til artikel 17, stk. 2, i GDPR.

De rimelige skridt bør omfatte tekniske foranstaltninger under hensyntagen til den tilgængelige teknologi og omkostningerne til at gennemføre dem. Den dataansvarlige bør så vidt muligt – efter at personoplysningerne er slettet – underrette alle, som personoplysningerne tidligere er blevet videregivet til, i overensstemmelse med artikel 19 i GDPR.

102. Ud over den dataansvarliges forpligtelse til at slette personlige data på den registreredes anmodning er den dataansvarlige i henhold til de generelle principper i GDPR forpligtet til at begrænse de personoplysninger, der opbevares (se *afsnit 8*).

103. For videoovervågning er det værd at bemærke, at når f.eks. billedet sløres uden mulighed for efterfølgende gendannelse af de personlige data, som det tidligere indeholdt, betragtes dataene som slettet i overensstemmelse med GDPR.

> Eksempel: En dagligvarebutik har problemer med hærværk, især udvendigt, og anvender derfor videoovervågning uden for indgangen i direkte nærhed af væggene. En forbipasserende anmoder om at få sine personoplysninger slettet fra samme øjeblik. Den dataansvarlige har pligt til at reagere på anmodningen uden unødig forsinkelse og senest inden for en måned. Da de pågældende optagelser ikke længere opfylder det formål, de oprindeligt blev opbevaret til (der har ikke været hærværk siden den registrerede kom forbi), er der på tidspunktet for anmodningen ingen legitim interesse i at opbevare data, som ville have forrang for registreredes interesser. Den dataansvarlige skal slette personoplysningerne.

104.

6.2.2 Indsigelsesret

105. For videoovervågning baseret på *legitim interesse* (artikel 6, stk. 1, litra f), i GDPR) eller på nødvendigheden af at udføre en opgave i *samfundets interesse* (artikel 6, stk. 1, litra e), i GDPR) har den registrerede til enhver tid ret til af grunde vedrørende vedkommendes særlige situation at gøre indsigelse mod behandlingen i henhold til artikel 21 i GDPR. Medmindre den dataansvarlige påviser tvingende legitime grunde, der tilsidesætter den registreredes rettigheder og interesser, skal behandlingen af oplysninger om den person, der har gjort indsigelse, da ophøre. Den dataansvarlige bør være forpligtet til at reagere på anmodninger fra den registrerede uden unødig forsinkelse og senest inden for en måned.

106. I forbindelse med videoovervågning kan denne indsigelse fremsættes, enten når man begiver sig ind i det overvågede område, når man er der, eller efter at man har forladt det. I praksis betyder dette, at medmindre den dataansvarlige har tvingende legitime grunde, er det kun lovligt at overvåge et område, hvor der kan identificeres fysiske personer, hvis enten

    (1) den dataansvarlige er i stand til straks at standse kameraet i at behandle personoplysninger, når der anmodes herom, eller

    (2) adgangen til det overvågede område er så specifikt afgrænset, at den dataansvarlige kan sikre godkendelse fra den registrerede, inden denne begiver sig ind i området, og at det ikke er et område, som den registrerede har adgangsret til som borger.

107. Disse retningslinjer tilsigter ikke at identificere, hvad der anses for at være en *tvingende* legitim interesse (artikel 21 i GDPR).

108. Når videoovervågning anvendes til direkte markedsføring, har den registrerede ret til at gøre indsigelse mod behandlingen på et skønsmæssigt grundlag, da retten til at gøre indsigelse er absolut i denne sammenhæng (artikel 21, stk. 2 og 3, i GDPR).

Eksempel: En virksomhed oplever problemer med brud på sikkerheden ved sin offentlige indgang og anvender videoovervågning grundet legitim interesse i at optage dem, der begiver sig ind ulovligt. En besøgende gør indsigelse mod behandlingen af sine oplysninger gennem videoovervågningssystemet af grunde vedrørende vedkommendes særlige situation. Virksomheden afviser imidlertid i dette tilfælde anmodningen med den forklaring, at de opbevarede optagelser er nødvendige til en igangværende intern undersøgelse, og at virksomheden derfor har tvingende legitime grunde til at fortsætte med at behandle personoplysningerne.

109.

