Dataskyddsenheten

Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Bostads AB Poseidon

2022-12-27

Innehåll

1 Dataskydd i kommunal verksamhet

Att få ta del av och hantera andra människors personliga uppgifter på ett sådant sätt som kommunala förvaltningar och bolag gör innebär att förvalta ett stort förtroende. Dataskyddsförordningen (GDPR) har tillkommit för att särskilt skydda människors rätt till integritet, och för att värna var och ens rätt att få ha kontroll över vad som sker med uppgifter om ens person. Att förvaltningar och bolag hanterar personuppgifter i enlighet med gällande lag bör vara en självklarhet i syfte att visa omsorg om det förtroende som givits den som har att hantera uppgifterna.

Arbetet med att säkerställa att personuppgifter behandlas enligt reglerna i GDPR behöver genomsyra arbetet inom de kommunala verksamheterna på alla olika plan. Det gäller allt från rutiner och processer för det dagliga arbetet, till arbetet med innovations- och digitaliseringslösningar för framtidens arbetssätt på förvaltningar och bolag inom Göteborgs Stad. I det framåtsyftande arbetet är GDPR ett viktigt redskap för att kunna säkerställa en digitalisering som håller över tid.

1.1 Göteborgs Stads dataskyddsombud

Dataskyddsenheten på Intraservice är Göteborgs Stads dataskyddsombud. Vad som är dataskyddsombudets uppgifter framgår direkt av lagstiftningen i GDPR.[1] Dataskyddsombudets viktigaste uppgift är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. Detta sker bland annat genom att samla in information om hur personuppgifter behandlas och genom att kontrollera hur bestämmelser och interna styrdokument som styr dataskyddsarbetet efterlevs.

Dataskyddsombudet har också till uppgift att ge råd och information till förvaltningar och bolag i dataskyddsfrågor. Detta sker genom att dataskyddsombudet är behjälplig när frågor rörande behandlingen av personuppgifter uppkommer hos verksamheterna. Dataskyddsombudet erbjuder också regelbundet utbildningar för stadens medarbetare. Rådgivning ges även till förvaltningar och bolag när dessa genomför konsekvensbedömningar, vilket är en skyldighet som följer av GDPR. Efter att ha identifierat ett särskilt behov av stöd i arbetet med konsekvensbedömningar, har dataskyddsenheten under 2022 tagit fram mallar och mallstöd för det arbetet.

Det är nämnd/styrelse som har det yttersta ansvaret för att verksamheterna följer dataskyddslagstiftningen och dataskyddsombudet ska enligt lag rapportera om detta till högsta förvaltningsnivå.[2] Dataskyddsombudet har inte mandat att fatta beslut åt verksamheterna. Det är i stället genom råd och rekommendationer som dataskyddsombudet bistår verksamheterna med underlag för att dessa själva ska kunna fatta väl underbyggda beslut.

[1] Artikel 39 i GDPR
[2] Artikel 38.3 i GDPR

2 Granskning av dataskyddsarbetet 2022

2.1 Dataskyddsombudets kontrollfunktion

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras i artikel 39 i GDPR. I Göteborgs Stad innebär en del av denna övervakning att dataskyddsombudet genomför kontroller av dataskyddsarbetet inom den personuppgiftsansvariges organisation.

Enligt dataskyddsregelverket ska dataskyddsombudet arbeta utifrån en riskbaserad metod som utgår från risker för de registrerades fri- och rättigheter. Genom att utgå från en sådan metod minskas risken för negativa konsekvenser även för verksamheten själv. Sådana konsekvenser kan omfatta bland annat skadestånd, sanktionsavgifter, försämrat varumärke eller minskad tillit för verksamheten.

För dataskyddsombudet är kontrollarbetet ett sätt att få en bild av vilka risker och/eller brister som eventuellt föreligger inom en verksamhet. Genom kontroller kan dataskyddsombudet kartlägga verksamhetens dataskyddsarbete, och därigenom hjälpa verksamheten att få en nulägesbild av hur de faktiskt ligger till i sitt dataskyddsarbete. Denna kartläggning kan sedan användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Kontrollarbetets syfte är inte främst att peka ut brister utan ska ses som en vägledning för verksamheten och ett verktyg för att identifiera relevanta prioriteringar. Det är sedan upp till varje verksamhet att besluta om hur det interna dataskyddsarbetet ska utformas utifrån verksamhetens förutsättningar för att på bästa sätt kunna hantera identifierade risker. I det arbetet är dataskyddsombudet behjälplig med rådgivning utifrån verksamhetens behov och de risker som identifierats.

2.2 Fördjupad kontroll

2.2.1 Kontroll av kamerabevakning 2022

Den fördjupade kontrollen har utförts för bolagets kamerabevakning. Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

Dataskyddsombudets övergripande intryck efter kontrollen är att bolaget fortsatt behöver arbeta med att säkerställa att det finns tydliga underlag för respektive kamerabevakning. Flera av de underlag som finns är dock väl utförda och det är tydligt att bolaget arbetar för att förbättra sin kamerahantering. Bolaget förefaller ha goda förutsättningar att slutföra det förbättringsarbete som påbörjats. I rapporten har dataskyddsombudet dock haft några anmärkningar och har därför lämnat rekommendationer till verksamheten för att förbättra sitt arbete och säkerställa följsamhet mot GDPR.

Rekommendationerna avser bland annat behov av att förtydliga sina bedömningar kring tillståndsplikt, tid för bevakningen och rättslig grund. I flera fall finns bedömningar, men inte för samtliga bevakningar. Bolaget bör även bedöma om bevakningarna kräver att konsekvensbedömningar görs utifrån kriterierna i GDPR, i de fall det inte har gjorts, och säkerställa att inspelat material hanteras på ett tillräckligt säkert sätt.

För en av bolagets kamerabevakningar har dataskyddsombudet ifrågasatt behovet av bevakningen, då det av framtagna underlag inte tydliggjorts ett behov. Dataskyddsombudet rekommenderar därför att bolaget säkerställer att den aktuella bevakningen har ett legitimt ändamål, är nödvändig för att uppnå ändamålet och har en rättslig grund.

