Riktlinjer 3/2019 för behandling av personuppgifter genom videoenheter

Version 2.0

Antagna den 29 januari 2020

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

Versionshistorik

Version 2.1	26 februari 2020	Ändring av materiellt fel
Version 2.0	29 januari 2020	Antagande av riktlinjerna efter offentligt samråd
Version 1.0	10 juli 2019	Antagande av riktlinjerna inför offentligt samråd

Innehållsförteckning

Europeiska dataskyddsstyrelsen har antagit följande riktlinjer

med beaktande av artikel 70.1 e i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (nedan kallad *den allmänna dataskyddsförordningen*),

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37 till detta, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[1] och

med beaktande av artikel 12 och artikel 22 i arbetsordningen.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

1 INLEDNING

1. Den intensiva användningen av videoenheter påverkar medborgarnas beteende. Ett betydande genomförande av dessa verktyg på många av de ytor där enskilda personer rör sig i sina dagliga liv kommer att öka pressen på individerna att förhindra upptäckt av vad som kan uppfattas som avvikelser. Dessa tekniker kan i praktiken begränsa möjligheterna till anonym rörlighet och anonym användning av tjänster och generellt begränsa möjligheten att förbli obemärkt. Dataskyddskonsekvenserna är enorma.

2. Även om enskilda personer kan vara bekväma med videoövervakning i exempelvis ett visst säkerhetssyfte, måste garantier införlivas för att undvika missbruk av personuppgifter för helt olika och – för föremålet för uppgifterna – oväntade ändamål (såsom marknadsföring, övervakning av anställdas prestationer osv.). Dessutom införs nu många verktyg som utnyttjar de bilder som tas, och förvandlar traditionella kameror till smarta kameror. I kombination med dessa verktyg och tekniker innebär mängden data som genereras av videon en ökad risk för sekundär användning (oavsett om den är relaterad till systemets syfte eller inte), eller till och med missbruk. De allmänna principerna i den allmänna dataskyddsförordningen (artikel 5) bör alltid beaktas noggrant vid hantering av videoövervakning.

3. Videoövervakningssystem förändrar på många sätt hur yrkesverksamma från privat och offentlig sektor interagerar på privata eller offentliga platser i syfte att förbättra säkerheten, erhålla publikanalys, leverera personlig reklam osv. Videoövervakning har blivit högpresterande genom att intelligent videoanalys genomförs i allt högre grad. Dessa tekniker kan vara mer inkräktande (såsom komplex biometrisk teknik) eller mindre inkräktande (såsom enkla beräkningsalgoritmer). Att förbli anonym och bevara sin integritet blir generellt allt svårare. De dataskyddsfrågor som tas upp kan variera från en situation till en annan, vilket även den rättsliga analysen gör beroende på vilken teknik som används.

[1] Hänvisningar till ”medlemsstater” som görs i hela detta yttrande ska förstås som hänvisningar till ”EES-medlemsstater”.

4. Förutom integritetsfrågor finns även risker kopplade till att dessa enheter kanske inte fungerar som de ska, och de snedvridningar som de kan orsaka. Forskare rapporterar att programvara som används för identifiering, igenkänning eller analys av ansikten fungerar olika beroende på ålder, kön och etnicitet hos den person som identifieras. Algoritmer som baseras på olika demografiska faktorer kan innebära en snedvridning i fråga om ansiktsigenkänning, vilket riskerar att stärka fördomar i samhället. Därför måste personuppgiftsansvariga också säkerställa att biometrisk behandling av data som härrör från videoövervakning regelbundet bedöms utifrån relevans och att tillräckliga garantier ställs.

5. Utgångspunkten bör inte vara att videoövervakning är en nödvändighet när det finns andra sätt att uppnå det underliggande syftet. Annars riskerar vi en förändring av kulturella normer där avsaknad av integritet blir allmänt accepterat.

6. Dessa riktlinjer syftar till att ge vägledning om hur den allmänna dataskyddsförordningen ska tillämpas vid behandling av personuppgifter via videoenheter. Exemplen är inte uttömmande, men det allmänna resonemanget kan tillämpas på alla potentiella användningsområden.

2 TILLÄMPNINGSOMRÅDE[2]

2.1 Personuppgifter

7. Systematisk automatisk övervakning av vissa utrymmen med optiska eller audiovisuella medel, främst för att skydda egendom eller individers liv och hälsa, har blivit ett viktigt fenomen i våra liv. Denna aktivitet innebär insamling och bevarande av bilder eller audiovisuell information om alla personer som går in i det övervakade utrymmet och som kan identifieras genom sitt utseende eller andra specifika element. Dessa personers identitet kan fastställas med dessa uppgifter. Insamlingen möjliggör även ytterligare behandling av personuppgifter avseende personernas närvaro och beteende på platsen i fråga. Den potentiella risken för missbruk av dessa uppgifter ökar i förhållande till det övervakade utrymmets dimension och antalet personer som rör sig på platsen. Detta faktum återspeglas i den allmänna dataskyddsförordningens artikel 35.3 c, enligt vilken en konsekvensbedömning måste utföras avseende dataskydd vid systematisk övervakning av en allmän plats i stor omfattning, och artikel 37.1 b, enligt vilken personuppgiftsbiträden ska utse ett dataskyddsombud om behandlingen till sin natur innebär regelbunden och systematisk övervakning av registrerade.

8. Förordningen gäller dock inte behandling av uppgifter som saknar hänvisning till en person, t.ex. om en person inte kan identifieras, direkt eller indirekt.

> Exempel: Den allmänna dataskyddsförordningen är inte tillämplig på falska kameror (dvs. alla kameror som inte fungerar som kameror och därmed inte behandlar några personuppgifter). *I vissa medlemsstater kan det dock omfattas av annan lagstiftning.*
>
> Exempel: Inspelningar från hög höjd omfattas endast av den allmänna dataskyddsförordningen om de behandlade uppgifterna under rådande omständigheter kan relateras till en viss person.
>
> Exempel: En videokamera är integrerad i en bil som parkeringshjälp. Om kameran är konstruerad eller justerad på ett sådant sätt att den inte samlar in någon information om fysiska personer (såsom registreringsskyltar eller information som kan identifiera förbipasserande) ska den allmänna dataskyddsförordningen inte tillämpas.

9.

2.2 Tillämpning av direktivet om uppgiftsskydd vid brottsbekämpning (EU 2016/680)

10. Framför allt behandling av personuppgifter som behöriga myndigheter utför i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga hot mot den allmänna säkerheten omfattas av direktiv (EU) 2016/680.

2.3 Undantag för hushåll

11. Enligt artikel 2.2 c omfattas inte behandling av personuppgifter som utförs av en fysisk person som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll, av den allmänna dataskyddsförordningen[3].

[2] Europeiska dataskyddsstyrelsen noterar att om den allmänna dataskyddsförordningen tillåter det kan särskilda krav i nationell lagstiftning gälla.

[3] Se även skäl 18.

12. Denna bestämmelse – det så kallade hushållsundantaget – i samband med videoövervakning måste tolkas snävt. Därmed ska det så kallade hushållsundantaget, så som fastslagits av EU-domstolen, *tolkas så, att det endast avser sådan verksamhet som utgör en del av enskildas privat- eller familjeliv, vilket uppenbart inte är fallet i fråga om sådan behandling av personuppgifter som består i att de offentliggörs på Internet och därmed blir åtkomliga för ett obestämt antal personer*[4]. Dessutom, om ett videoövervakningssystem, i den mån det innebär kontinuerlig registrering och lagring av personuppgifter och *även delvis omfattar ett område dit allmänheten har tillträde och därmed går utanför uppgiftshanterarens privata sfär kan denna verksamhet inte anses vara "av rent privat natur eller som har samband med hans hushåll" i den mening som avses i artikel 3.2 andra strecksatsen i direktiv 95/46*[5].

13. Videoutrustning som används i privatpersoners lokaler kan i vissa fall omfattas av undantaget för hushåll. Detta beror på flera faktorer, som alla måste beaktas för att en slutsats ska kunna dras. Förutom de ovannämnda faktorer som anges i domstolens avgöranden måste användaren av videoövervakning i hemmet beakta om han eller hon har någon form av personlig relation till de registrerade, om övervakningens omfattning eller frekvens har koppling till någon form av yrkesverksamhet från hans eller hennes sida och om övervakningens potentiella negativa inverkan på de registrerade. Förekomsten av någon av de ovannämnda faktorerna betyder inte nödvändigtvis att behandlingen ligger utanför tillämpningsområdet för hushållsundantaget. En övergripande bedömning krävs för att fastställa detta.

> Exempel: En turist spelar in videor både med sin mobiltelefon och med en videokamera för att dokumentera sin semester. Han visar filmerna för vänner och familj, men gör dem inte tillgängliga för ett obestämt antal personer. Detta faller inom ramen för hushållsundantaget.
>
> Exempel: En downhill-cyklist vill filma med en actionkamera när hon cyklar nedför ett berg. Hon cyklar i ett avlägset område och tänker bara använda inspelningen hemma, för eget nöje. Detta skulle omfattas av undantaget för hushåll även om personuppgifter i viss utsträckning behandlas.
>
> Exempel: Någon övervakar och filmar sin egen trädgård. Egendomen är inhägnad och bara den kameraansvariga själv och hans familj går in i trädgården regelbundet. Detta skulle omfattas av undantaget för hushåll, förutsatt att videoövervakningen inte ens delvis sträcker sig till ett offentligt utrymme eller angränsande egendom.

14.

[4] Domstolens dom av den 6 november 2003 i mål C-101/01, Bodil Lindqvist, punkt 47.

[5] Domstolens dom av den 11 december 2014 i mål C-212/13, František Ryneš mot Úřad pro ochranu osobních údajů, punkt 33.

3 BEHANDLINGENS LAGLIGHET

15. Före användning måste behandlingens syfte specificeras i detalj (artikel 5.1 b). Videoövervakning kan tjäna många syften, t.ex. vara ett stöd för att skydda egendom och andra tillgångar, för enskilda personers liv och fysiska integritet, och för att samla in bevis för civilrättsliga anspråk[6]. Dessa övervakningssyften bör dokumenteras skriftligen (artikel 5.2) och måste specificeras för varje övervakningskamera som används. Kameror som används för samma ändamål av en enda ansvarig kan dokumenteras tillsammans. De registrerade måste dessutom informeras om syftet med behandlingen i enlighet med artikel 13 (*se avsnitt 7, Insyns- och informationsskyldigheter*). Att basera videoövervakning enbart på syftet ”säkerhet” eller ”för din säkerhet” är inte tillräckligt specifikt (artikel 5.1 b). Det strider dessutom mot principen att personuppgifter ska behandlas på ett lagligt, rättvist och öppet sätt i förhållande till den registrerade (se artikel 5.1 a).

16. I princip kan varje rättslig grund enligt artikel 6.1 utgöra en rättslig grund för behandling av videoövervakningsdata. Till exempel gäller artikel 6.1 c när nationell lagstiftning föreskriver en skyldighet att genomföra videoövervakning[7]. I praktiken är dock de bestämmelser som mest sannolikt kommer att användas

- artikel 6.1 f (berättigat intresse),
- artikel 6.1 e (nödvändighet att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning).