7 GENNEMSIGTIGHEDS- OG OPLYSNINGSPLIGT[18]

110. Det har længe været et fast punkt i den europæiske databeskyttelseslovgivning, at registrerede skal gøres opmærksomme på, at der anvendes videoovervågning. De bør i detaljer oplyses om de steder, der overvåges.[19] Den generelle gennemsigtigheds- og oplysningspligt er fastlagt i artikel 12 og efterfølgende artikler i GDPR . Yderligere oplysninger findes i artikel 29-Gruppens retningslinjer for gennemsigtighed i henhold til forordning 2016/679 (WP260), som er godkendt af Det Europæiske Databeskyttelsesråd den 25. maj 2018. I overensstemmelse med WP260, afsnit 26, er det artikel 13 i GDPR, der finder anvendelse, hvis der indsamles personoplysninger "[...] ved observation af en registreret (f.eks. ved brug af udstyr til automatisk dataregistrering eller dataregistreringssoftware som f.eks. kameraer [...]".

111. På baggrund af den informationsmængde, der skal gives til den registrerede, kan de dataansvarlige følge en lagdelt tilgang, når de vælger at anvende en kombination af metoder til at sikre gennemsigtighed (WP 260-Gruppen, afsnit 35, WP89, afsnit 22) For videoovervågning bør de vigtigste oplysninger vises på selve advarselsskiltet (første lag), mens de supplerende obligatoriske oplysninger kan gives på anden måde (andet lag).

7.1 Information – første lag (advarselsskilt)

112. Den første lag vedrører den primære måde, den dataansvarlige først involverer sig med den registrerede på. Til dette trin kan dataansvarlige anvende et advarselsskilt med de relevante oplysninger. Denne information kan gives i kombination med et standardikon, der giver et meningsfuldt overblik over den planlagte behandling på en klart synlig, letforståelig og letlæselig måde. (artikel 12, stk. 7, i GDPR). Oplysningernes format bør tilpasses det enkelte sted (WP 89, afsnit 22).

7.1.1 Placeringen af advarselsskiltet

113. Oplysningerne bør placeres på en sådan måde (i øjenhøjde), at den registrerede let kan se omstændighederne ved overvågningen, inden han begiver sig ind i det overvågede område. Kameraets position behøver ikke afsløres, når blot der ikke er tvivl om, hvilke områder der overvåges, og overvågningens sammenhæng er præciseret entydigt (WP 89, afsnit 22). Den registrerede skal kunne få indtryk af, hvilket område der dækkes med kamera, for således at kunne undgå at blive overvåget, eller om nødvendigt tilpasse sin adfærd.

7.1.2 Indholdet i det første lag

114. Det første lag af informationen (advarselsskiltet) bør sædvanligvis indeholde de vigtigste oplysninger, f.eks. om formålet med behandlingen, den dataansvarliges identitet, eksistensen af den registreredes rettigheder samt oplysninger om behandlingens vigtigste virkninger.[20] Disse oplysninger kan f.eks. omfatte legitime interesser, der forfølges af den dataansvarlige (eller af en tredjepart), og kontaktoplysninger for den databeskyttelsesansvarlige (hvis relevant). De skal desuden henvise til det mere detaljerede andet lag af informationen, og til, hvor og hvordan man finder det.

---

[18] Der kan gælde særlige krav i den nationale lovgivning.

[19] Jf. WP89, artikel 29-Gruppens udtalelse 4/2004 om behandling af personoplysninger ved hjælp af videoovervågning).

[20] Jf. WP260, afsnit 38.

115. Desuden bør skiltet indeholde eventuel information, der kan tænkes at overraske den registrerede (WP260, afsnit 38). Denne kan f.eks. være overførsler til tredjeparter, navnlig hvis de er uden for EU, og opbevaringsperioden. Er disse oplysninger ikke angivet, bør den registrerede kunne stole på, at der udelukkende er tale om løbende overvågning (uden registrering eller videregivelse af dataene til tredjeparter).

Eksempel (ikke-bindende forslag):

116.