2.3 Årlig kontroll av dataskyddsarbetet

Verksamhetens interna dataskyddsarbete följs årligen upp genom en enkät. Enkäten består av tolv punkter (”fasta kontrollpunkter”) där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Enkäten är avsedd att spänna över de viktigaste delarna inom dataskyddsarbetet för att på så sätt fånga in en större bredd av frågor. Metoden syftar till att få till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

2.3.1 Metod och risknivåer

I arbetet används en modell som består av fyra kategorier, vilka representerar fyra olika risknivåer. Verksamheten får utifrån sina svar ett värde som visar vilken risknivå verksamheten befinner sig på inom respektive kontrollpunkt. Genom att arbeta med risknivåer möjliggörs ett riskbaserat arbetssätt för både verksamhet och dataskyddsombud, då resultaten ger en bild av vad verksamheten behöver prioritera i dataskyddsarbetet framåt.[3]

Beskrivning av risknivåer

Risknivåer	Färgkod
Nivå 1. Höga risker identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten.	
Nivå 2. Risker identifierade som bedöms vara omfattande och/eller kräver omgående åtgärder.	
Nivå 3. Risker identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.	
Nivå 4. Inga direkta risker av betydelse identifierade. Indikerar att verksamheten har ett systematiskt dataskyddsarbete.	

[3] I arbetet med enkäten har dataskyddsenheten utgått från Myndigheten för samhällsskydd och beredskaps (MSB) uppföljningsstruktur för den offentliga förvaltningens systematiska informationssäkerhetsarbete.

2.4 Poseidons dataskyddsarbete 2022

I detta avsnitt anges vilken risknivå verksamheten befinner sig inom för respektive kontrollpunkt, baserat på verksamhetens svar på de fasta kontrollpunkterna. Under varje kontrollpunkt presenteras även dataskyddsombudets bedömning gällande verksamhetens risker utifrån de iakttagelser som dataskyddsombudet gjort under året.

2.4.1 Kontrollpunkt 1: Dataskyddsorganisation

Kontrollpunkten avser verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete, och omfattar bland annat verksamhetens dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt tillhandahållna resurser för arbetet.

Dataskyddsombudets kommentarer:

Bolagets skattning ligger kvar på samma nivå (4) som föregående år, men med en marginell försämring av medelvärdet. I och med att samtliga påståenden har besvarats med alternativen *Ja, det stämmer bra* eller *Ja, det stämmer helt*, anser bolaget sig ha goda organisatoriska förutsättningar för att kunna bedriva ett effektivt och fungerande dataskyddsarbete. Skattningen indikerar att det inom ramen för kontrollpunkten inte föreligger några risker av betydelse och bolaget arbetar på ett systematiskt vis.

Höga skattningar på denna punkt innebär att det finns tydliga mandat och rapporteringsvägar, att organisationen har de resurser som den behöver, att dataskydd är en naturlig och integrerad del i det dagliga arbetet i alla delar av verksamheten osv. Dataskyddsombudet har inte fått några indikationer som medför en annan bedömning än den som bolaget gör, men har inte heller kontrollerat dataskyddsorganisationen särskilt.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att identifiera och hantera personuppgiftincidenter.

Dataskyddsombudets kommentarer:

Bolagets skattning är något lägre detta år jämfört med föregående och man ligger nu på nivå 3 (dock fortsatt väldigt nära nivå 4). Sammantaget indikerar skattningen att det inom ramen för kontrollpunkten har identifierats risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga.

Enligt skattningen har bolaget i stort ett välfungerande arbete med personuppgiftsincidenter, men behöver arbeta vidare med att ta fram en rutin för när och hur information till de registrerade ska tillhandahållas vid en incident samt säkerställa att samtliga incidenter rapporteras i tid till Integritetsskyddsmyndigheten.

Dataskyddsombudet har ingen anledning att göra en annan bedömning än bolaget kring skattningen. Bolaget har haft nio incidenter under 2022. Åtta av dessa har bedömts vara av sådan karaktär att de inte behövt anmälas till Integritetsskyddsmyndigheten.

En incident har anmälts till tillsynsmyndigheten. Denna incident kunde på grund av semestertider inte anmälas i tid till tillsynsmyndigheten. Dataskyddsombudet rekommenderar därför att bolagets rutiner för incidenthantering säkerställer att det alltid finns någon på plats som kan hantera uppkomna incidenter och anmäla incidenter inom de 72 timmar som lagstiftningen anger (när behov av anmälan föreligger).

2.4.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Kontrollpunkten avser verksamhetens dokumentation av biträdesavtal och andra överenskommelser gällande dataskydd, och förutsätter att verksamheten har identifierat samt registrerat personuppgiftsbiträden i personuppgiftsregistret. Även verksamhetens rutiner för uppdatering och uppföljning av tecknade biträdesavtal innefattas.

Dataskyddsombudets kommentarer:

Bolagets skattning är densamma som föregående år och bolaget ligger kvar på nivå 3, men mycket nära nivå 4. Sammantaget indikerar skattningen att det inom ramen för kontrollpunkten har identifierats risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga.

Enligt skattningen har bolaget i stort ett välfungerande arbete med biträdesavtal och andra överenskommelser. Bolaget behöver däremot säkerställa att man har rutiner för att kontinuerligt genomföra efterlevnadskontroller av anlitade personuppgiftsbiträden. Med hänsyn till att det har tecknats personuppgiftsbiträdesavtal med cirka 75 % av de som har bedömts utgöra personuppgiftsbiträden till bolaget, bör bolaget fortsätta att teckna dessa så att en nivå på 100 % uppnås.

2.4.4 Kontrollpunkt 4: Personuppgiftsregister

Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även verksamhetens arbete med, och rutin för, att säkerställa ett uppdaterat och heltäckande personuppgiftsregister innefattas.

Dataskyddsombudets kommentarer:

Bolagets skattning visar på en marginell försämring inom ramen för kontrollpunkten, men bolaget ligger kvar på nivå 4. Skattningen indikerar att det inom ramen för kontrollpunkten inte föreligger några risker av betydelse och att bolaget arbetar på ett systematiskt vis med sitt personuppgiftsregister.