I ganska exceptionella fall kan den personuppgiftsansvariga använda artikel 6.1 a (samtycke) som rättslig grund.

3.1 Berättigat intresse, artikel 6.1 f

17. Den rättsliga bedömningen av artikel 6.1 f bör baseras på följande kriterier i enlighet med skäl 47.

3.1.1 Förekomst av berättigade intressen

18. Videoövervakning är laglig om den är nödvändig för att uppnå syftet med ett berättigat intresse för en personuppgiftsansvarig eller tredje part, såvida inte dessa intressen åsidosätts av den registrerades intressen eller grundläggande rättigheter och friheter (artikel 6.1 f). Berättigade intressen som utövas av en personuppgiftsansvarig eller tredje part kan vara juridiska[8], ekonomiska eller icke-materiella intressen[9]. Den personuppgiftsansvariga bör dock beakta att om den registrerade motsätter sig övervakningen i enlighet med artikel 21 kan den personuppgiftsansvariga endast fortsätta med videoövervakningen av den registrerade om det är ett *tvingande* berättigat intresse som åsidosätter den registrerades intressen, rättigheter och friheter eller för att upprätta, utöva eller försvara rättsliga anspråk.

[6] Reglerna för insamling av bevis för civilrättsliga fordringar varierar i medlemsstaterna.

[7] I dessa riktlinjer analyseras eller detaljgranskas inte nationell lagstiftning, som kan skilja sig åt mellan medlemsstaterna.

[8] Domstolens dom av den 4 maj 2017 i mål C-13/16, Rīgas satiksme.

[9] Se WP217, artikel 29-arbetsgruppen.

19. I en verklig och farlig situation kan syftet att skydda egendom mot inbrott, stöld eller vandalism utgöra ett berättigat intresse för videoövervakning.

20. Det berättigade intresset måste vara verkligt och behovet måste vara aktuellt (det får alltså inte vara fiktivt eller spekulativt)[10]. Det måste finnas en koppling till en verklig nödsituation – såsom tidigare skador eller allvarliga incidenter – innan övervakningen påbörjas. Mot bakgrund av principen om ansvarsskyldighet gör personuppgiftsansvariga klokt i att dokumentera relevanta incidenter (med angivelse av datum, typ, ekonomisk förlust) och därmed sammanhängande brottsrubriceringar. Dessa dokumenterade incidenter kan utgöra starka bevis för att det föreligger ett berättigat intresse. Förekomsten av ett berättigat intresse och behovet av övervakning bör omprövas med jämna mellanrum (t.ex. en gång om året beroende på omständigheterna).

> Exempel: En butiksägare vill öppna en ny butik och installera ett videoövervakningssystem för att förhindra vandalism. Han kan genom att presentera statistik visa att det finns starka skäl för att förvänta sig vandalism i området. Erfarenheter från angränsande butiker är också användbara. Den personuppgiftsansvariga i fråga måste inte nödvändigtvis själv ha utsatts för skada så länge situationen i området visar att det föreligger fara eller liknande, vilket kan vara en indikation på ett berättigat intresse. Det räcker dock inte att presentera nationell eller allmän brottsstatistik utan att analysera området i fråga eller farorna för den specifika butiken.

21.

22. Överhängande farliga situationer kan utgöra ett berättigat intresse, vilket är fallet för banker eller butiker som säljer värdefulla varor (t.ex. smycken) eller områden som är kända för att vara typiska brottsplatser för egendomsbrott (t.ex. bensinstationer).

23. I den allmänna dataskyddsförordningen anges också tydligt att offentliga myndigheter inte kan luta sig tillbaka mot ett berättigat intresse när de fullgör sina uppgifter (artikel 6.1 andra meningen).

3.1.2 Behov av behandling

24. Personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (uppgiftsminimering), se artikel 5.1 c. Innan ett videoövervakningssystem installeras bör den personuppgiftsansvariga alltid kritiskt undersöka om denna åtgärd för det första är lämplig för att uppnå det önskade målet, och för det andra om den är lämplig och nödvändig för sina syften. Videoövervakningsåtgärder bör endast väljas om syftet med behandlingen inte rimligen kan uppfyllas på andra sätt som är mindre inkräktande för den registrerades grundläggande rättigheter och friheter.

25. Givet att utgångsläget är att en personuppgiftsansvarig vill förhindra egendomsrelaterade brott skulle man i stället för att installera ett videoövervakningssystem också kunna vidta alternativa säkerhetsåtgärder, såsom att hägna in egendomen, inrätta regelbundna säkerhetspatruller, använda grindvakter, tillhandahålla bättre belysning, installera säkerhetslås, manipuleringssäkra fönster och dörrar eller förse väggar med antigraffiti-beläggning eller skyddande folie. Dessa åtgärder kan vara lika effektiva som videoövervakningssystem mot inbrott, stöld och vandalism. Den personuppgiftsansvariga måste från fall till fall bedöma om sådana åtgärder kan vara en rimlig lösning.

[10] Se WP217, artikel 29-arbetsgruppen, s. 24. Se även domstolens dom i mål C-708/18 s. 44.

26. Innan ett kamerasystem används måste han eller hon bedöma var och när videoövervakningsåtgärder är absolut nödvändiga. Vanligtvis uppfyller ett övervakningssystem som fungerar nattetid samt utanför ordinarie arbetstider behoven av att förhindra eventuella faror för egendomen.

27. I allmänhet upphör behovet av videoövervakning för att skydda den personuppgiftsansvarigas lokaler vid fastighetsgränserna.[11] Det finns dock fall där övervakningen av egendomen inte är tillräcklig för ett effektivt skydd. I vissa enskilda fall kan det vara nödvändigt att utöka videoövervakningen till lokalernas närmaste omgivning. I sådana fall bör den personuppgiftsansvariga överväga fysiska och tekniska metoder, till exempel att blockera eller pixla icke relevanta områden.

> Exempel: En bokhandel vill skydda sina lokaler mot vandalism. Övervakningskamerorna bör som regel endast filma själva lokalerna, eftersom det inte finns något behov av att övervaka närliggande lokaler eller offentliga områden i närheten av bokhandlarlokalerna för detta ändamål.

28.

29. Frågor rörande behandlingens nödvändighet uppstår också när det gäller hur bevis bevaras. I vissa fall kan det vara nödvändigt att använda lösningar med så kallade svarta lådor, där bilderna raderas automatiskt efter en viss lagringsperiod och endast tillgängliggörs vid en incident. I andra situationer är det kanske inte nödvändigt att spela in videomaterialet alls, utan lämpligare att i stället använda realtidsövervakning. Valet mellan lösningar med svarta lådor och realtidsövervakning bör också baseras på det syfte som eftersträvas. Om syftet med videoövervakningen till exempel är att bevara bevis är realtidsalternativet vanligtvis inte lämpligt. Ibland kan övervakning i realtid också vara mer inkräktande än lagring och automatisk borttagning av material efter en begränsad tidsperiod (om någon t.ex. alltid tittar på bildskärmen kan det vara mer inkräktande än om det inte finns någon övervakare och materialet lagras direkt i en svart låda). Principen om uppgiftsminimering måste beaktas i detta sammanhang (artikel 5.1 c). Man bör också fundera över möjligheten för den personuppgiftsansvariga att i stället för videoövervakning använda säkerhetspersonal, som kan reagera och ingripa omedelbart.

3.1.3 Intresseavvägning

30. Om man antar att videoövervakning är nödvändig för att skydda en personuppgiftsansvarigs berättigade intressen, får ett videoövervakningssystem endast tas i drift om den personuppgiftsansvarigas eller en tredje parts berättigade intressen (t.ex. skydd av egendom eller fysisk integritet) inte åsidosätts av den registrerades intressen eller grundläggande rättigheter och friheter. Den personuppgiftsansvariga måste överväga 1) i vilken utsträckning övervakningen påverkar enskilda personers intressen, grundläggande rättigheter och friheter och 2) om detta orsakar kränkningar eller negativa konsekvenser med avseende på den registrerades rättigheter. En avvägning av dessa intressen är obligatorisk. Å ena sidan grundläggande rättigheter och friheter och å andra sidan den personuppgiftsansvarigas berättigade intressen måste utvärderas och vägas noggrant mot varandra.

[11] Detta kan också omfattas av nationell lagstiftning i vissa medlemsstater.

Exempel: Ett privat parkeringsbolag har dokumenterat återkommande problem med stölder i parkerade bilar. Parkeringsplatsen är ett öppet utrymme och kan lätt nås av vem som helst, men är tydligt märkt med skyltar och vägspärrar som omger utrymmet. Parkeringsföretaget har ett berättigat intresse (att förhindra stölder i kundernas bilar) av att övervaka området under den tid på dygnet som problemen äger rum. De registrerade övervakas inom en begränsad tidsram, de befinner sig inte inom området för fritidsändamål och det ligger också i deras eget intresse att stölder förhindras. Intresset hos de registrerade som inte ska övervakas åsidosätts i detta fall av den personuppgiftsansvarigas berättigade intresse.

Exempel: En restaurang bestämmer sig för att installera videokameror på toaletterna för att kontrollera att dessa är rena. I detta fall är det uppenbart att de registrerades rättigheter åsidosätter den personuppgiftsansvarigas intressen, och kamerorna får därför inte installeras.

31.

3.1.3.1 Fatta beslut från fall till fall

32. Eftersom en avvägning av intressen är obligatorisk enligt förordningen måste beslutet fattas från fall till fall (se artikel 6.1 f). Det räcker inte att hänvisa till abstrakta situationer eller jämföra liknande fall med varandra. Den personuppgiftsansvariga måste utvärdera riskerna för intrång i den registrerades rättigheter, och det avgörande kriteriet är intrångets intensitet för den registrerades rättigheter och friheter.

33. Intensiteten kan bland annat definieras utifrån vilken typ av information som samlas in (informationsinnehåll), omfattningen (informationstäthet, rumslig och geografisk omfattning), antalet berörda registrerade, antingen som ett specifikt antal eller som en andel av den berörda befolkningen, situationen i fråga, den registrerades faktiska intressen, alternativa metoder samt uppgifternas art och omfattning.

34. Viktiga balanseringsfaktorer kan vara storleken på det område som övervakas och antalet registrerade som övervakas. Användningen av videoövervakning i avlägsna områden (t.ex. för att övervaka vilda djur eller skydda kritisk infrastruktur som exempelvis en privat radioantenn) måste bedömas annorlunda än videoövervakning på gågator eller köpcentrum.

Exempel: Om en bilkamera är installerad (t.ex. för att samla in bevis i händelse av en olycka) är det viktigt att se till att denna kamera inte konstant spelar in trafiken, och de personer som befinner sig nära vägen. Annars kan intresset av att ha videoinspelningar som bevis om en trafikolycka rent teoretiskt skulle inträffa inte motivera det allvarliga intrånget i de registrerades rättigheter[11].

35.

