

Dokumentation och policy för trygghetskameror (GDPR)

Innehåll

Innehållsförteckning	1
Syftet med trygghetskameror	2
Allmänt	2
Bakgrund	2
Förklaring och motivering enligt BRÅ	3
Drift lagring och backup	4
Utrustning	4
Backup	4
Access och behörigheter	4
Incident	5
Incidentprocess	5
Personuppgiftsincident	5
GDPR	5
Integritetspolicy	5
Leverantörer	6
Kontaktuppgifter	6

Syftet med trygghetskameror

Allmänt

Syftet med trygghetskameror är i första hand att:

- avskräcka från brott
- bidra till att utreda och bevisa brott eller incidenter
- öka tryggheten

Bakgrund

Alla ska vara förvissade om att incidenter blir dokumenterade så att det inte på något sätt råder någon tvekan om vad som skedde och att det inte blir "ord mot ord" där inget kan bevisas. Placeringen av trygghetskameror kommer endast att ske i publika ytor utan ljudupptagning.

Möjliga incidenter kan vara:

- Obehöriga personer på området
- Hot
- Sexuella trakasserier
- Stölder
- Sabotage av utrustning eller ren vandalism
- Inbrott

Alla allvarliga incidenter polisanmäls men utan bevis står ofta ord mot ord och utredningarna läggs ner i brist på bevis. Årligen kontaktas vi även av Polis som i olika externa utredningar efterfrågar information av oss.

Vi har även mer eller mindre dagligen frågor från kunder som vill försäkra sig om att vi har kameräövervakning något som överlag ses som en trygghet.

Förklaring och motivering enligt BRÅ

Brottsförebyggande åtgärder delas ofta in i två kategorier; sociala och situationella. Sociala åtgärder tar sikte på att förändra individers benägenhet att begå brott medan situationella åtgärder syftar till att förändra förhållanden i tillfället som främjar till brott. Det kan handla om att försvåra genomförandet av brott, öka upptäcktsrisken, minska vinsten av brott eller försvåra bortförklaringar.

I första hand syftar kameraövervakning som brottsförebyggande åtgärd till att avskräcka från brott och ordningsstörningar. Personer som skulle ha begått brott förväntas i större utsträckning än tidigare avstå när det finns kameror på platsen som leder till att den upplevda upptäcktsrisken ökar. En utgångspunkt är då att den potentiella brottslingen handlar rationellt, det vill säga väger fördelar mot nackdelar (vad som kan fås ut av brottet jämfört med att drabbas av de negativa konsekvenserna), inom kriminologin kallat rational choice (exempelvis Clarke, 1992). Detta förutsätter att individen har en viss grad av självkontroll. Upptäcktsrisken, och därmed kameraövervakning, har därför troligen störst betydelse för så kallade frestelsebrott som stöld och rån.

Men även på så kallade friktionsbrott, som hot och våld, kan kameraövervakning ha en förebyggande eller förhindrande effekt. I bland annat sådana situationer kan kameraövervakning vara ett hjälpmedel för att utnyttja resurser inom exempelvis polisen effektivare.

Inspelat material kan även användas för att bidra till att utreda och bevisa brott. Denna möjlighet kan i vissa sammanhang vara betydelsefull för att åtgärden ska fungera avskräckande i ett längre tidsperspektiv. Slutligen kan kameraövervakning också skapa trygghet (upplevd eller faktisk) för allmänheten. En ökad trygghet kan i sin tur leda till att fler människor, och därmed fler vakande ögon, finns på platsen.

Kameraövervakning kan emellertid också få oönskade konsekvenser. En sådan är att övervakningen kan leda till att intrånget i integriteten upplevs alltför stort för människor som vistas på de kameraövervakade platserna, för att eliminera detta informeras genom att varje anläggning är tydligt skyltad.

Drift lagring och backup

Utrustning

Den utrustning och teknik som behövs för införande av trygghetskameror är i dag relativt tekniskt avancerad. Detta har resulterat i att vi har begränsat bl.a. åtkomst, lagringstid mm.

Tanken med kameror, bildöverföring och inspelning är att i första hand verifiera händelser men vissa kameror är även placerade så att identifiering av personer kan ske.

Lagringsenhet

Inspelning sätts igång när rörelse registreras. Övervakning med kameror utomhus sker ej. Överföring av bilder från kamera till inspelningsutrustning sker alltid via kabel. Inspelningsutrustningen är inlåst och enheten själv har en hög säkerhet i form av:

- Lösenordsskydd
- Digest-autentisering
- Användaråtkomstlogg
- Centraliserad certifikathantering

Kameror

Kameror och kommunikation mellan kamera och inspelningsutrustning är även skyddade av:

- Lösenordsskydd
- Nätverksåtkomstkontroll
- Digest-autentisering
- SD-kortkryptering

Backup

Endast ett fåtal nyckelpersoner har access till inspelat material och all personal är bunden av ett sekretessavtal som förhindrar spridning av data/information. Allt inspelat material lagras lokalt på varje gym och sparas i 30 dagar varefter det automatiskt raderas, de första +24 timmarna lagrade på krypterad molnlagring på Europeisk server för de kunder som väljer detta.

Access och behörigheter

Access och behörigheter etc. styrs av Intraguard Kameraövervakning AB:s ansvarige för fysisk säkerhet.

Incident

Om inspelat material mot förmodan skulle komma ut till annan part klassas det som en personuppgiftsincident.

Incidentprocess

Vi kommer omedelbart att bedöma, reagera på och lära sig av incidenter för att minska risken att det sker igen. Beroende på incidentens karaktär och påverkan involveras de personer som krävs för att hantera denna.

Personuppgiftsincident

Rapporteras till Integritetsmyndigheten/Datainspektionen av oss eller av registrerad användare.

GDPR

Behandling av personuppgifter

Vi följer de riktlinjer som omfattas av GDPR.

Integritetpolicy

- Inspelat material nyttjas endast i vad som står under "syfte med kameraövervakning"
- Ingen information kommer att säljas eller överföras till tredjepart
- Ingen information kommer att lagras utanför EU
- Ingen information kommer att användas för ett automatiserat beslutsfattande.

Leverantörer

Vår leverantör för både inspelningsutrustning och kameror är:

Intraguard Kamera Övervakning AB

031 220 230

support@intraguard.se

Kontaktuppgifter

Vid frågor gällande kameraövervakning kontakta:

Intraguard Kamera Övervakning AB

031 220 230

support@intraguard.se

Datainspektionen

Om Vi inte följer upprättade krav och riktlinjer kan överklagan ske till Datainspektionen:

Telefon: 08-657 61 00

email datainspektionen@datainspektionen.se

Fax: 08-652 86 52