Eftersom bolaget angett att cirka 75 % av bolagets behandlingar finns registrerade i registret enligt skattningen och att 75 % av dessa innehåller den information som ska finnas med enligt art. 30 GDPR, rekommenderar dataskyddsombudet att bolaget fortsätter arbetet med registret. Eftersom samtliga behandlingar som en personuppgiftsansvarig utför ska finnas i registret och att registret ska innehålla komplett information rekommenderas bolaget att fortsätta sitt arbete inom detta område.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Bolagets skattning är något högre än föregående års skattning på denna kontrollpunkt och bolaget hamnar nu på nivå 4. Skattningen indikerar att det inom ramen för kontrollpunkten inte föreligger några risker av betydelse och att bolaget arbetar på ett systematiskt vis med övergripande strategier för dataskydd.

Enligt skattningen bör bolaget säkerställa att man har rutiner för att efterleva GDPR:s krav vid olika sammankomster, såväl digitala som fysiska. Bolagets informationstillgångar bör även fortsätta klassificeras utifrån *Konfidentialitet, Riktighet* och *Tillgänglighet* i enlighet med stadens styrande dokument. Detta då bolaget har angett att cirka 75 % av bolagets informationstillgångar har klassificerats.

2.4.6 Kontrollpunkt 6: Utbildning

Kontrollpunkten avser verksamhetens arbete med att utbilda och upprätthålla kunskapsnivån i dataskyddsfrågor hos anställda.

Dataskyddsombudets kommentarer:

Bolagets skattning är något högre än föregående års skattning på denna kontrollpunkt och bolaget hamnar nu på nivå 4. Skattningen indikerar att det inom ramen för kontrollpunkten inte föreligger några risker av betydelse och bolaget arbetar på ett systematiskt vis med utbildning inom dataskydd.

Bolagets svar på denna kontrollpunkt indikerar att medarbetarna regelbundet utbildas inom dataskydd och att den allmänna kunskapsnivån ger goda förutsättningar för att bedriva dataskyddsarbetet. Höga skattningar på denna punkt innebär exempelvis att i princip alla anställda korrekt ska kunna identifiera en personuppgiftsincident, att vissa roller ska veta hur och när en konsekvensbedömning ska göras och att ansvariga ska ha koll på tillvägagångssätt när registrerade utövar sina rättigheter i förhållande till bolaget.

Dataskyddsombudet gör ingen annan bedömning än bolaget, men har inte heller kontrollerat kunskapsnivåerna inom bolaget särskilt.

2.4.7 Kontrollpunkt 7: Integritetspolicy

Kontrollpunkten avser verksamhetens utformning samt tillhandahållande av dess integritetspolicy till registrerade (både internt och externt). Även verksamhetens rutin för att upprätthålla en aktuell integritetspolicy omfattas.

Dataskyddsombudets kommentarer:

Bolagets skattning detta år är något lägre än föregående år och bolaget hamnar nu på risknivå 3, vilket indikerar att det finns risker som behöver åtgärdas, men att de inte är brådskande, omfattande eller allvarliga.

Efter att ha sett över bolagets externa integritetspolicy på en övergripande nivå anser dataskyddsombudet att årets skattning är mer korrekt än föregående års skattning och att det finns skäl att se till att utövandet av informationsplikten förbättras. Bolagets integritetspolicy innehåller dock relativt tydlig information och det är positivt att bolaget i stor utsträckning använder sig av en så kallad skiktad metod för att informera specifika grupper av registrerade hur deras personuppgifter behandlas.

Kraven på att uppfylla informationsplikten är dock högt ställda. För att informationsplikten ska anses vara uppfylld ska det bland annat tydligt framgå

ändamål och rättslig grund, hur länge uppgifterna lagras eller vara väldigt tydligt för den registrerade hur lagringstiden bedöms. Det ska även framgå vilka som är mottagare, vad som gäller när det kommer till de registrerades rättigheter samt vara tydligt om och i så fall vilka tredjelandsöverföring som sker.

Även om mycket av ovanstående finns med i policyn så bör bolaget se över exempelvis hur man informerar om lagringstid. Det kan vara okej att hänvisa till kriterierna för hur lagringstiden bedöms om exakt lagringstid inte anges. Den registrerade ska dock, utifrån sin egen situation, i så fall kunna bedöma lagringstiden utifrån kriterierna. Det är inte tillräckligt att ange att uppgifterna sparas så länge som det är nödvändigt för ändamålet. Dataskyddsombudet bedömer det också som tveksamt om hänvisning till en dokumenthanteringsplan som den registrerade inte har tillgång till kan anses tillräckligt. Bolaget bör även säkerställa att de registrerades rättigheter specificeras för respektive behandling då tillämpligheten kan variera.

En ordentlig översyn av helheten bör genomföras kontinuerligt, inte minst med hänsyn till den praxis som nu finns kopplat till informationsplikten och som kontinuerligt fortsätter att komma. Vid avstämning med bolaget framgår att de har identifierat detta behov, inte minst utifrån det tillsynsbeslut som Integritetsskyddsmyndigheten fattat gentemot det svenska företaget Klarna. Dataskyddsombudet anser att detta talar för att det finns en medvetenhet inom bolaget och goda förutsättningar att förbättra sin policy.

2.4.8 Kontrollpunkt 8: E-post och dokumenthantering

Kontrollpunkten avser verksamhetens rutiner för e-post och dokumenthantering. I detta är en aktuell och fastställd dokumenthanteringsplan med gallringsbeslut en förutsättning för att verksamheten ska kunna säkra följsamhet gentemot dataskyddsförordningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Dataskyddsombudets kommentarer:

Bolaget har förbättrat sitt resultat på denna kontrollpunkt jämfört med föregående år och ligger nu på nivå 3. Skattningen indikerar nu att det finns risker, men att de inte bedöms vara brådskande, omfattande eller allvarliga. Föregående år indikerade resultatet att det fanns risker som bedömdes vara omfattande och/eller kräva omgående åtgärder.