3.1.3.2 Registrerades rimliga förväntningar

36. Enligt skäl 47 kräver förekomsten av ett berättigat intresse noggrann bedömning. Här måste den registrerades rimliga förväntningar vid tidpunkten och i samband med behandlingen av dess personuppgifter inkluderas. När det gäller systematisk övervakning kan förhållandet mellan den registrerade och den personuppgiftsansvariga variera avsevärt och påverka de rimliga förväntningar som den registrerade kan ha. Tolkningen av begreppet rimliga förväntningar bör inte bara baseras på de subjektiva förväntningarna i fråga. Det avgörande kriteriet måste snarare vara om en objektiv tredje part rimligen kan förvänta sig och dra slutsatsen att den är föremål för övervakning i denna specifika situation.

37. En anställd förväntar sig t.ex. i de flesta fall inte att bli övervakad av sin arbetsgivare på sin arbetsplats[12]. Man förväntar sig heller inte att bli övervakad i sin privata trädgård, i bostadsområden eller i undersöknings- och behandlingsrum. På samma sätt är det inte rimligt att förvänta sig övervakning i sanitära utrymmen eller bastuanläggningar – övervakning av sådana områden är ett kraftigt intrång i de registrerades rättigheter. De registrerades rimliga förväntningar är att ingen videoövervakning sker i dessa områden. Å andra sidan kan en banks kunder förväntas räkna med att övervakas i banken eller vid bankomaten.

38. Registrerade kan också förvänta sig att inte övervakas inom allmänt tillgängliga områden, särskilt om dessa områden vanligtvis används för återhämtning, rekreation och fritidsverksamhet, samt på platser där individer vistas och/eller kommunicerar, såsom sittplatser, bord på restauranger, parker, biografer och fitnessanläggningar. Här kommer den registrerades intressen eller rättigheter och friheter ofta att åsidosätta den personuppgiftsansvarigas berättigade intressen.

> Exempel: På toaletter förväntar sig registrerade att inte övervakas. Videoövervakning för att t.ex. förhindra olyckor står inte i proportion till sitt syfte.

39.

40. Skyltar som informerar de registrerade om videoövervakningen saknar betydelse när det gäller att fastställa vad en registrerad objektivt kan förvänta sig. Detta innebär t.ex. att en butiksägare inte kan räkna med att hans eller hennes kunder *objektivt* har rimliga förväntningar på att övervakas bara för att en skylt vid ingången informerar dem om övervakningen.

3.2 Nödvändigheten av att utföra en arbetsuppgift av allmänt intresse eller som ett led i den personuppgiftsansvarigas myndighetsutövning (artikel 6 e)

41. Personuppgifter kan behandlas genom videoövervakning enligt artikel 6.1 e om det är nödvändigt för genomförandet av en uppgift som utförs i allmänhetens intresse eller i samband med myndighetsutövning[13]. Det kan hända att myndighetsutövning inte tillåter sådan behandling men att andra rättsliga grunder, såsom ”hälsa och säkerhet” för skydd av besökare och anställda, kan ge begränsat utrymme för behandling, samtidigt som hänsyn tas till skyldigheterna enligt den allmänna dataskyddsförordningen och de registrerades rättigheter.

42. Medlemsstaterna får behålla eller införa särskild nationell lagstiftning för videoövervakning för att anpassa tillämpningen av bestämmelserna i den allmänna dataskyddsförordningen genom att fastställa ännu mer specifika krav för behandling, så länge det är förenligt med de principer som fastställs i den allmänna dataskyddsförordningen (t.ex. lagringsbegränsning, proportionalitet).

[12] Se även artikel 29-arbetsgruppen, yttrande 2/2017 om databehandling i arbetet, WP249, antaget den 8 juni 2017.

[13] Grunden för behandlingen ska fastställas i unionslagstiftningen eller i medlemsstaternas lagstiftning och ”ska vara nödvändigt för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning” (artikel 6.3).

3.3 Samtycke, artikel 6.1 a

43. Samtycke måste ges fritt, specifikt, informerat och otvetydigt enligt beskrivningen i riktlinjerna för samtycke[14].

44. När det gäller systematisk övervakning kan den registrerades samtycke endast i undantagsfall tjäna som rättslig grund enligt artikel 7 (se skäl 43). Det ligger i sakens natur att denna teknik övervakar ett okänt antal personer samtidigt. Den personuppgiftsansvariga kan knappast bevisa att den registrerade har gett sitt samtycke innan personuppgifterna behandlas (artikel 7.1). Om den registrerade återkallar sitt samtycke kommer det att vara svårt för den personuppgiftsansvariga att bevisa att personuppgifter inte längre behandlas (artikel 7.3).

> Exempel: Idrottare kan begära övervakning under enskilda övningar för att analysera sin teknik och prestanda. Om en idrottsklubb å andra sidan tar initiativ till att övervaka ett helt team för samma ändamål är samtycket ofta ogiltigt, eftersom de enskilda idrottarna kan känna sig pressade att ge sitt samtycke för att inte negativt påverka sina lagkamrater.

45.

46. Om den personuppgiftsansvariga vill förlita sig på samtycke är det hans eller hennes skyldighet att se till att alla registrerade som kommer in i det videoövervakade området har gett sitt samtycke. Detta samtycke måste uppfylla villkoren i artikel 7. Inträde på ett övervakat område (t.ex. när personer uppmanas att gå genom en särskild korridor eller port för att komma in på ett övervakat område) utgör inte en förklaring eller bekräftande åtgärd för samtycke, såvida det inte uppfyller kriterierna i artiklarna 4 och 7 enligt beskrivningen i riktlinjerna för samtycke[15].

47. Med tanke på maktobalansen mellan arbetsgivare och arbetstagare bör arbetsgivarna i de flesta fall inte förlita sig på samtycke när de behandlar personuppgifter, eftersom det är osannolikt att uppgifterna ges frivilligt. Riktlinjerna för samtycke bör beaktas i detta sammanhang.

48. En medlemsstats nationella lagar eller kollektivavtal, inbegripet ”verksamhetsöverenskommelser”, får föreskriva särskilda bestämmelser om behandling av anställdas personuppgifter i anställningsförhållanden (se artikel 88).

---

[14] Artikel 29-arbetsgruppen (artikel 29.1 i arbetsprogrammet) ”Riktlinjer om samtycke enligt förordning (EU) 2016/679” (WP259 rev. 01) – godkända av Europeiska dataskyddsstyrelsen

[15] Artikel 29-arbetsgruppen ”Riktlinjer för samtycke enligt förordning (EU) 2016/679” (WP259), godkända av Europeiska dataskyddsstyrelsen – som bör beaktas.

4 UTLÄMNANDE AV VIDEOINSPELNINGAR TILL TREDJE PART

49. I princip gäller de allmänna bestämmelserna i den allmänna dataskyddsförordningen för utlämnande av videoinspelningar till tredje part.

4.1 Utlämnande av videoinspelningar till tredje part i allmänhet

50. Utlämnande definieras i artikel 4.2 som överföring (t.ex. individuell kommunikation), spridning (t.ex. offentliggörande online) eller tillhandahållande på annat sätt. Tredje parter definieras i artikel 4.10. När utlämnande görs till tredjeländer eller internationella organisationer gäller även de särskilda bestämmelserna i artikel 44 ff.

51. Varje utlämnande av personuppgifter är en separat typ av behandling av personuppgifter för vilka den personuppgiftsansvariga måste ha en rättslig grund i artikel 6.

> Exempel: En personuppgiftsansvarig som vill ladda upp en inspelning på internet måste luta sig mot en rättslig grund för denna behandling, till exempel genom att erhålla samtycke från den registrerade i enlighet med artikel 6.1 a.

52.

53. Överföring av videoinspelningar till tredje man för andra ändamål än de för vilka uppgifterna samlades in är möjlig enligt bestämmelserna i artikel 6.4.

> Exempel: Videoövervakning av en spärr (på en parkeringsplats) har installerats för att lösa problem med skadegörelse. En skada uppstår och inspelningen överförs till en advokat som ska utreda ärendet. I detta fall är syftet med inspelningen detsamma som syftet med överföringen.
>
> Exempel: Videoövervakning av en spärr (på en parkeringsplats) har installerats för att lösa problem med skadegörelse. Inspelningen publiceras på nätet som underhållning. I detta fall har syftet ändrats och är inte förenligt med det ursprungliga syftet. Det skulle dessutom vara problematiskt att fastställa en rättslig grund för denna behandling (offentliggörande).

54.

55. En tredje part som tar del av filmerna måste göra en egen rättslig analys, i synnerhet identifiera sin rättsliga grund enligt artikel 6 för sin behandling (t.ex. att ta emot materialet).

4.2 Utlämnande av videoinspelningar till brottsbekämpande organ

56. Utlämnandet av videoinspelningar till brottsbekämpande organ är också en oberoende process som kräver en separat motivering för den personuppgiftsansvariga.

57. Enligt artikel 6.1 c är behandling laglig om den är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvariga. Även om tillämpliga polislagar är något som helt och hållet kontrolleras av medlemsstaterna finns det med största sannolikhet allmänna regler som styr överföringen av bevis till brottsbekämpande organ i varje medlemsstat. Behandlingen av den personuppgiftsansvariga som överlämnar uppgifterna regleras i den allmänna dataskyddsförordningen. Om den nationella lagstiftningen kräver att den personuppgiftsansvariga ska samarbeta med brottsbekämpande myndigheter (t.ex. vid en utredning) är den rättsliga grunden för överlämnande av uppgifterna en rättslig skyldighet enligt artikel 6.1 c.

58. Ändamålsbegränsningen i artikel 6.4 är då ofta oproblematisk, eftersom utlämnandet uttryckligen hänför sig till medlemsstaternas lagstiftning. De särskilda kraven för en ändring av syftet i leden a–e behöver därför inte beaktas.

Exempel: En butiksägare gör inspelningar vid ingången till butiken. Filmen visar en person som stjäl en annan persons plånbok. Polisen ber den personuppgiftsansvariga att överlämna materialet för att hjälpa till i utredningen. I detta fall skulle butiksägaren använda den rättsliga grunden enligt artikel 6.1 c (rättslig skyldighet) jämförd med relevant nationell lagstiftning för överföring.

59.

Exempel: En kamera installeras i en butik av säkerhetsskäl. Butiksägaren tror att han har spelat in något misstänkt på sin film och beslutar sig för att skicka materialet till polisen (utan några indikeringar på att det pågår en utredning av något slag). I detta fall måste butiksägaren bedöma om villkoren i artikel 6.1 f, i de flesta fall, är uppfyllda. Detta är vanligtvis fallet om butiksägaren har rimlig misstanke om att ett brott har begåtts.

60.

61. De brottsbekämpande myndigheternas behandling av personuppgifter omfattas inte av den allmänna dataskyddsförordningen (se artikel 2.2 d), utan i stället av direktivet om uppgiftsskydd vid brottsbekämpning (EU 2016/680).

5 BEHANDLING AV SÄRSKILDA KATEGORIER AV UPPGIFTER

62. Videoövervakningssystem samlar vanligtvis in stora mängder personuppgifter som kan avslöja data av mycket personlig karaktär och till och med särskilda kategorier av data. Data som till synes inte är signifikanta och som ursprungligen samlades in via video kan användas för att ta fram information i andra syften (t.ex. för att kartlägga en individs vanor). Videoövervakning anses dock inte alltid behandla särskilda kategorier av personuppgifter.