7.2 Andet lag af informationen

117. Det andet lag skal ligeledes gøres tilgængelig på et sted, der er lettilgængeligt for den registrerede, som f.eks. et ark med fuldstændig information på et centralt sted (f.eks. informationsskranken, receptionen eller kassen) eller på en lettilgængelig plakat. Som nævnt skal varselsskiltet med det første lag klart henvise til oplysningerne i det andet lag. Desuden er det bedst, hvis informationen i det første lag henviser til en digital kilde (f.eks. QR-kode eller webadresse) i det andet lag. Informationen bør dog også være lettilgængelig ikke-digitalt. Det bør være muligt at få adgang til informationen i det andet lag uden at begive sig ind i det undersøgte område, især hvis informationen gives digitalt (hvilket f.eks. kan gøres med et link). Andre passende midler kan være et telefonnummer, man kan ringe til. Uanset hvordan informationen gives, skal den imidlertid indeholde alt, hvad der er obligatorisk i henhold til artikel 13 i GDPR.

118. Som supplement til disse muligheder og for at gøre dem mere effektive fremmer Det Europæiske Databeskyttelsesråd anvendelsen af tekniske midler til at give oplysninger til de registrerede. Dette kan f.eks. omfatte geolokaliseringskameraer og oplysninger i kortlægningsapps eller på websteder, der gør det let for fysiske personer dels at identificere og fastlægge videokilderne knyttet til udøvelsen af deres rettigheder, dels at få mere detaljerede oplysninger om behandlingen.

Eksempel: Ejeren af en butik overvåger sin forretning. For at overholde artikel 13 er det tilstrækkeligt på et let synligt sted ved indgangen til butikken at anbringe et advarselsskilt, som indeholder det første lag af information. Butiksejeren skal desuden lægge et informationsblad frem med oplysningerne i det andet lag ved kassen eller et andet centralt, lettilgængeligt sted i butikken.

119.

8 OPBEVARINGSPERIODER OG KRAV OM SLETNING

120. Personoplysninger må ikke opbevares længere end det er nødvendigt til de formål, hvortil personoplysningerne behandles (artikel 5, stk. 1, litra c) og e), i GDPR). I nogle medlemsstater kan der være særlige bestemmelser om opbevaringsperioder for videoovervågning i overensstemmelse med artikel 6, stk. 2, i GDPR.

121. Hvorvidt det er nødvendigt at opbevare personoplysningerne, eller om de ikke bør opbevares, bør kontrolleres inden for en snæver tidsramme. Sædvanligvis er det legitime formål med videoovervågning at beskytte ejendom eller opbevare bevismateriale. Sædvanligvis kan stedfundne skader konstateres inden for en eller to dage. For at fremme overholdelse af databeskyttelsesreglerne er det i den dataansvarliges interesse at træffe organisatoriske forhåndsforanstaltninger (f.eks. om nødvendigt at udpege en repræsentant til at screene og sikre videomateriale). For at tage hensyn til principperne i artikel 5, stk. 1, litra c) og e) i GDPR, (dataminimering og opbevaringsbegrænsning) bør personoplysningerne (f.eks. til detektering af hærværk) i de fleste tilfælde slettes, ideelt automatisk efter få dage. Jo længere opbevaringsperioden er (især, hvis den er over 72 timer), des bedre begrundelse skal der gives for legitimiteten af formålet og nødvendigheden af opbevaring. Hvis den dataansvarlige anvender video til at overvåge sine lokaler og desuden har til hensigt at opbevare oplysningerne, skal den dataansvarlige sikre, at opbevaringen faktisk er nødvendig til formålet. I så fald skal opbevaringsperioden klart defineres og fastsættes for hvert enkelt formål. Det er den dataansvarliges ansvar at fastsætte opbevaringsperioden i overensstemmelse med principperne om nødvendighed og proportionalitet og at påvise, at bestemmelserne i GDPR overholdes.

> Eksempel: Ejeren af en lille butik vil normalt bemærke alt hærværk samme dag som det finder sted. En normal opbevaringsperiode på 24 timer er derfor tilstrækkelig. Lukning i weekender og ferier kan dog begrunde en længere opbevaringsperiode. Konstateres der en skade, kan det også være nødvendigt at opbevare videooptagelserne længere for at kunne anlægge søgsmål mod gerningsmanden.

122.