Det är positivt att bolaget jämfört med föregående år nu anger att de informerar registrerade om hur deras personuppgifter behandlas vid första kontakt via e-post. Med hänsyn till hur bolaget har besvarat frågorna under kontrollpunkten bedömer dataskyddsombudet att arbetet med denna kontrollpunkt behöver prioriteras.

Bolaget behöver framförallt se till att det finns en aktuell, uppdaterad och fastställd dokumenthanteringsplan så att det finns tydlighet kring när och hur personuppgifter gallras. Kopplat till detta behövs också möjlighet att kontrollera att personuppgifter gallras enligt gällande gallringsbeslut. Utan dessa komponenter på plats kommer bolaget ha svårt att uppfylla de grundläggande principerna om uppgiftsminimering och lagringsminimering i GDPR.

Bolaget behöver även arbeta vidare med informationsklassificering av sina personuppgiftsbehandlingar och säkerställa att tidigare klassificeringar är aktuella. Bolaget behöver också säkerställa att det finns rutiner och anvisningar för hantering av personuppgifter i e-post, samt i övrigt säkerställa att det finns anvisningar för hur olika informationsklasser får hanteras och lagras.

2.4.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras, samt rutiner kopplat till detta.

Dataskyddsombudets kommentarer:

Bolagets skattning är marginellt högre på denna kontrollpunkt än föregående år, men det övergripande resultatet ligger kvar på nivå 3. Detta innebär att det inom ramen för kontrollpunkten finns risker, men att de inte bedöms vara brådskande, omfattande eller allvarliga. Skattningen ligger nära nivå 4.

Bolaget anger att ett flertal rutiner finns på plats. Det finns bland annat rutiner för att identifiera behandlingar med hög risk, inhämta dataskyddsombudets synpunkter efter utförd tröskelanalys och konsekvensbedömning, genomföra och dokumentera konsekvensbedömningar och bedöma risker för de registrerade.

Däremot anges också att det saknas rutiner för hur beslut om accepterande av risker i en konsekvensbedömning ska fattas och dokumenteras och för att inhämta de registrerades synpunkter när så är lämpligt. Vidare anges att bolaget har bedömt om en konsekvensbedömning behöver utföras för cirka 50 % av sina personuppgiftsbehandlingar och att konsekvensbedömningar utförts för cirka 50 % av de behandlingar där det sannolikt behöver utföras en sådan.

Med hänsyn till ovanstående bedömer dataskyddsombudet att det finns behov av förbättringar inom aktuellt område och rekommenderar att bolaget prioriterar detta arbete.

2.4.10 Kontrollpunkt 10: IT-projekt och upphandling

Kontrollpunkten avser verksamhetens organisation och rutiner för hantering av dataskyddsfrågor inom IT-projekt och upphandling. I detta ingår till exempel hur

verksamheten integrerar dataskyddsfrågor i arbetet med upphandling av nya, samt utvecklingen av, befintliga system och tjänster.

Dataskyddsombudets kommentarer:

Bolaget har skattat sig likadant som förra året på denna kontrollpunkt och bolaget ligger kvar på nivå 4. Detta innebär att det, utifrån skattningen, inte föreligger några risker av betydelse och bolaget arbetar på ett systematiskt vis med IT-projekt och upphandling.

Enligt skattningen säkerställer bolaget att dataskyddsperspektivet finns med i arbetet med nya IT- och digitaliseringslösningar samt vid utvecklingen av redan befintliga system och tjänster. Vid upphandlingen av nya system/tjänster så tas anpassning till inbyggt dataskydd och dataskydd som standard med i kravställningen.

Verksamheten rekommenderas dock ha som rutin att dataskyddsombudet involveras från start i dessa processer. Dataskyddsombudet har involverats inom ramen för konsekvensbedömningar, men bör involveras även i samband med kravställning osv.

2.4.11 Kontrollpunkt 11: IT-system och digitala verktyg

Kontrollpunkten avser verksamhetens rutiner för att säkerställa att verksamhetens personuppgiftshantering inom ramen för IT-system och digitala verktyg är förenlig med dataskyddsförordningen. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår även.

Dataskyddsombudets kommentarer:

Bolaget har skattat sitt arbete inom ramen för denna kontrollpunkt likadant som föregående år och ligger kvar på nivå 4. Sammantaget indikerar skattningen att det inom ramen för kontrollpunkten inte föreligger några risker av betydelse och bolaget arbetar på ett systematiskt vis med IT-system och digitala verktyg.

Bolaget behöver enligt skattningen dock utföra kontroller så att IT-system och digitala verktyg används på rätt sätt. Därför är det även nödvändigt att verksamheten ser till att informera medarbetarna om korrekt användning av systemen/verktygen. I övrigt har bolaget angett att de säkerställer att dataskyddsperspektivet beaktas vid införandet och användandet av kostnadsfria tjänster, såsom gratisappar och sociala medier. Bolaget har också angett att behörighetsstyrningen och rutiner kring denna fungerar väl.

Bolaget har skattat sig högt på påståendet om att användning av cookies på webbsidor följer kraven i GDPR och att de registrerade får information om behandlingen via verksamhetens integritetspolicy. I bolagets policy anges att såväl nödvändiga cookies för hemsidans funktionalitet som icke nödvändiga cookies i

form av statistik samlas in. Denna information är något motstridig mot den information som finns tillgänglig via bolagets cookieruta. Nödvändiga cookies kräver inget samtycke enligt lagen (2022:482) om elektronisk kommunikation för att få samlas in (tidigare SFS 2003:389) för att få samlas in, medan icke-nödvändiga kräver det. Bolagets cookieruta efterfrågar att besökaren klickar i att denne har förstått informationen om cookies. Vid avstämning med bolaget framgår att bolaget inte längre samlar in statistikcookies, varför bolaget bör säkerställa att informationen i integritetspolicyn är korrekt.

Vid kontroll av bolagets hemsida framgår att tredjepartscookies finns på hemsidan, som inte förefaller vara av ”nödvändig” karaktär. Då kakorna avser Youtube, bör bolaget säkerställa att det inte föreligger risk för otillåten tredjelandsöverföring.