63. Exempel: Videosekvenser som visar en registrerad person som bär glasögon eller är rullstolsburen betraktas i sig inte som särskilda kategorier av personuppgifter.

64. Om filmen behandlas för att ta fram särskilda kategorier av uppgifter ska dock artikel 9 tillämpas.

65. Exempel: Slutsatser om politiska åsikter skulle till exempel kunna dras från bilder som visar identifierbara registrerade som deltar i ett evenemang eller en strejk osv. Detta skulle omfattas av artikel 9.

Exempel: Om ett sjukhus installerar en videokamera för att övervaka en patients hälsotillstånd skulle detta betraktas som behandling av särskilda kategorier av personuppgifter (artikel 9).

66. I allmänhet bör man, när man installerar ett videoövervakningssystem, noga beakta principen om uppgiftsminimering. Därför bör den personuppgiftsansvariga, även i fall där artikel 9.1 inte är tillämplig, alltid försöka minimera risken för att bilder tas som avslöjar andra känsliga uppgifter (utöver artikel 9), oberoende av syftet.

67. Exempel: Videoövervakning som filmar en kyrka omfattas i sig inte av artikel 9. Den personuppgiftsansvariga måste dock göra en särskilt noggrann bedömning enligt artikel 6.1 f med beaktande av uppgifternas art och risken för att spela in andra känsliga uppgifter (utöver dem i artikel 9) i vid bedömningen av den registrerades intressen.

68. Om ett videoövervakningssystem används för att behandla särskilda uppgiftskategorier måste den personuppgiftsansvariga identifiera både ett undantag för behandling av särskilda kategorier av uppgifter enligt artikel 9 (dvs. ett undantag från den allmänna regeln att man inte bör behandla särskilda kategorier av uppgifter) och en rättslig grund enligt artikel 6.

69. Artikel 9.2 c ([...] *behandling är nödvändig för att skydda den registrerades eller någon annan fysisk persons vitala intressen* [...]) skulle i teorin och undantagsvis kunna användas, men den personuppgiftsansvariga skulle behöva motivera det som en absolut nödvändighet att skydda en persons vitala intressen och bevisa att denna *[…] registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke*. Den personuppgiftsansvariga får heller inte använda systemet av någon annan anledning.

70. Här är det viktigt att notera att varje undantag som förtecknas i artikel 9 sannolikt inte kan användas för att motivera behandling av särskilda kategorier av uppgifter genom videoövervakning. Närmare bestämt kan personuppgiftsansvariga som behandlar dessa uppgifter i samband med videoövervakning inte förlita sig på artikel 9.2 e, enligt vilken behandling är tillåten av personuppgifter som den registrerade uppenbart offentliggör. Att en person går in i kameraområdet innebär inte att denna registrerade avser offentliggöra särskilda kategorier av uppgifter som rör honom eller henne.

71. Dessutom kräver behandling av särskilda kategorier av uppgifter en ökad och fortsatt vaksamhet när det gäller vissa skyldigheter, till exempel en hög nivå av konsekvensbedömning avseende säkerhet och dataskydd där så är nödvändigt.

> Exempel: En arbetsgivare får inte använda videoövervakningsfilmer från en demonstration för att identifiera strejkdeltagare.

72.

5.1 Allmänna överväganden vid behandling av biometriska uppgifter

73. Användningen av biometriska uppgifter och i synnerhet ansiktsigenkänning medför ökade risker för registrerades rättigheter. Det är avgörande att sådan teknik används med vederbörlig respekt för principerna om laglighet, nödvändighet, proportionalitet och uppgiftsminimering i enlighet med den allmänna dataskyddsförordningen. Användningen av denna teknik kan visserligen uppfattas som särskilt effektiv, men personuppgiftsansvariga bör först och främst bedöma inverkan på grundläggande rättigheter och friheter och överväga mindre inkräktande metoder för att uppnå det legitima syftet med behandlingen.

74. För att betraktas som biometriska uppgifter enligt definitionen i den allmänna dataskyddsförordningen måste behandling av rådata, såsom fysiska, fysiologiska eller beteendemässiga egenskaper hos fysiska personer, innebära en mätning av dessa egenskaper. Eftersom biometriska uppgifter är resultatet av sådana mätningar anges i artikel 4.14 i den allmänna dataskyddsförordningen att det är *[...] personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av denna fysiska person [...]*. En videoinspelning av en enskild person kan dock inte i sig betraktas som biometriska uppgifter enligt artikel 9, om den inte har genomgått en särskild teknisk behandling för att bidra till identifieringen av en person[16].

75. För att betraktas som behandling av särskilda kategorier av personuppgifter (artikel 9) krävs det att biometriska uppgifter behandlas ”för att entydigt identifiera en fysisk person”.

76. Sammanfattningsvis måste mot bakgrund av artiklarna 4.14 och 9 följande tre kriterier beaktas:

- **Typ av uppgifter:** Uppgifter om fysiska personers fysiska, fysiologiska eller beteendemässiga egenskaper.
- **Behandlingssätt och behandlingsmetoder:** Uppgifter ”som är en följd av en specifik teknisk behandling”.
- **Syfte med behandlingen:** Uppgifterna ska användas för att unikt identifiera en fysisk person.

77. Användningen av videoövervakning, inklusive biometriska igenkänningsfunktioner som installerats av privata enheter för deras egna ändamål (t.ex. marknadsföring, statistik eller till och med säkerhet) kräver i de flesta fall ett uttryckligt samtycke från alla registrerade (artikel 9.2 a), men ett annat lämpligt undantag i artikel 9 skulle också kunna vara tillämpligt.

[16] I skäl 51 i den allmänna dataskyddsförordningen ges stöd för denna analys, och där anges att *[b]ehandling av foton bör inte systematiskt anses utgöra behandling av särskilda kategorier av personuppgifter, eftersom foton endast definieras som biometriska uppgifter när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person .*

Exempel: För att förbättra sin service ersätter ett privat företag kontrollpunkter för passageraridentifiering på en flygplats (avlämning av bagage, ombordstigning) med videoövervakningssystem som använder ansiktsigenkänningsteknik för att kontrollera identiteten på de passagerare som har valt att godkänna ett sådant förfarande. Eftersom behandlingen omfattas av artikel 9 måste passagerarna, som tidigare har gett sitt uttryckliga och informerade samtycke, registrera sig vid till exempel en automatisk terminal för att skapa och registrera en ansiktsmall kopplad till deras boardingkort och identitet. Kontrollpunkterna för ansiktsigenkänning måste vara tydligt åtskilda och t.ex. installeras i en portal där inga biometriska mallar för personer som inte gett sitt samtycke fångas upp. Endast de passagerare som tidigare gett sitt samtycke och gått vidare med registreringen kommer att använda portalen utrustad med det biometriska systemet.

Exempel: En personuppgiftsansvarig hanterar åtkomsten till sin byggnad med hjälp av en ansiktsigenkänningsmetod. Människor kan endast använda denna åtkomstmetod om de uttryckligen har gett sitt samtycke (i enlighet med artikel 9.2 a) i förväg. För att säkerställa att ingen som inte tidigare har gett sitt samtycke fångas upp bör metoden för ansiktsigenkänning utlösas av den registrerade själv, till exempel genom en knapptryckning. För att säkerställa att behandlingen är laglig måste den personuppgiftsansvariga alltid erbjuda ett alternativt sätt att komma in i byggnaden, utan biometrisk behandling, såsom med brickor eller nycklar.

78.

79. I denna typ av fall, där biometriska mallar genereras, ska personuppgiftsansvariga se till att alla mellanliggande mallar som görs där och då (med den registrerades uttryckliga och informerade samtycke) för att kunna jämföras med dem som de registrerade skapade vid tidpunkten för registreringen, omedelbart och säkert förstörs så fort ett matchnings- eller icke-matchningsresultat erhålls. De mallar som skapas för registreringen ska endast behållas för att förverkliga syftet med behandlingen och inte lagras eller arkiveras.

80. När syftet med behandlingen till exempel är att skilja en kategori av personer från en annan men inte att unikt identifiera någon, omfattas dock inte behandlingen av artikel 9.

Exempel: En butiksägare vill anpassa sin annons baserat på köns- och åldersegenskaper hos kunder som fångats upp av ett videoövervakningssystem. Om detta system inte genererar biometriska mallar för att unikt identifiera personer utan bara läser av dessa fysiska egenskaper för att klassificera personerna, skulle behandlingen inte omfattas av artikel 9 (så länge inga andra typer av särskilda kategorier av uppgifter behandlas).

81.

82. Artikel 9 gäller dock om den personuppgiftsansvariga lagrar biometriska uppgifter (oftast genom mallar som skapas genom extraktion av viktiga egenskaper från den råa formen av biometriska uppgifter (t.ex. ansiktsmätningar från en bild) för att unikt identifiera en person. Om en personuppgiftsansvarig vill läsa av en registrerad person som på nytt går in i området eller går in i ett annat område (till exempel för att prognostisera fortsatt anpassad annonsering) skulle syftet vara att unikt identifiera en fysisk person, vilket innebär att agerandet från början skulle omfattas av artikel 9. Detta kan vara fallet om en personuppgiftsansvarig lagrar genererade mallar för att tillhandahålla ytterligare skräddarsydd annonsering på flera olika platser i butiken. Eftersom systemet använder fysiska egenskaper för att upptäcka specifika individer som kommer tillbaka inom kamerans räckvidd (som besökarna i ett köpcentrum) och för att spåra dem, skulle det utgöra en biometrisk identifieringsmetod eftersom det syftar till att känna igen enskilda personer genom användning av specifik teknisk behandling.

Exempel: En butiksägare har installerat ett ansiktsigenkänningssystem i sin butik för att anpassa sina annonser till enskilda personer. Den personuppgiftsansvariga måste erhålla uttryckligt och informerat samtycke från alla registrerade innan detta biometriska system kan användas och skräddarsydd reklam levereras. Systemet skulle vara olagligt om det fångar upp besökare eller förbipasserande som inte har samtyckt till att deras biometriska mall skapas, även om mallen raderas så snart som möjligt. Dessa tillfälliga mallar utgör biometriska uppgifter som behandlas för att unikt identifiera en person som kanske inte vill få riktad reklam.

83.

84. Europeiska dataskyddsstyrelsen konstaterar att vissa biometriska system installeras i okontrollerade miljöer[17], vilket innebär att dessa system också fångar upp ansikten på personer som passerar genom kamerans område, inklusive personer som inte har gett sitt medgivande till den biometriska utrustningen, och därigenom skapar biometriska mallar. Dessa mallar jämförs med de mallar som har skapats av registrerade som har gett sitt förhandsgodkännande under en registreringsprocess (dvs. användare av biometrisk utrustning) för att den personuppgiftsansvariga ska känna igen om personen är användare av biometrisk utrustning eller inte. I detta fall är systemet ofta utformat för att diskriminera de individer som det vill känna igen från en databas från dem som inte är registrerade. Eftersom syftet är att unikt identifiera fysiska personer behövs fortfarande ett undantag enligt artikel 9.2 i den allmänna dataskyddsförordningen för alla som fångas av kameran.