9 TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER

123. Som anført i artikel 32, stk. 1, i GDPR skal behandling af personoplysninger under videoovervågning ikke kun være juridisk tilladt, men dataansvarlige og databehandlere skal også sørge for tilstrækkelige sikkerhedsforanstaltninger. Gennemførte **organisatoriske og tekniske foranstaltninger** skal stå **i et rimeligt forhold til risiciene for fysiske personers rettigheder og frihedsrettigheder** som følge af hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse eller adgang til videoovervågningsdata. I henhold til artikel 24 og 25 i GDPR skal dataansvarlige gennemføre tekniske og organisatoriske foranstaltninger, også til overholdelse af alle principper om databeskyttelse under behandlingen og for at give mulighed for, at registrerede kan udøve deres rettigheder som defineret i artikel 15-22 i GDPR. Dataansvarlige bør indføre interne rammer og politikker, der sikrer denne gennemførelse, både på tidspunktet for fastlæggelsen af behandlingsmetoderne og på tidspunktet for selve behandlingen, herunder foretage konsekvensanalyser vedrørende databeskyttelse, når der er behov for dem.

9.1 Oversigt over videoovervågningssystemer

124. Et videoovervågningssystem (VSS)[21] består af analogt og digitalt udstyr samt software til at optage billeder af et sted, håndtere billederne og vise dem for en operatør. Dets komponenter kan opdeles i følgende kategorier:

- Videomiljøet: billedoptagelse, sammenkoblinger og billedhåndtering:
  - formålet med billedoptagelse er at generere et billede af den virkelige verden i et format, der kan anvendes af resten af systemet.
  - sammenkoblingerne beskriver al transmission af data inden for videomiljøet, dvs. forbindelser og kommunikationer. Eksempler på forbindelser er kabler, digitale net og trådløse overførsler. Kommunikationer beskriver alle video-, kontrol- og datasignaler, som kan være digitale eller analoge
  - billedhåndtering omfatter analyse, opbevaring og præsentation af billeder og billedsekvenser.
- Ud fra et systemstyringsperspektiv har et VSS følgende logiske funktioner:
  - dataforvaltning og aktivitetsstyring, som omfatter håndtering af operatørkommandoer og systemgenererede aktiviteter (alarmprocedurer, varsling af operatører)
  - grænseflader til andre systemer kan omfatte tilslutning til andre systemer af sikkerhedsmæssig art (adgangskontrol, brandalarm) og anden art (systemer til bygningsstyring, automatisk nummerpladegenkendelse).
- I et VSS omfatter sikkerheden systemsikkerhed og datafortrolighed, -integritet og -tilgængelighed:
  - systemsikkerheden omfatter den fysiske sikkerhed af alle systemkomponenter og kontrol af adgangen til VSS
  - datasikkerheden omfatter forebyggelse af tab eller manipulation af data.

[21] Databeskyttelsesforordningen indeholder ingen definition heraf; en teknisk beskrivelse kan f.eks. findes i DS/EN 62676-1-1:2014: 2014 Videoovervågningssystemer til brug i sikringsinstallationer – Del 1-1: Krav til videosystemer.

125.