Det förekommer också ett större antal tredjepartsförfrågningar, varav flera avser parter med amerikanska ägare. Bolaget bör även här se över tredjepartsförfrågningarna utifrån risk för tredjelandsöverföring.

Avseende sociala medier så använder bolaget såväl Facebook som LinkedIn och Youtube. Vid avstämning med bolaget framgår att det pågår en koncerngemensam översyn av de sociala medierna, inte minst med hänsyn till domen i Schrems II-målet.

I Schrems II-domen (juli 2020) förtydligade EU-domstolen vad som gäller för överföringar av personuppgifter till länder utanför EU/EES, så kallade tredjelandsöverföringar. Domen sade, i breda drag, att det skydd för personuppgifter som finns i USA inte är likvärdigt med det som finns i EU/EES varför den personuppgiftsansvarige antingen måste vidta extra skyddsåtgärder eller avbryta behandlingen. I Schrems II-domen prövades särskilt Facebook, men även andra sociala medier såsom Instagram, Youtube och LinkedIn är exempel på sociala medier som överför personuppgifter till USA.

Dataskyddsombudets rekommendationer är att upphöra med att behandla personuppgifter i sociala medier i de fall följsamhet mot GDPR inte kan säkerställas. I detta utgår dataskyddsombudet helt ifrån bestämmelserna i GDPR och den praxis som finns tillgänglig. Även om dataskyddsombudet anser det positivt att bolaget tillsammans med koncernen genomför en analys av användningen, bör bolaget vidta ytterligare åtgärder för att följsamhet mot förordningen ska kunna säkerställas vid användningen av Facebook, Youtube och LinkedIn. Dataskyddsombudet noterar att personuppgifter förekommer i bolagets sociala medier.

2.4.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering.

Dataskyddsombudets kommentarer:

Bolaget ligger kvar på nivå 4 precis som förra året, men har också gjort en marginell förbättring av medelvärdet. Enligt skattningen behöver bolaget enbart ta fram en rutin för tillbakadragande av samtycke.

Dataskyddsombudet har ingen anledning att ifrågasätta bolagets skattning. Under 2022 har dataskyddsombudet fått kännedom om ett par tillfällen då registrerade har velat nyttja sin rätt till registerutdrag. Enligt vad dataskyddsombudet kan bedöma, verkar dessa begäranden ha hanterats i enlighet med förordningens bestämmelser.

2.5 Sammanfattande rekommendationer

För att på ett praktiskt plan kunna identifiera vad verksamheten behöver arbeta med inom ramen för respektive kontrollpunkt behövs en noggrann genomgång av enkätresultaten. I detta rekommenderas verksamheten att samråda med dataskyddsombudet för att se hur arbetet framåt bör utformas och vilka delar som bör prioriteras utifrån verksamhetens risker. Även för verksamheter med låga risker krävs kontinuerliga insatser för att denna risknivå ska bibehållas.

Utifrån identifierade risker rekommenderar dataskyddsombudet att bolaget under 2023 prioriterar följande delar av dataskyddsarbetet:

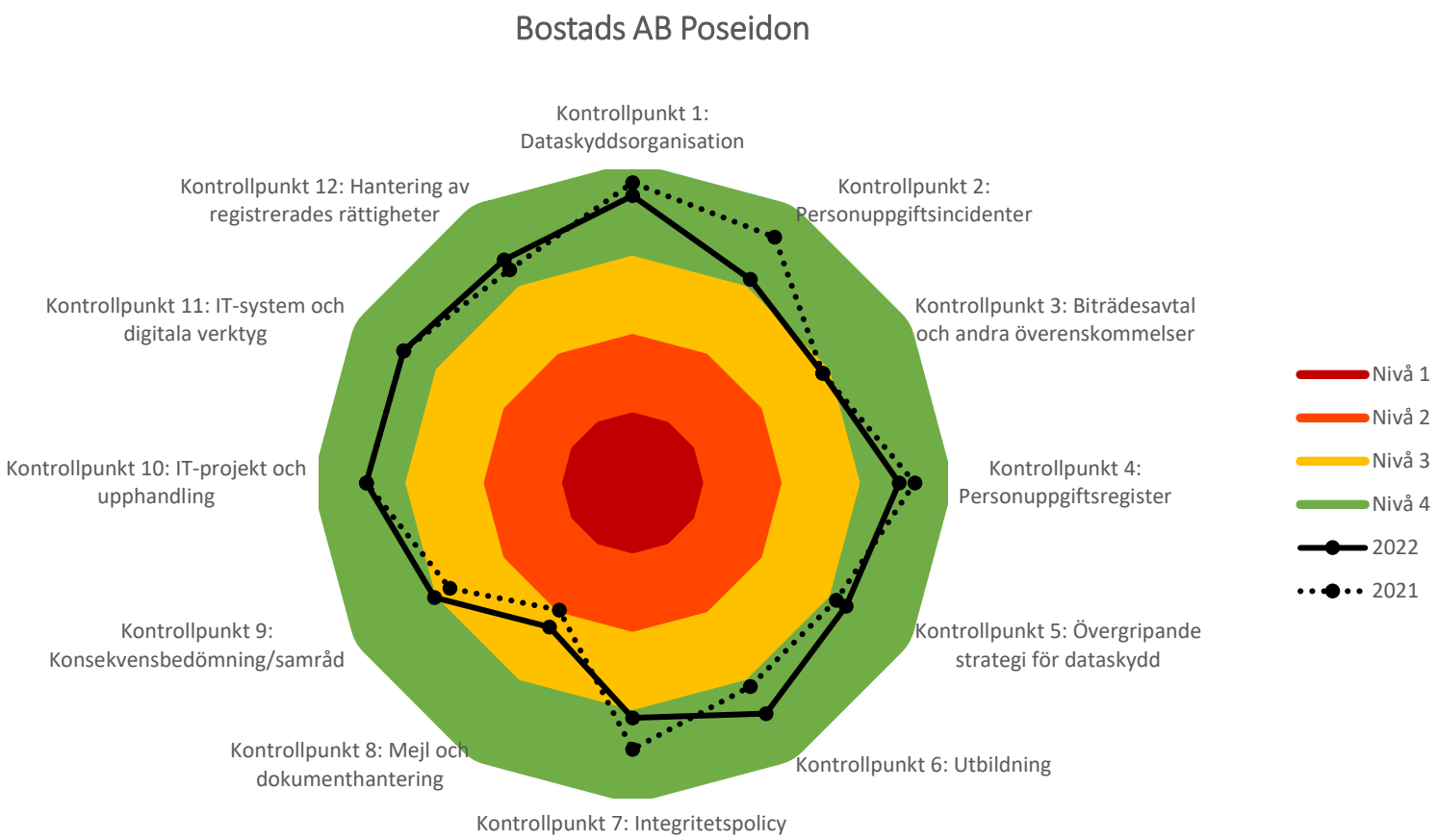
- Kontrollpunkt 2: Personuppgiftsincidenter.
- Kontrollpunkt 8: E-post och dokumenthantering.
- Kontrollpunkt 9: Konsekvensbedömning/samråd.
- Kontrollpunkt 11: IT-system och digitala verktyg.