Exempel: Ett hotell använder videoövervakning för att automatiskt uppmärksamma hotellchefen på att en VIP-gäst har anlänt så fort personens ansikte känns igen. VIP-gästerna gav i förväg sitt uttryckliga samtycke till ansiktsigenkänning innan de registreras i en databas som upprättats för detta ändamål. Dessa system för behandling av biometriska uppgifter skulle vara olagliga om inte alla andra gäster som övervakas (för att identifiera VIP-gästerna) gett sitt samtycke till behandlingen i enlighet med artikel 9.2 a i den allmänna dataskyddsförordningen.

Exempel: En personuppgiftsansvarig installerar ett videoövervakningssystem med ansiktsigenkänning vid ingången till konserthallen som han eller hon ansvarar för. Den personuppgiftsansvariga måste skapa tydligt separerade ingångar; en med ett biometriskt system och en utan (där man i stället t.ex. scannar en biljett). De ingångar som är utrustade med biometriska anordningar ska installeras och göras tillgängliga på ett sätt som hindrar systemet från att göra biometriska mallar av åskådare som inte gett sitt samtycke.

85.

86. Slutligen ska den personuppgiftsansvariga, när samtycke krävs enligt artikel 9 i den allmänna dataskyddsförordningen, inte villkora tillgången till hans eller hennes tjänster med ett godkännande av den biometriska behandlingen. Med andra ord, och i synnerhet när den biometriska behandlingen används för autentiseringsändamål, måste den personuppgiftsansvariga erbjuda en alternativ lösning som inte inbegriper biometrisk behandling – utan begränsningar eller extrakostnader för den registrerade. Denna alternativa lösning behövs också för personer som inte uppfyller kraven för den biometriska anordningen (om registrering eller läsning av de biometriska uppgifterna är omöjlig eller funktionshinder gör den svår att använda osv.) och om den biometriska anordningen inte är tillgänglig (för att den t.ex. är trasig). I dessa fall måste en alternativ lösning genomföras för att säkerställa

[17] Det innebär att den biometriska utrustningen är placerad på en plats som är öppen för allmänheten och kan användas för alla förbipasserande, i motsats till biometriska system i kontrollerade miljöer som endast kan användas med deltagande av personer som gett sitt samtycke.

kontinuiteten i den föreslagna tjänsten, som dock begränsas till exceptionell användning. I undantagsfall kan det finnas situationer där behandling av biometriska uppgifter är kärnverksamheten för en tjänst som tillhandahålls genom avtal, ett museum kan t.ex. ha en utställning där man visar hur ansiktsigenkänningsanordningar används. I dessa fall kan de registrerade inte neka till behandlingen av biometriska uppgifter om de önskar delta i utställningen. Här är det samtycke som krävs enligt artikel 9 fortfarande giltigt om kraven i artikel 7 är uppfyllda.

5.2 Föreslagna åtgärder för att minimera riskerna vid behandling av biometriska uppgifter

87. I enlighet med principen om uppgiftsminimering måste personuppgiftsansvariga säkerställa att data som extraheras från en digital bild för att skapa en mall inte blir alltför omfattande och endast innehåller den information som krävs för det angivna syftet, och därmed undvika eventuell ytterligare behandling. Åtgärder bör vidtas för att garantera att mallar inte kan överföras över biometriska system.

88. För identifiering och autentisering/verifiering kommer sannolikt mallen att behöva lagras för användning i en senare jämförelse. Den personuppgiftsansvariga måste överväga den lämpligaste platsen för lagring av data. I miljöer som kontrolleras (avgränsade korridorer eller kontrollpunkter) ska mallarna lagras i enskilda anordningar som innehas av användarna och som enbart kontrolleras av dem själva (i smarttelefoner eller id-kort) eller – för särskilda ändamål och vid objektiva behov – i en centraliserad databas i krypterad form med en nyckel/ett lösenord som endast den berörda personen har tillgång till för att förhindra obehörig åtkomst till mallen eller lagringsplatsen. Om den personuppgiftsansvariga inte kan undvika att ha tillgång till mallarna måste han eller hon vidta lämpliga åtgärder för att säkerställa säkerheten för de lagrade uppgifterna. Detta kan inbegripa kryptering av mallen med hjälp av en kryptografisk algoritm.

89. Den personuppgiftsansvariga ska under alla omständigheter vidta alla nödvändiga försiktighetsåtgärder för att bevara de behandlade uppgifternas tillgänglighet, integritet och konfidentialitet. I detta syfte ska den personuppgiftsansvariga särskilt vidta följande åtgärder: Dela upp data under överföring och lagring, lagra biometriska mallar och rådata eller identitetsuppgifter i särskilda databaser, kryptera biometriska uppgifter, särskilt biometriska mallar, och fastställa en policy för kryptering och nyckelhantering, införa organisatoriska och tekniska åtgärder för att upptäcka bedrägerier, associera en integritetskod med uppgifterna (t.ex. en signatur eller hashkod) och förbjuda all extern åtkomst till de biometriska uppgifterna. Sådana åtgärder kommer att behöva tas fram i takt med teknikens utveckling.

90. Dessutom bör personuppgiftsansvariga radera rådata (ansiktsbilder, talsignaler, sätt att gå osv.) och säkerställa att denna radering är effektiv. Om det inte längre finns någon laglig grund för behandlingen måste rådatan raderas. I den mån de biometriska mallarna erhållits med hjälp av sådana uppgifter kan upprättandet av databaser anses utgöra ett likvärdigt eller till och med större hot (eftersom det kanske inte alltid är lätt att läsa en biometrisk mall utan kunskap om hur den har programmerats, medan rådata kommer att vara byggstenarna i alla mallar). Om den personuppgiftsansvariga skulle behöva lagra sådana uppgifter måste brustillsatsmetoder (såsom vattenmärkning) undersökas, vilket skulle göra mallen omöjlig att återskapa. Den personuppgiftsansvariga måste också radera biometriska uppgifter och mallar som en säkerhetsåtgärd för eventuell obehörig åtkomst till terminalen för avläsning och jämförelse eller lagringsservern och radera alla data som inte är användbara för vidare behandling i slutet av den biometriska enhetens livslängd.

6 DEN REGISTRERADES RÄTTIGHETER

91. På grund av databehandlingens karaktär vid användning av videoövervakning behöver vissa registrerades rättigheter enligt den allmänna dataskyddsförordningen förtydligas ytterligare. Detta kapitel är dock inte uttömmande, alla rättigheter enligt den allmänna dataskyddsförordningen gäller för behandling av personuppgifter genom videoövervakning.

6.1 Rätten till tillgång

92. En registrerad har rätt att erhålla bekräftelse från den personuppgiftsansvariga om huruvida hans eller hennes personuppgifter behandlas eller inte. När det gäller videoövervakning innebär detta att om inga uppgifter lagras eller överförs på något sätt när realtidsövervakningen har slutat, är den enda information en personuppgiftsansvarig kan ge att inga personuppgifter längre behandlas (utöver de allmänna informationsskyldigheterna enligt artikel 13, se *avsnitt 7 – Insyns- och informationsskyldigheter*). Om uppgifter dock fortfarande behandlas vid tidpunkten för begäran (dvs. om uppgifterna lagras eller behandlas kontinuerligt på något annat sätt) bör den registrerade få tillgång och information i enlighet med artikel 15.

93. Det finns dock ett antal begränsningar som i vissa fall kan gälla rätten till tillgång.

- Artikel 15.4 i den allmänna dataskyddsförordningen, som inverkar negativt på andras rättigheter

94. Med tanke på ovissheten om hur många personer som registreras i en och samma videoövervakningssekvens skulle en säkerhetskontroll leda till ytterligare behandling av andra registrerades personuppgifter. Om den registrerade önskar få en kopia av materialet (artikel 15.3) kan detta inverka negativt på andra registrerades rättigheter och friheter i materialet. För att förhindra detta bör den personuppgiftsansvariga därför beakta att videoinspelningen, på grund av sin inkräktande karaktär, i vissa fall inte bör delas ut när andra registrerade kan identifieras. Skyddet av tredje parts rättigheter bör dock inte användas som en ursäkt för att förhindra enskilda personers legitima krav på tillgång. Den personuppgiftsansvariga bör i dessa fall genomföra tekniska åtgärder för att tillgodose begäran om tillgång (t.ex. bildredigering såsom maskering eller förvrängning). Personuppgiftsansvariga är dock inte skyldiga att genomföra sådana tekniska åtgärder om de på annat sätt kan säkerställa att de kan reagera på en begäran enligt artikel 15 inom den tidsfrist som anges i artikel 12.3.

- Artikel 11.2 i den allmänna dataskyddsförordningen, den personuppgiftsansvariga kan inte identifiera den registrerade

95. Om videoinspelningen inte kan sökas för personuppgifter (dvs. den personuppgiftsansvariga skulle förmodligen behöva gå igenom en stor mängd lagrat material för att hitta den registrerade) kan den personuppgiftsansvariga kanske inte identifiera den registrerade.

96. Av dessa skäl bör den registrerade (förutom att identifiera sig själv, inbegripet med identitetshandling eller personligen) i sin begäran till den personuppgiftsansvariga specificera när han eller hon – inom en rimlig tidsram i förhållande till den registrerade – kom in i det övervakade området. Den personuppgiftsansvariga bör i förväg underrätta den registrerade om vilken information som behövs för att begäran ska kunna uppfyllas. Om den personuppgiftsansvariga kan visa att det inte går att identifiera den registrerade ska han eller hon om möjligt informera den registrerade om detta. I en sådan situation bör den personuppgiftsansvariga i sitt svar till den registrerade informera om det exakta området för övervakning, verifiera vilka kameror som

användes och så vidare, så att den registrerade får full förståelse för vilka av hans/hennes personuppgifter som kan ha behandlats.

> Exempel: Om en registrerad begär en kopia av sina personuppgifter som behandlats genom videoövervakning vid ingången till ett köpcentrum med 30 000 besökare per dag, bör den registrerade ange när han eller hon passerade det övervakade området inom ett tidsspann på ungefär en timme. Om den personuppgiftsansvariga fortfarande behandlar materialet ska en kopia av inspelningen tillhandahållas. Om andra registrerade kan identifieras i samma material bör denna del av materialet anonymiseras (t.ex. genom att kopian eller delar av den görs suddiga) innan det lämnas till den registrerade som begärde en kopia.
>
> Exempel: Om den personuppgiftsansvariga automatiskt raderar alla bilder till exempel inom två dagar, kan han eller hon inte leverera bilder till den registrerade efter dessa två dagar. Om den personuppgiftsansvariga tar emot en begäran efter dessa två dagar bör den registrerade informeras om detta.

97.

- Artikel 12 i den allmänna dataskyddsförordningen, orimliga begäranden

98. Vid orimliga eller uppenbart ogrundade begäranden från en registrerad får den personuppgiftsansvariga antingen ta ut en rimlig avgift i enlighet med artikel 12.5 a i den allmänna dataskyddsförordningen eller vägra att agera på begäran (artikel 12.5 b i den allmänna dataskyddsförordningen). Den personuppgiftsansvariga måste kunna visa att begäran uppenbart är ogrundad eller orimlig.