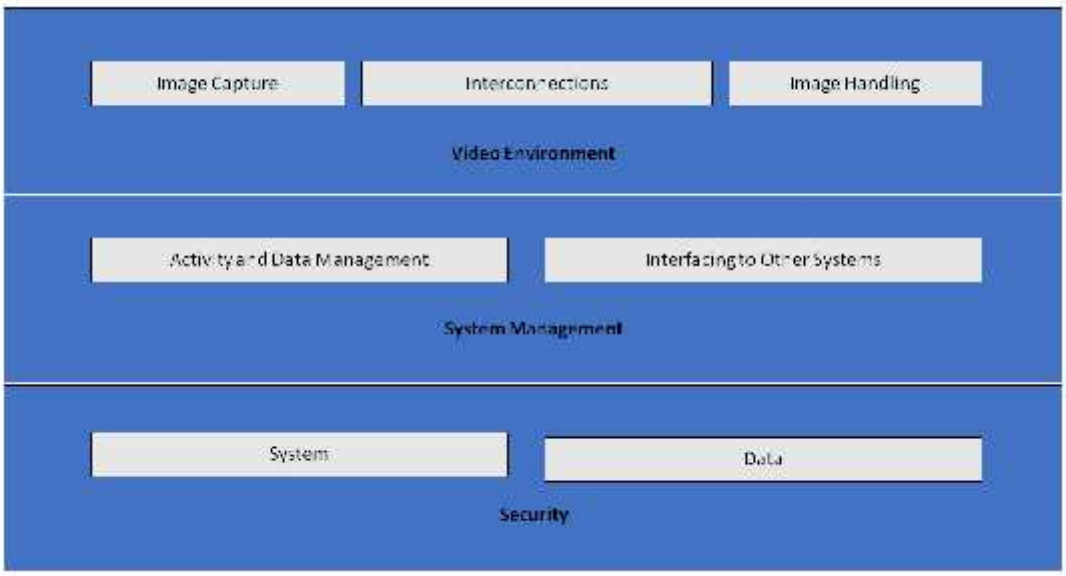

Image Capture	Billedoptagelse
Interconnections	Sammenkoblinger
Image Handling	Billedhåndtering
Video Environment	Videomiljø
Activity and Data Management	Aktivitetsstyring og dataforvaltning
Interfacing to Other Systems	Grænseflade til andre systemer
System Management	Systemstyring
System	System
Data	Data
Security	Sikkerhed

Figur1- videoovervågningssystem

9.2 Databeskyttelse gennem design og gennem standardindstillinger

126. Som anført i artikel 25 i GDPR skal dataansvarlige gennemføre passende tekniske og organisatoriske foranstaltninger til databeskyttelse, så snart de planlægger videoovervågning – inden de begynder at indsamle og behandle videooptagelser. Disse principper understreger behovet for integrerede teknologier til beskyttelse af privatlivets fred, standardindstillinger, der minimerer databehandlingen, og tilvejebringelse af de nødvendige værktøjer, der muliggør maksimal beskyttelse af personoplysninger[22].

127. Dataansvarlige bør integrere databeskyttelse og beskyttelse af privatlivets fred ikke kun i de tekniske specifikationer, men også i organisationens praksis. Med hensyn til organisationens praksis bør den dataansvarlige indføre en passende styringsramme og fastlægge og håndhæve politikker og procedurer for videoovervågning. Fra et teknisk synspunkt bør specifikationen og udformningen af systemet omfatte krav til behandling af personoplysninger i overensstemmelse med principperne i artikel 5 i GDPR (behandlingens lovlighed, formål og databegrænsning, dataminimering gennem

[22] WP 168, udtalelse om "fremtiden for privatlivets fred", fælles bidrag fra artikel 29-gruppen vedrørende databeskyttelse og Gruppen vedrørende Politi og Retsvæsen ved Europa-Kommissionens høring om Europa-Kommissionens høring om retsgrundlaget for den grundlæggende ret til beskyttelse af personoplysninger, (vedtaget 1. december 2009).

standardindstillinger i den i artikel 25, stk. 2, i GDPR anvendte forstand, integritet og fortrolighed, ansvarlighed mv.). Hvis en dataansvarlig påtænker at anskaffe et kommercielt videoovervågningssystem, skal den dataansvarlige medtage disse krav i købsspecifikationen. Den dataansvarlige skal sikre overholdelse af disse krav for alle systemets komponenter og for alle data, der behandles af systemet i hele komponenternes livscyklus.

9.3 Konkrete eksempler på relevante foranstaltninger

128. Størstedelen af de foranstaltninger, der kan anvendes til at skabe sikkerhed ved videoovervågning, særligt ved anvendelse af digitalt udstyr og software, vil ikke adskille sig fra dem, der anvendes i andre IT-systemer. Uanset den valgte løsning skal den dataansvarlige imidlertid beskytte alle videoovervågningssystemets komponenter og data tilstrækkeligt i alle faser, dvs. under opbevaring (data i hvile), overførsel (data i transit) og behandling (data i brug). Hertil er det nødvendigt, at dataansvarlige og databehandlere kombinerer organisatoriske og tekniske foranstaltninger.