3 Bilagor

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.

Bilaga 2: Fördjupad kontroll 2022 – Kamerabevakning.

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.



Fördjupad kontroll

Kontrollpunkt 11: Kamerabevakning Bostads AB Poseidon

Bakgrund

Den fördjupade kontrollen avseende kamerabevakning har haft till syfte att kartlägga verksamhetens kamerabevakning som innebär personuppgiftsbehandling och undersöka om hanteringen uppfyller kraven i dataskyddsförordningen (GDPR) och kamerabevakningslagen. Fokus har legat på ifall det finns dokumenterade bedömningar, om tillräcklig information lämnas till de registrerade och i förekommande fall om tillstånd finns. Kontrollen har genomförts genom att verksamheten har fått svara på ett antal frågor och bifoga underlag. I vissa fall har även uppföljande/kompletterande frågor och avstämningar varit nödvändiga.

Iakttagelser från kontrollen

Personuppgiftsansvariga ska i sin användning av kamerabevakning, i de fall det innebär en personuppgiftsbehandling, följa reglerna i dataskyddsförordningen och kamerabevakningslagen. Även i de fall då kamerabevakningen inte medför att tillstånd behöver sökas hos Integritetsskyddsmyndigheten (IMY) behöver reglerna i GDPR följas.

Rättslig reglering och vägledning

En verksamhet som planerar en kamerabevakning måste noga tänka igenom bevakningen och dokumentera sina bedömningar. En del i detta är att säkerställa att bevakningen uppfyller kraven enligt dataskyddsförordningen. Det innebär att bevakningen bl.a. behöver ha ett tydligt avgränsat ändamål, rättslig grund och att förordningens principer beaktas. För att uppfylla principen om uppgiftsminimering behöver platsen/platserna som bevakas vara begränsade och endast omfatta det som syftet med bevakningen kräver. Det får också enbart ske bevakning på de tider då bevakningen, med hänsyn till syftet, är nödvändig. Om kamerabevakningen sker med bildinspelning behöver det även säkerställas att lagring inte sker under längre tid än vad som är nödvändigt. Enligt vägledning från IMY är huvudregeln att materialet inte bör sparas längre än 72 timmar. Verksamheten behöver också säkerställa att konsekvensbedömningar görs i de fall då kraven för detta är uppfyllda. Det ska också lämnas information om kamerabevakningen till de registrerade. Informationen ska vara lättillgänglig och begriplig.

Offentliga aktörer och andra som utför en uppgift av allmänt intresse är tillståndspliktiga vid bevakning på platser dit allmänheten har tillträde, men bara om bevakningen innebär varaktig eller regelbundet upprepad personbevakning. Även om kamerabevakningen inte är tillståndspliktig innebär det inte automatiskt att den är tillåten.

Poseidons användning av kamerabevakning

Bolaget bedriver kamerabevakning på 12 platser i staden, med totalt 46 kameror. Syftet är att öka säkerheten/tryggheten för medarbetare och hyresgäster genom att förhindra, förebygga samt utreda brott och allvarliga störningar. Något tillstånd för övervakningen har inte sökts.

Bolaget har i sina svar till dataskyddsombudet angett att kamerabevakningen har varit och fortsatt är föremål för översyn. Detta eftersom brister, särskilt utifrån bestämmelserna i GDPR, tidigare har identifierats. Bolaget har genomfört och försätter att genomföra ett förbättringsarbete för att säkerställa följsamhet till såväl kamerabevakningslagen som GDPR.

Dataskyddsombudets rekommendationer

Tillstånd

Offentliga aktörer och andra som utför en uppgift av allmänt intresse är tillståndspliktiga vid bevakning på platser dit allmänheten har tillträde, men bara om bevakningen innebär varaktig eller regelbundet upprepad personbevakning. Även om kamerabevakningen inte är tillståndspliktig innebär det inte automatiskt att den är tillåten.

Bolaget uppger att man inte sökt något tillstånd för kamerabevakning. Detta då bolagets bevakning sker på platser dit allmänheten inte har tillträde. Under förutsättning att den information som bolaget inkommit med är korrekt instämmer dataskyddsombudet i att behandlingen inte är av en sådan art att den kräver ett tillstånd för att få genomföras. Utifrån underlagen är det dock svårt att göra en definitiv bedömning av samtliga platser då det i vissa fall saknas utförliga beskrivningar. Omständigheten att allmänheten inte har tillträde är dock sådan att det utesluter tillståndsplikt. Det hade dock varit bra om bolaget utifrån varje bevakning tog fram underlag som beskriver varför allmänheten inte kan anses ha tillträde. Detta eftersom tolkningen av om allmänheten har tillträde eller ej ska göras brett.[1] Det kan exempelvis handla om att någon kamera är riktad på ett visst vis att den visar yttre entréer eller liknande eller att det skulle finnas ett visst antal platser i ett parkeringsgarage som är upplåtna för allmänheten, även om parkeringen i övrigt enbart är tillgänglig för hyresgäster. Utifrån vad som kan utläsas tolkar dataskyddsombudet det som att sådana omständigheter inte föreligger, men rekommenderar ändå Poseidon att förtydliga sina underlag så att bedömningen av tillståndsplikten blir tydlig.