6.2 Rätt till radering och rätt till invändning

6.2.1 Rätt till radering (rätten att bli bortglömd)

99. Om den personuppgiftsansvariga fortsätter att behandla personuppgifter utöver övervakning i realtid (t.ex. genom lagring) får den registrerade begära att personuppgifterna raderas enligt artikel 17 i den allmänna dataskyddsförordningen.

100. På begäran är den personuppgiftsansvariga skyldig att radera personuppgifterna utan onödigt dröjsmål om någon av de omständigheter som anges i artikel 17.1 i den allmänna dataskyddsförordningen är tillämplig (och inget av de undantag som anges i artikel 17.3 i den allmänna dataskyddsförordningen är det). Detta inbegriper skyldigheten att radera personuppgifter när de inte längre behövs för det ändamål för vilket de ursprungligen lagrades, eller när behandlingen är olaglig (se även *avsnitt 8 – Lagringsperioder och skyldighet att radera*). Dessutom bör personuppgifter, beroende på den rättsliga grunden för behandlingen, raderas

- *för samtycke* varje gång samtycket dras tillbaka (och det inte finns någon annan rättslig grund för behandlingen),
- för *berättigade intressen*
    - varje gång den registrerade utövar rätten att invända (se *avsnitt 6.2.2*) och det inte finns några tvingande och berättigade skäl för behandlingen, eller
    - vid direkt marknadsföring (inklusive profilering) när den registrerade motsätter sig behandlingen.

101. Om den personuppgiftsansvariga har offentliggjort videoinspelningar (t.ex. genom utsändning eller strömning online) måste rimliga åtgärder vidtas för att informera andra personuppgiftsansvariga (som nu behandlar personuppgifterna i fråga) om begäran i enlighet med artikel 17.2 i den allmänna dataskyddsförordningen. De rimliga åtgärderna bör inbegripa tekniska åtgärder, med beaktande av tillgänglig teknik och kostnaderna för genomförandet. I den mån det är möjligt bör den personuppgiftsansvariga i enlighet med artikel 19 i den allmänna dataskyddsförordningen, efter att ha raderat personuppgifterna, underrätta alla som tidigare har fått tillgång till personuppgifterna.

102. Utöver den personuppgiftsansvarigas skyldighet att radera personuppgifter på den registrerades begäran är den personuppgiftsansvariga enligt de allmänna principerna i den allmänna dataskyddsförordningen skyldig att begränsa de personuppgifter som lagras (se *avsnitt 8*).

103. När det gäller videoövervakning är det värt att notera att om t.ex. bilden görs suddig utan möjlighet att retroaktivt återställa de personuppgifter som den tidigare innehöll, anses personuppgifterna vara raderade i enlighet med den allmänna dataskyddsförordningen.

> Exempel: En närbutik har problem med vandalism, särskilt på utsidan, och använder därför videoövervakning utanför ingången i direkt anslutning till väggarna. En förbipasserande begär att få sina personuppgifter raderade från det ögonblick då han eller hon passerade förbi. Den personuppgiftsansvariga är skyldig att besvara begäran utan onödigt dröjsmål och senast inom en månad. Eftersom filmen i fråga inte längre uppfyller det syfte för vilket de ursprungligen lagrades (ingen vandalism inträffade under den tidpunkt då den registrerade passerade), finns det vid tidpunkten för begäran inget berättigat intresse av att lagra de uppgifter som skulle åsidosätta de registrerades intressen. Den personuppgiftsansvariga måste radera personuppgifterna.

104.

6.2.2 Rätten att göra invändningar

105. För videoövervakning baserad på *berättigat intresse* (artikel 6.1 f i den allmänna dataskyddsförordningen) eller för nödvändigheten av att utföra en uppgift i *allmänhetens intresse* (artikel 6.1 e i den allmänna dataskyddsförordningen) har den registrerade alltid rätt att av skäl som hänför sig till hans eller hennes särskilda situation invända mot behandlingen i enlighet med artikel 21 i den allmänna dataskyddsförordningen. Såvida inte den personuppgiftsansvariga uppvisar tvingande legitima skäl som åsidosätter den registrerades rättigheter och intressen, måste behandlingen av uppgifter om den person som har invändningar sedan upphöra. Den personuppgiftsansvariga bör vara skyldig att besvara den registrerades begäranden utan onödigt dröjsmål och senast inom en månad.

106. När det gäller videoövervakning kan denna invändning göras antingen när man beger sig in i, under tiden i eller efter att man har lämnat det övervakade området. I praktiken innebär detta att om inte den personuppgiftsansvariga har tvingande legitima skäl, är övervakningen av ett område där fysiska personer kan identifieras endast laglig om

(1) den personuppgiftsansvariga omedelbart kan stoppa kameran från att behandla personuppgifter när så begärs, eller

(2) det övervakade området är så specifikt avgränsat att den personuppgiftsansvariga kan säkerställa godkännandet från den registrerade innan han eller hon kommer in i det, och det inte är ett område som den registrerade personen i egenskap av medborgare har rätt att vistas inom.

107. Dessa riktlinjer syftar inte till att fastställa vad som anses vara ett *tvingande* berättigat intresse (artikel 21 i den allmänna dataskyddsförordningen).

108. När videoövervakning används i direkt marknadsföringssyfte har den registrerade rätt att invända mot behandlingen efter eget omdöme eftersom rätten till invändningar är absolut i detta sammanhang (artikel 21.2 och 21.3 i den allmänna dataskyddsförordningen).

> Exempel: Ett företag har problem med säkerhetsöverträdelser vid ingången för allmänheten och använder videoövervakning med berättigat intresse som grund, i syfte att fånga dem som tar sig in på området olagligen. En besökare motsätter sig behandlingen av personuppgifter via videoövervakningssystemet av skäl som hänför sig till hans eller hennes särskilda situation. I detta fall avvisar företaget dock begäran med en förklaring om att de lagrade bilderna behövs på grund av en pågående intern utredning, och har därmed tvingande berättigade skäl att fortsätta att behandla personuppgifterna.

109.

7 INSYNS- OCH INFORMATIONSSKYLDIGHETER[18]

110. Det har länge varit fastställt i europeisk dataskyddslagstiftning att registrerade bör vara medvetna om att videoövervakning pågår. De bör informeras på ett detaljerat sätt om de platser som övervakas[19]. I den allmänna dataskyddsförordningen fastställs de allmänna insyns- och informationsskyldigheterna i artikel 12 och följande artiklar. Artikel 29-arbetsgruppens riktlinjer om öppenhet enligt förordning (EU) 2016/679 (WP260), som godkändes av Europeiska dataskyddsstyrelsen den 25 maj 2018, innehåller ytterligare detaljer. I enlighet med WP260 punkt 26 är det artikel 13 i den allmänna dataskyddsförordningen som är tillämplig om personuppgifter samlas in ”[...] från en registrerad genom observation (t.ex. med hjälp av automatiserade dataupptagningsenheter eller programvara för datainsamling såsom kameror [...].”

111. Mot bakgrund av den mängd information som ska tillhandahållas den registrerade kan en stegvis metod följas av personuppgiftsansvariga om de väljer att använda en kombination av metoder för att säkerställa insyn (WP260, punkt 35; WP89, punkt 22). När det gäller videoövervakning bör den viktigaste informationen visas på själva varningsskylten (första nivån), medan ytterligare obligatoriska uppgifter kan tillhandahållas på andra sätt (andra nivån).

7.1 Information på första nivån (varningsskylt)

112. Den första nivån avser det sätt på vilket den personuppgiftsansvariga först och främst samarbetar med den registrerade. I detta skede kan personuppgiftsansvariga använda en varningsskylt som visar relevant information. Den visade informationen får tillhandahållas tillsammans med standardiserade symboler för att ge en överskådlig, begriplig, lättläst och meningsfull överblick över den planerade behandlingen (artikel 12.7 i den allmänna dataskyddsförordningen). Formatet för informationen bör anpassas till platsen i fråga (WP89 punkt 22).

7.1.1 Placering av varningsskylten

113. Informationen bör placeras på ett sådant sätt att den registrerade lätt kan känna igen övervakningsförhållandena innan han eller hon går in i det övervakade området (ungefär på ögonnivå). Kamerans position måste inte avslöjas så länge det inte råder tvivel om vilka områden som övervakas och övervakningssammanhanget klargörs otvetydigt (WP 89, punkt 22). Den registrerade måste kunna uppskatta vilket område som fångas upp av en kamera så att han eller hon vid behov kan undvika övervakning eller anpassa sitt beteende.

7.1.2 Innehållet på första nivån

114. Informationen på den första nivån (varningsskylten) bör i allmänhet förmedla den viktigaste informationen, t.ex. uppgifter om syftet med behandlingen, den personuppgiftsansvarigas identitet och den registrerades rättigheter, tillsammans med information om behandlingens främsta inverkan[20]. Detta kan till exempel omfatta de berättigade intressen som den personuppgiftsansvariga (eller en tredje part) har och kontaktuppgifter för dataskyddsombudet (i förekommande fall). Här måste det också hänvisas till den mer detaljerade informationen på andra nivån och var och hur man hittar den.

---

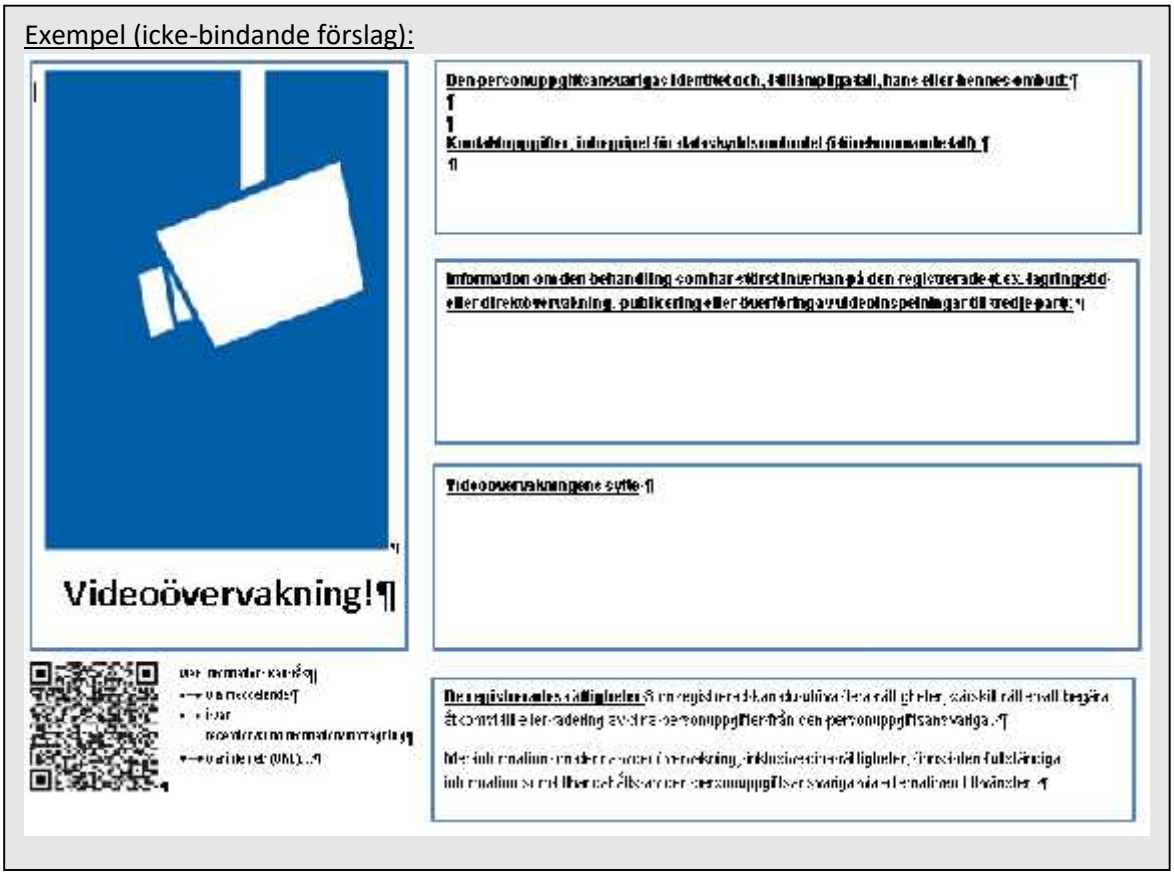
[18] Särskilda krav i nationell lagstiftning kan gälla.