129. Ved valg af tekniske løsninger bør den dataansvarlige desuden overveje privatlivsvenlige teknologier, også fordi de øger sikkerheden. Eksempler på sådanne teknologier er systemer, der muliggør maskering eller scrambling af områder, der ikke er relevante for overvågningen, eller bortredigering af billeder af udenforstående ved udlevering af videooptagelser til registrerede.[23] På den anden side bør de valgte løsninger ikke tilvejebringe unødvendige funktioner (f.eks. ubegrænset bevægelsesfrihed for kameraer, zoom-funktion, radiotransmission, analyse og lydoptagelser). Funktioner, der er tilvejebragt, men ikke nødvendige, skal deaktiveres.

130. Der findes megen litteratur om dette emne, herunder internationale standarder og tekniske specifikationer for den fysiske sikkerhed af multimediesystemer[24] og sikkerheden af generelle IT-systemer[25]. Derfor giver dette afsnit kun en overordnet oversigt over emnet.

9.3.1 Organisatoriske foranstaltninger

131. Ud over det potentielle behov for en konsekvensanalyse vedrørende databeskyttelse (se *afsnit 10*) bør dataansvarlige tage følgende punkter i betragtning, når de udarbejder deres egne politikker og procedurer for videoovervågning:

- Hvem er ansvarlig for driften og betjeningen af videoovervågningssystemet.
- Formålet med og omfanget af projektet til videoovervågning.
- Behørig og forbudt anvendelse (hvor og hvornår er videoovervågning tilladt, og hvor og hvornår er det ikke, f.eks. brug af skjulte kameraer og lyd foruden videooptagelse)[26].
- Foranstaltninger til gennemsigtighed som omhandlet i *afsnit 7 (gennemsigtigheds- og oplysningspligt).*
- Hvordan video registreres, og hvor længe, herunder arkivering af videooptagelser i forbindelse med sikkerhedshændelser.
- Hvem skal gennemgå relevant uddannelse, og hvornår.

---

[23] Anvendelse af sådanne teknologier kan endda i visse tilfælde være obligatorisk for at overholde artikel 5, stk. 1, litra c). De kan i hvert fald tjene som eksempler på bedste praksis.

[24] IEC TS 62045 – "Multimedia security– Guideline for privacy protection of equipment and systems in and out of use".

[25] ISO/IEC 27000 – Serien "Information security management systems".

[26] Dette kan afhænge af nationale love og sektorspecifikke forordninger.

- Hvem har adgang til videooptagelser, og til hvilke formål.
- Operationelle procedurer (f.eks. hvem foretager videoovervågning, og hvorfra, og hvad skal man gøre i tilfælde af en hændelse med brud på datasikkerheden).
- Hvilke procedurer skal eksterne parter følge ved anmodning om videooptagelser, og procedurerne for at afvise eller indvillige i at udlevere sådanne optagelser.
- Procedurer for anskaffelse, installation og vedligeholdelse af VSS.
- Procedurer for hændelseshåndtering og genopretning.

9.3.2 Tekniske foranstaltninger

132. **Systemsikkerhed** betyder fysisk sikkerhed for alle systemets komponenter, og systemets integritet, dvs. **beskyttelse og modstandsdygtighed mod forsætlig eller uforsætlig indgriben i dets normale funktioner** og **adgangskontrol**. Datasikkerhed betyder **fortrolighed** (data er kun tilgængelige for adgangsberettigede), **integritet** (forebyggelse af tab og manipulation af data) og **tilgængelighed** (data er tilgængelige, når det er påkrævet).

133. Den **fysiske sikkerhed** er en vigtig del af databeskyttelsen og udgør frontlinjen i beskyttelse af VSS-udstyr mod tyveri, hærværk, naturkatastrofer, menneskeskabte katastrofer og tilfældige skader (f.eks. fra elektrisk overspænding, ekstreme temperaturer og spild af kaffe). For analoge systemer spiller den fysiske sikkerhed den vigtigste rolle i deres beskyttelse.

134. **System- og datasikkerhed**, dvs. beskyttelse mod forsætlig og uforsætlig indgriben i dets normale funktioner, kan bestå i:

- Beskyttelse af hele VSS-infrastrukturen (herunder fjernkameraer, kabler og strømforsyning) mod fysisk manipulation og tyveri.
- Beskyttet overførsel af optagelser ved hjælp af kommunikationskanaler, der er sikret mod aflytning
- Datakryptering.
- Brug af hardware- og softwarebaserede løsninger såsom firewalls, antivirussystemer og Intrusion Detection Systems mod cyberangreb.
- Detektion af svigt af komponenter, software og sammenkoblinger.
- Midler til genoprettelse af tilgængeligheden af og adgangen til systemet i tilfælde af en fysisk eller teknisk hændelse.