Tider och platser som kamerabevakas

Den plats som kamerabevakas måste vara identifierad och avgränsad, så att bevakning inte sker på en större plats än nödvändigt med hänsyn till ändamålet. Om kameran inte kan riktas för att minska omfattningen av filmningen, behöver tekniska åtgärder vidtas som kan maskera områden. Även tiden på dygnet där kamerabevakningen sker är viktig att reglera. Filmning får bara ske under tider där man kan visa att ett behov finns.

[1] Jfr. RÅ 2000 ref. 52.

Poseidon bedriver kamerabevakning på tolv platser runt om i staden med totalt 46 kameror. Bevakningen sker i entréer och trapphus, i garage och i miljörum. Omfattningen av bevakningen varierar mellan att enbart ske ”efter mörkrets intrång” och dygnet runt.

Utifrån den information som dataskyddsombudet har tagit del av förefaller det rimligt, med hänsyn till ändamålen med kamerabevakningen, att bevakningen sker i angiven omfattning. I flera fall har bolaget angett varför en viss tid för bevakningen anses som lämplig, men eftersom det i flera fall också saknas överväganden är det svårt för dataskyddsombudet att helt avgöra om tiden för bevakningen är väl avvägd. Bolaget bör noggrant dokumentera sina överväganden i de fall det saknas.

Avseende lagringstid har bolaget uppgett att lagringstiden varierar och av underlagen framgår inte alltid hur lång lagringstiden är. Bolaget bör åtgärda detta där det saknas. Utifrån vad dataskyddsombudet kan utläsa varierar lagringstiden, men verkar i regel vara mellan fem och 14 dagar. Det förekommer dock uppgifter för vissa kameror om en lagringstid på 72 timmar. I underlagen anges dock att detta ska ändras. Av den exempelskylt för information till de registrerade som bolaget har skickat med som underlag framgår också en lagringstid på 72 timmar.

Huvudregeln för inspelat material är att det får lagras i 72 timmar, vilket gör att bolagets lagringstid på 14 dagar klart överstiger huvudregeln. Det är dock möjligt att frångå huvudregeln om det finns skäl för det, men bolaget behöver då tydligt ange och bedöma hur lång tid det tar för verksamheten att upptäcka en incident och hur lång tid det tar att omhänderta materialet för att skicka det till polisen vid brott. Bolaget har inte särskilt angivit varför lagringstiden behöver vara fem eller 14 dagar, vilket bör åtgärdas. Dataskyddsombudet kan inte, utifrån de underlag som finns, bedöma om lagringstiden är ett väl avvägt avsteg från huvudregeln på 72 timmar.

Sammantaget rekommenderar dataskyddsombudet att lagringstiden ses över och att bolaget tydligt dokumenterar sina överväganden för att säkerställa att lagringstiden verkligen är befogad i förhållande till ändamålen och omständigheterna kring hur lång tid det tar att upptäcka och hantera en incident.

Ändamål och rättslig grund

Kamerabevakningen måste ha ett tydligt syfte, ett berättigat och specifikt ändamål, för att vara tillåten. Ändamålet styr vad som får göras, och nya ändamål får inte läggas till om de inte är förenliga med det ursprungliga ändamålet. Kamerabevakningen måste också vara nödvändig för att uppnå det specifika ändamålet.

Poseidon har angett att ändamålet med behandlingen är att öka säkerheten/tryggheten för medarbetare och hyresgäster genom att förhindra, förebygga samt utreda brott och allvarliga störningar.

Utöver ändamål måste det finnas stöd i en rättslig grund i dataskyddsförordningen för att kamerabevakningen ska få utföras. Om tillstånd inte krävs är den rättsliga grunden berättigat intresse ofta tillämplig.

Bolaget har uppgett att den rättsliga grund som man stödjer sin behandling på är berättigat intresse. För bevakningen i Hjällbo och Kortedala, samt på Anders Personsgatan har bolaget genomfört en tydlig intresseavvägning där behovet av

behandlingen vägs mot den registrerades (den som filmas) integritetsintresse. Dataskyddsombudet har inget att invända i denna del. För övriga bevakningar saknas sådan bedömning i det underlag som dataskyddsombudet har tagit del av. Om sådan inte finns bör bolaget säkerställa att det upprättas.

Avseende bevakningen med sex eller tio kameror (framgår olika antal av olika underlag) på Borgaregatan ifrågasätter dataskyddsombudet behovet av bevakningen. Det framgår nämligen av underlaget till bevakningen att det är ”tämligen lugnt” i det aktuella garaget och att något material aldrig heller behövt överlämnas till polisen från det aktuella garaget. Det saknas också en tillräckligt utförlig bedömning kring varför det skulle finnas ett behov av kamerabevakningen, även om det kortfattat framgår att garaget skulle bli tillhåll för narkotikaförsäljning om bolaget monterade ned kamerorna (framgår dock inte varför så skulle ske). Dataskyddsombudet bedömer att det av bolagets motivering inte kan utläsas att kamerabevakning på den aktuella platsen är nödvändig. Om bolaget inte kan påvisa nödvändigheten, kan inte heller bevakningen anses förenlig med lagstiftningen. Utifrån nuvarande bedömning förefaller bolaget varken ha ett berättigat ändamål med bevakningen eller en tillämplig rättslig grund då den rättsliga grunden berättigat intresse förutsätter att behandlingen är nödvändig.

Konsekvensbedömningar och dokumenterade bedömningar/analyser

En konsekvensbedömning är i vissa fall ett krav enligt dataskyddsförordningen. IMY anger till exempel att systematisk övervakning av en allmän plats i stor omfattning, genom till exempel kameraövervakning, innebär att en konsekvensbedömning ska göras. Även en behandling som sannolikt leder till hög risk för de registrerades fri- och rättigheter kräver att en konsekvensbedömning görs. Syftet med en konsekvensbedömning är att identifiera risker och åtgärder samt bedöma om behandlingen är nödvändig och proportionerlig i förhållande till syftet.