[19] Se WP89, artikel 29-arbetsgruppens yttrande 4/2004 om behandling av personuppgifter genom videoövervakning.

[20] Se punkt 38 i WP260.

115. Dessutom bör skylten innehålla all information som kan vara förvånande för den registrerade (WP260, punkt 38). Detta skulle exempelvis kunna vara information om överföringar till tredje parter, särskilt om de är belägna utanför EU, och om lagringsperioden. Om denna information inte anges bör den registrerade kunna lita på att det endast finns en direktövervakning (utan registrering eller överföring av uppgifter till tredje part).

116. Exempel (icke-bindande förslag):



7.2 Information på andra nivån

117. Informationen på den andra nivån måste också göras åtkomlig på en plats som är lättillgänglig för de registrerade, till exempel i ett komplett informationsblad på en central plats (t.ex. vid informationsdisken, i receptionen eller kassan) eller på en väl synlig affisch. Som nämnts ovan måste varningsskylten på den första nivån tydligt hänvisa till informationen på den andra nivån. Dessutom ska informationen på den första nivån helst hänvisa till en digital källa (t.ex. en QR-kod eller en webbplatsadress) för den andra nivån. Informationen bör dock också finnas lättillgänglig icke-digitalt. Det bör vara möjligt att få tillgång till informationen på den andra nivån utan att gå in i det undersökta området, särskilt om informationen tillhandahålls digitalt (detta kan uppnås exempelvis genom en länk). Andra lämpliga medel kan vara ett telefonnummer som kan ringas. Oavsett hur informationen tillhandahålls måste den innehålla allt som är obligatoriskt enligt artikel 13 i den allmänna dataskyddsförordningen.

118. Utöver dessa alternativ, och även för att göra dem effektivare, främjar Europeiska dataskyddsstyrelsen användningen av tekniska medel för att tillhandahålla information till registrerade. Detta kan t.ex. inbegripa geolokaliseringskameror inklusive information i kartläggningsappar eller webbplatser, så att individer å ena sidan enkelt kan identifiera och tydligt se de videokällor som är relevanta för utövandet av deras rättigheter, och å andra sidan få mer detaljerad information om behandlingen.

Exempel: En butiksägare övervakar sin butik. För att uppfylla kraven i artikel 13 räcker det att placera en varningsskylt vid en lätt synlig punkt vid ingången till butiken, som innehåller information på den första nivån. Dessutom måste han eller hon tillhandahålla ett informationsblad med information på den andra nivån i kassan eller någon annan central och lättillgänglig plats i butiken.

119.

8 LAGRINGSPERIODER OCH SKYLDIGHET ATT RADERA

120. Personuppgifter får inte lagras längre än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas (artikel 5.1 c och e i den allmänna dataskyddsförordningen). I vissa medlemsstater kan det finnas särskilda bestämmelser för lagringsperioder när det gäller videoövervakning i enlighet med artikel 6.2 i den allmänna dataskyddsförordningen.

121. Huruvida personuppgifter måste lagras eller inte bör kontrolleras inom en snäv tidslinje. I allmänhet är legitima syften för videoövervakning ofta egendomsskydd eller bevarande av bevis. Skador som inträffat kan vanligtvis identifieras inom ett eller två dygn. För att göra det lättare att påvisa efterlevnaden av dataskyddsregelverket ligger det i den personuppgiftsansvarigas intresse att vidta organisatoriska åtgärder i förväg (t.ex. vid behov utse en representant för att granska och säkerhetskontrollera videomaterial). Med beaktande av principerna i artikel 5.1 c och e i den allmänna dataskyddsförordningen, nämligen uppgiftsminimering och begränsning av lagring, bör personuppgifterna i de flesta fall (t.ex. för att upptäcka vandalism) raderas, helst automatiskt, efter några dagar. Ju längre lagringsperiod som fastställts (särskilt om den är längre än 72 timmar), desto mer argument krävs för att motivera syftet och behovet av lagring. Om den personuppgiftsansvariga inte bara använder videoövervakning för att övervaka sina lokaler utan även avser att lagra uppgifterna, måste han eller hon säkerställa att lagringen faktiskt är nödvändig för att uppnå syftet. I så fall måste lagringsperioden vara klart definierad och individuellt fastställd för varje enskilt ändamål. Det är den personuppgiftsansvarigas ansvar att fastställa lagringstiden i enlighet med nödvändighets- och proportionalitetsprinciperna och att visa att bestämmelserna i den allmänna dataskyddsförordningen följs.

> Exempel: En ägare av en liten butik skulle normalt upptäcka vandalism samma dag. Följaktligen är en normal lagringsperiod på 24 timmar tillräcklig. Helgdagar eller längre helger kan dock vara skäl som motiverar en längre lagringsperiod. Om en skada upptäcks kan butiksägaren också behöva lagra videoinspelningen under en längre period för att vidta rättsliga åtgärder mot gärningsmannen.

122.

9 TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER

123. Såsom anges i artikel 32.1 i den allmänna dataskyddsförordningen måste behandling av personuppgifter under videoövervakning inte bara vara tillåten enligt lag, utan personuppgiftsansvariga och personuppgiftsbiträden måste också på lämpligt sätt säkra uppgifterna. Genomförda **organisatoriska och tekniska åtgärder** måste **stå i proportion till riskerna för fysiska personers rättigheter och friheter** till följd av oavsiktlig eller olaglig förstörelse, förlust, ändring, otillåten utlämning eller tillgång till videoövervakningsdata. Enligt artiklarna 24 och 25 i den allmänna dataskyddsförordningen måste personuppgiftsansvariga genomföra tekniska och organisatoriska åtgärder även för att skydda alla dataskyddsprinciper under behandlingen och skapa sätt för registrerade att utöva sina rättigheter enligt artiklarna 15–22 i den allmänna dataskyddsförordningen. Personuppgiftsansvariga bör anta interna ramar och strategier som säkerställer detta genomförande både vid tidpunkten för fastställandet av metoderna för behandling och vid tidpunkten för behandlingen i sig, inklusive vid behov utförda konsekvensbedömningar av dataskydd.

9.1 Översikt över videoövervakningssystem

124. Ett videoövervakningssystem[21] består av analog och digital utrustning samt programvara för att ta bilder av en plats, hantera bilderna och visa dem för en operatör. Dess komponenter är grupperade i följande kategorier:

- Videomiljö: Bildtagning, sammankopplingar och bildhantering:
  - Syftet med bildtagning är att skapa en bild av verkligheten i ett format som kan användas av resten av systemet.
  - Sammankopplingar beskriver all överföring av data inom videomiljön, dvs. anslutningar och kommunikation. Exempel på anslutningar är kablar, digitala nätverk och trådlösa överföringar. Kommunikation beskriver alla video- och kontrolldatasignaler, som kan vara digitala eller analoga.
  - Bildhantering inkluderar analys, lagring och presentation av en bild eller en bildsekvens.
- Ur systemhanteringsperspektiv har ett videoövervakningssystem följande logiska funktioner:
  - Datahantering och aktivitetshantering, vilket omfattar hantering av operatörskommandon och systemgenererade aktiviteter (larmförfaranden, varningar till operatörer).
  - Gränssnitt mot andra system kan omfatta anslutning till annan säkerhet (åtkomstkontroll, brandlarm) och andra system (byggnadssystem, automatisk nummerskyltsigenkänning).
- Videoövervakningssystemets säkerhet består av system- och datakonfidentialitet, integritet och tillgänglighet:
  - Systemsäkerhet omfattar fysisk säkerhet för alla systemkomponenter och kontroll av åtkomsten till videoövervakningssystemet.
  - Datasäkerhet omfattar förebyggande av förlust eller manipulering av data.

[21] Den allmänna dataskyddsförordningen ger ingen definition, men en teknisk beskrivning finns till exempel i EN 62676-1-1:2014 *Video surveillance systems for use in security applications – Part 1-1: Video system requirements.*

125.

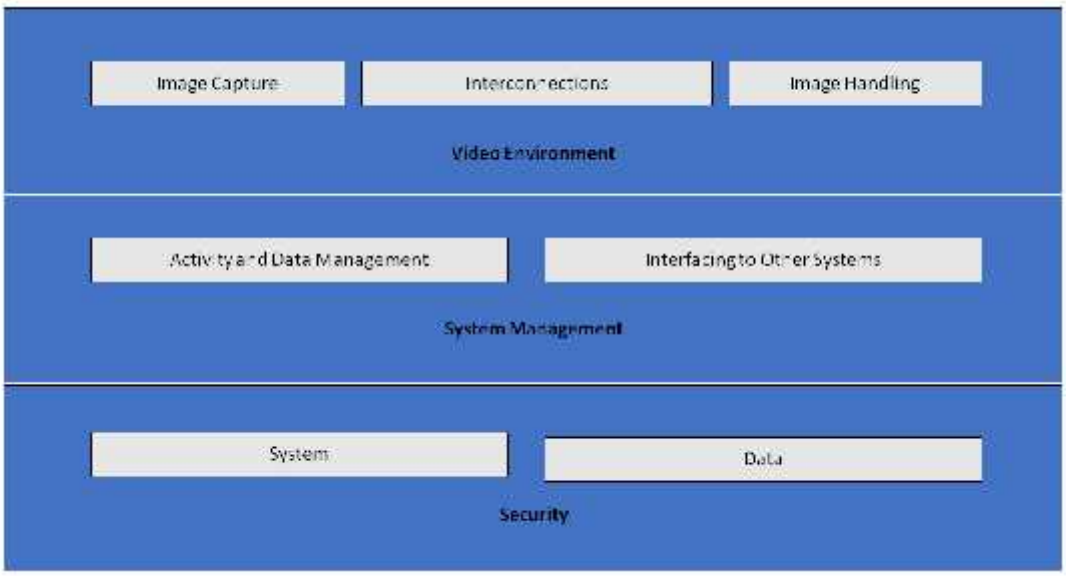


Image Capture	Bildtagning
Interconnections	Sammankoppling
Image Handling	Bildhantering
Video Environment	Videomiljö
Activity and Data Management	Aktivitet och datahantering
Interfacing to Other Systems	Gränssnitt mot andra system
System Management	Systemhantering
System	System
Data	Data
Security	Säkerhet

Figur 1 - Videoövervakningssystem

9.2 Inbyggt dataskydd och dataskydd som standard

126. Såsom anges i artikel 25 i den allmänna dataskyddsförordningen måste personuppgiftsansvariga vidta lämpliga tekniska och organisatoriska åtgärder för uppgiftsskydd så snart de planerar videoövervakning – innan de börjar samla in och behandla videofilmer. I dessa principer betonas behovet av inbyggd integritetsfrämjande teknik, standardinställningar som minimerar databehandlingen och tillhandahållandet av nödvändiga verktyg som möjliggör högsta möjliga skydd av personuppgifter[22].