135. **Adgangskontrol** sikrer, at kun autoriserede personer kan få adgang til systemet og dataene, mens andre er forhindret i at få det. Foranstaltninger, der støtter fysisk og logisk adgangskontrol, omfatter:

- at sørge for, at alle lokaler, hvor der foretages videoovervågning, og hvor der opbevares videooptagelser, er sikret mod ukontrolleret adgang for tredjeparter.
- at placere overvågningskameraer sådan, at kun autoriserede operatører kan se dem (især når kameraerne er placeret i åbne områder som f.eks. en reception).
- at procedurer for tildeling, ændring og inddragelse af fysisk og logisk adgang er fastlagt og håndhæves.
- at der er gennemført metoder og midler til autentificering og godkendelse af brugere, herunder f.eks. adgangskodernes længde og ændringshyppighed.
- regelmæssig registrering og gennemgang af brugernes handlinger (både hvad angår systemet og dataene).
- løbende overvågning og detektion af adgangssvigt, og afhjælpning af konstaterede svagheder hurtigst muligt.

10 KONSEKVENSANALYSE VEDRØRENDE DATABESKYTTELSE

136. I henhold til artikel 35, stk. 1, i GDPR, skal dataansvarlige foretage konsekvensanalyser vedrørende databeskyttelse (DPIA), når en type databehandling forventes at ville medføre høj risiko for fysiske personers rettigheder og frihedsrettigheder. I henhold til artikel 35, stk. 3, litra c), i GDPR skal dataansvarlige foretage konsekvensanalyse vedrørende databeskyttelse, hvis behandlingen består i systematisk overvågning af et offentligt tilgængeligt område i stor målestok. I henhold til artikel 35, stk. 3, litra b), i GDPR kræves der desuden konsekvensanalyse vedrørende databeskyttelse, når den dataansvarlige har til hensigt at behandle særlige kategorier af oplysninger i stort omfang.

137. "Retningslinjer for konsekvensanalyse vedrørende databeskyttelse"[27] indeholder yderligere rådgivning og mere detaljerede eksempler, der er relevante for videoovervågning (f.eks. vedrørende "anvendelse af et kamerasystem til overvågning af køreadfærd på motorveje"). I henhold til artikel 35, stk. 4, i GDPR skal hver tilsynsmyndighed offentliggøre en liste over behandlingsaktiviteter, der er omfattet af obligatorisk konsekvensanalyse vedrørende databeskyttelse i det pågældende land. Sådanne lister findes sædvanligvis på myndighedens websted. På baggrund af det typiske formål med videoovervågning (beskyttelse af personer og ejendom, opdagelse, forebyggelse og kontrol af lovovertrædelser, indsamling af bevismateriale, og biometrisk identifikation af mistænkte) er det rimeligt at antage, at mange tilfælde af videoovervågning vil kræve en DPIA. Dataansvarlige bør derfor nøje konsultere disse dokumenter for at afgøre, om der er behov for en sådan analyse, og om nødvendigt foretage den. Resultatet af den udførte konsekvensanalyse vedrørende databeskyttelse bør være bestemmende for den dataansvarliges valg af de databeskyttelsesforanstaltninger, der indføres.

138. Det er desuden vigtigt at bemærke, at hvis resultaterne af DPIA viser, at behandlingen vil indebære en høj risiko trods de sikkerhedsforanstaltninger, som den dataansvarlige påtænker, vil det være nødvendigt at høre den pågældende tilsynsmyndighed forud for behandlingen. Nærmere oplysninger om forudgående høring findes i artikel 36.

På vegne af Det Europæiske Databeskyttelsesråd

Formanden

(Andrea Jelinek)

[27] WP248 rev.01, Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og fastlæggelse af, om behandlingen "sandsynligvis vil indebære en høj risiko" i den i forordning (EU) 2016/679 anvendte forstand. – godkendt af Det Europæiske Databeskyttelsesråd