127. Personuppgiftsansvariga bör bygga upp skyddsåtgärder för data- och integritetsskydd inte bara i teknikens designspecifikationer utan även i organisatoriska rutiner. När det gäller organisatoriska rutiner bör personuppgiftsansvarig anta en lämplig förvaltningsram, upprätta och genomföra policyer och förfaranden för videoövervakningen. Ur teknisk synvinkel bör systemspecifikation och utformning inbegripa krav för behandling av personuppgifter i enlighet med principerna i artikel 5 i den allmänna dataskyddsförordningen (laglighet avseende behandling, syfte och uppgiftsbegränsning, uppgiftsminimering som standard i den mening som avses i artikel 25.2 i den allmänna

[22] WP 168, Yttrande om framtidens integritetsskydd, gemensamt bidrag från artikel 29-arbetsgruppen för dataskydd och arbetsgruppen om polis och rättsväsende till Europeiska kommissionens för samråd om den rättsliga ramen för den grundläggande rätten till skydd av personuppgifter (antaget den 1 december 2009).

dataskyddsförordningen, integritet och konfidentialitet, ansvarsskyldighet osv.). Om en personuppgiftsansvarig planerar att förvärva ett kommersiellt videoövervakningssystem måste han eller hon inkludera dessa krav i inköpsspecifikationen. Den personuppgiftsansvariga måste säkerställa att dessa krav tillämpas på alla komponenter i systemet och på alla data som behandlas av systemet, under komponenternas hela livscykel.

9.3 Konkreta exempel på relevanta åtgärder

128. De flesta åtgärder som kan användas för att säkra videoövervakning, särskilt när digital utrustning och programvara används, skiljer sig inte från dem som används i andra it-system. Oavsett vilken lösning som väljs måste den personuppgiftsansvariga dock på lämpligt sätt skydda alla komponenter i ett videoövervakningssystem och data under alla stadier, dvs. under lagring (data i vila), överföring (data under transport) och behandling (data som används). Därför är det nödvändigt att personuppgiftsansvariga och personuppgiftsbiträden kombinerar organisatoriska och tekniska åtgärder.

129. När tekniska lösningar väljs bör den personuppgiftsansvariga även överväga integritetsvänlig teknik eftersom den förbättrar säkerheten. Exempel på sådan teknik är system som möjliggör maskerings- eller förvrängningsområden som inte är relevanta för övervakningen, eller bortredigering av bilder av tredje personer, när videoinspelningar tillhandahålls registrerade personer[23]. Å andra sidan bör de valda lösningarna inte tillhandahålla funktioner som inte är nödvändiga (t.ex. obegränsad förflyttning av kameror, zoomfunktion, radioöverföring, analys och ljudinspelningar). Funktioner som tillhandahålls men som inte är nödvändiga måste avaktiveras.

130. Det finns mycket litteratur om detta ämne, däribland internationella standarder och tekniska specifikationer för den fysiska säkerheten i multimediasystem[24] och säkerheten i allmänna it-system[25]. Därför ges i det här avsnittet endast en detaljerad översikt om ämnet.

9.3.1 Organisatoriska åtgärder

131. Förutom att en potentiell konsekvensbedömning avseende dataskydd kan komma att behövas (se *avsnitt 10*), bör personuppgiftsansvariga beakta följande punkter när de skapar sina egna riktlinjer och förfaranden för videoövervakning:

- Vem är ansvarig för hantering och drift av videoövervakningssystemet?
- Videoövervakningsprojektets syfte och omfattning.
- Lämplig och förbjuden användning (var och när videoövervakning är tillåten och var och när den inte är tillåten, t.ex. användning av dolda kameror och ljud utöver videoinspelning)[26].
- Insynsåtgärder enligt *avsnitt 7 (Insyns- och informationsskyldigheter).*
- Hur video spelas in och under hur lång tid, inklusive arkivlagring av videoinspelningar med anknytning till säkerhetsincidenter.
- Vem som måste genomgå relevant utbildning och när.

---

[23] Användningen av sådan teknik kan till och med vara obligatorisk i vissa fall för att uppfylla kraven i artikel 5.1 c. I alla händelser kan de tjäna som exempel på bästa praxis.

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

[25] ISO/IEC 27000 – *Information security management systems series.*

[26] Detta kan bero på nationella lagar och sektorsspecifika bestämmelser.

- Vem som har tillgång till videoinspelningar och för vilket ändamål.
- Operativa förfaranden (t.ex. av vem och varifrån videoövervakningen övervakas, vad som ska göras i händelse av ett dataintrång).
- Vilka förfaranden som externa parter måste följa för att begära videoinspelningar och förfaranden för att neka eller bevilja sådana begäranden.
- Förfaranden för upphandling, installation och underhåll av videoövervakningssystemet.
- Förfaranden för hantering och återställning av incidenter.

9.3.2 Tekniska åtgärder

132. **Systemsäkerhet** innebär **fysisk säkerhet** för alla systemkomponenter och systemintegritet, dvs. **skydd mot och motståndskraft vid avsiktliga och oavsiktliga störningar av dess normala drift** och **åtkomstkontroll**. Datasäkerhet innebär **sekretess** (data är endast tillgängliga för dem som beviljas åtkomst), **integritet** (förebyggande av dataförlust eller manipulation) och **tillgänglighet** (data kan nås när det krävs).

133. **Fysisk säkerhet** är en viktig del av dataskyddet och den första försvarslinjen, eftersom den skyddar videoövervakningssystemet från stöld, vandalism, naturkatastrofer, katastrofer orsakade av människor och oavsiktliga skador (t.ex. från plötsliga elektriska tillströmningar, extrema temperaturer och spillt kaffe). När det gäller analoga system spelar den fysiska säkerheten huvudrollen i skyddet.

134. **System- och datasäkerhet**, dvs. skydd mot avsiktlig och oavsiktlig påverkan på den normala driften, kan omfatta följande:

- Skydd av hela infrastrukturen för videoövervakningssystemet (inklusive fjärrkameror, kablar och strömförsörjning) mot fysisk manipulation och stöld.
- Skydd av videoöverföring med kommunikationskanaler som är säkra mot avlyssning.
- Datakryptering.
- Användning av maskin- och programvarubaserade lösningar som brandväggar, antivirus- eller intrångsdetekteringssystem mot it-angrepp.
- Identifiering av fel på komponenter, programvara och sammankopplingar.
- Sätt att återställa tillgänglighet och åtkomst till systemet i händelse av en fysisk eller teknisk incident.

135. **Åtkomstkontroll** säkerställer att endast auktoriserade personer kan komma åt systemet och data, medan andra hindras från att göra det. Åtgärder som stöder fysisk och logisk åtkomstkontroll inkluderar följande:

- Säkerställa att alla lokaler där videoövervakning sker och videoband lagras skyddas mot oövervakad åtkomst av utomstående.
- Placera monitorerna på ett sätt (särskilt när de befinner sig på öppna områden, såsom en mottagning) som gör att endast behöriga operatörer kan se dem.
- Förfaranden för att bevilja, ändra och återkalla fysisk och logisk åtkomst definieras och verkställs.
- Metoder och medel för användarautentisering och auktorisering, inklusive t.ex. lösenordslängd och ändringsfrekvens, genomförs.
- Användarutförda åtgärder (både till systemet och data) registreras och granskas regelbundet.
- Övervakning och upptäckt av åtkomstfel sker kontinuerligt och identifierade brister åtgärdas så snart som möjligt.

10 KONSEKVENSBEDÖMNING AVSEENDE DATASKYDD

136. Enligt artikel 35.1 i den allmänna dataskyddsförordningen är personuppgiftsansvariga skyldiga att genomföra konsekvensbedömningar avseende dataskydd när en typ av databehandling sannolikt kommer att leda till en hög risk för fysiska personers rättigheter och friheter. Enligt artikel 35.3 c i den allmänna dataskyddsförordningen ska personuppgiftsansvariga genomföra konsekvensbedömningar avseende dataskydd om behandlingen utgör en systematisk övervakning av en allmän plats i stor omfattning. Enligt artikel 35.3 b i den allmänna dataskyddsförordningen krävs dessutom en konsekvensbedömning av uppgiftsskyddet när den personuppgiftsansvariga avser att behandla särskilda kategorier av uppgifter i stor omfattning.

137. Riktlinjerna om konsekvensbedömning avseende dataskydd[27] ger ytterligare råd och mer detaljerade exempel som är relevanta för videoövervakning (t.ex. när det gäller ”användning av ett kamerasystem för att övervaka körbeteendet på motorvägar”). Enligt artikel 35.4 i den allmänna dataskyddsförordningen ska varje tillsynsmyndighet offentliggöra en förteckning över behandlingsverksamheter som omfattas av kravet på en konsekvensbedömning avseende dataskydd i deras land. Dessa förteckningar finns vanligtvis på myndigheternas webbplatser. Med tanke på de typiska syftena med videoövervakning (skydd av människor och egendom, upptäckt, förebyggande och kontroll av brott, insamling av bevis och biometrisk identifiering av misstänkta) är det rimligt att anta att många fall av videoövervakning kommer att kräva en konsekvensbedömning avseende dataskydd. Därför bör personuppgiftsansvariga noga studera dessa dokument för att avgöra om en sådan bedömning krävs och utföra den vid behov. Resultatet av den utförda konsekvensbedömningen bör ligga till grund för de dataskyddsåtgärder som den personuppgiftsansvariga väljer att genomföra.

138. Det är också viktigt att notera att om resultaten från konsekvensbedömningen avseende dataskydd visar att behandlingen skulle leda till en hög risk trots de säkerhetsåtgärder som den personuppgiftsansvariga planerar, måste den berörda tillsynsmyndigheten rådfrågas före behandlingen. Närmare uppgifter om tidigare samråd finns i artikel 36.

För Europeiska dataskyddsstyrelsen

Ordföranden

(Andrea Jelinek)

[27] WP248 rev. 01, Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, – godkända av Europeiska dataskyddsstyrelsen