Bolaget har genomfört en konsekvensbedömning avseende den kamerabevakning som bedrivs i Hjällbo. Bolaget har på fråga varför konsekvensbedömningar inte utförts för övriga bevakningar angett att kamerabevakningen inte anses integritetskänslig. Bolaget bör bedöma om övriga bevakningar behöver konsekvensbedömas i enlighet med bestämmelserna i GDPR. Att enbart ange att bevakningen inte anses integritetskänslig är inte tillräckligt, utan bolaget behöver genomföra bedömningen utifrån de kriterier som finns uppställda i GDPR och som anges i IMY:s förteckning över kriterier som gör att konsekvensbedömningar behöver genomföras. I de underlag som dataskyddsombudet tagit del av finns vissa risk- och behovsanalyser gjorda för vissa bevakningar, vilket är positivt. Dessa underlag är väl utförda och tydliga. Dataskyddsombudet uppfattar dock inte dessa som konsekvensbedömningar utifrån GDPR:s bestämmelser, även om de innehåller en del sådana moment som en konsekvensbedömning ska innehålla och med fördel kan återanvändas vid upprättandet av konsekvensbedömningar.

Säkerhet för bevakningen

Om kamerabevakningen innebär en personuppgiftsbehandling och leverantören av bevakningen hanterar personuppgifter på verksamhetens uppdrag, krävs ett personuppgiftsbiträdesavtal. Avtalet reglerar biträdets befogenheter, lagringstid, med mera. Det är också viktigt att verksamheten har koll på vilken teknik som används.

Bolaget uppger att tekniken som används är lagrad video och att systemet som används på samtliga anläggningar heter Axis. All video lagras i leverantörens molntjänst. Endast bild spelas in. Leverantör för samtliga anläggningar är Safeteam. Personuppgiftsbiträdesavtal har tecknats med leverantören.

Enligt artikel 32 GDPR behöver den personuppgiftsansvarige säkerställa en tillräcklig teknisk och organisatorisk säkerhet. Inspelat material som visar personer som befinner sig i närheten av sin hemmiljö, kan uppfattas som särskilt integritetskänsligt. IMY anger i sin vägledning att bevakning av platser dit allmänheten inte har tillträde i flera fall kan vara än mer integritetskänslig.[2] Detta kan innebära att den behandling av personuppgifter som bevakningen innebär behöver omgärdas av högre säkerhet än andra personuppgifter. Även om molntjänster i många fall har en hög säkerhet så riskerar användningen att ge upphov till att fler personer än nödvändigt ges tillgång till materialet, såväl hos personuppgiftsansvarig, som hos personuppgiftsbiträdet. Även om dataskyddsombudet uppfattar det som att bolaget vidtar vissa åtgärder för vem som har rätt att ta del av materialet och när, så bedömer dataskyddsombudet att bolaget ytterligare bör säkerställa skyddet för personuppgifterna – särskilt när de behandlas hos leverantören.

Information till de registrerade

Om kamerabevakning sker måste information lämnas på ett begripligt och lättillgängligt sätt. IMY rekommenderar att information sker via två så kallade informationslager. Det första ska ges på en informationsskylt med den viktigaste informationen om bevakningen. Ett andra informationslager med all information kan ges på annat sätt.

Bolaget hänvisar till information på sin hemsida avseende personuppgiftsbehandlingen. Bolaget har också bifogat underlag som visar en exempelskylt som sätts upp vid bevakningen. Dataskyddsombudet anser att den information som lämnas på skyltarna (utifrån exempelskylten) motsvarar den information som ska lämnas i det första informationslagret. Informationen hade dock kunnat vara mer tydligt uppdelad och pedagogiskt utformad. Om skyltarna ännu inte finns uppsatta på samtliga platser som bevakas, bör säkerställas att så görs.

Sammanfattade rekommendationer

- Förtydliga bedömningen kring varför bevakningen inte är tillståndspliktig i bolagets underlag.
- Dokumentera bolagets överväganden kopplat till tider som kamerabevakningen sker.
- Se över lagringstiden och dokumentera de överväganden som bolaget gör för att säkerställa att lagringstiden verkligen är befogad i förhållande ändamålen och omständigheterna kring hur lång tid det tar att upptäcka och hantera en incident.
- Säkerställ att en dokumenterad intresseavvägning finns för samtliga bevakningar.
- Säkerställ att bevakningen på Borgaregatan har ett legitimt ändamål, är nödvändig för att uppnå ändamålet och har en rättslig grund.

[2] Integritetsskyddsmyndighetens vägledning vid kamerabevakning, rapport 2021:2, s. 31.

- Bedöm om konsekvensbedömningar behöver genomföras utifrån GDPR:s bestämmelser för de bevakningar som det inte har genomförts sådana för.
- Säkerställ att personuppgifterna i inspelat material hanteras på ett tillräckligt säkert sätt.

Bilagor

- Frågor och informationsutskick

Information om fördjupad kontroll 2022

Kontrollpunkt 11: Kamerabevakning

Personuppgiftsbehandlingar som sker i samband med kamerabevakning behöver uppfylla kraven i dataskyddsförordningen. Därtill finns reglering i form av kamerabevakningslagen (2018:1200), vars syfte bl.a. är att säkerställa att fysiska personer skyddas mot otillbörligt intrång i den personliga integriteten. Sedan lagens införande 2018 har det skett vissa förändringar inom kamerabevakningsområdet och flera aktörer undantas nu från det tidigare kravet på att ansöka om tillstånd.

Även om en verksamhet inte behöver ansöka om tillstånd för att få kamerabevaka är det viktigt att den som bedriver bevakning beaktar reglerna i dataskyddsförordningen och säkerställer att nödvändiga bedömningar görs och dokumenteras. Den som använder kamerabevakning behöver också säkerställa att tillräcklig information lämnas om den aktuella bevakningen, för vilket det finns specifika krav.

Granskningen avser att kontrollera huruvida verksamhetens användning av kamerabevakning uppfyller dataskyddsförordningen och kamerabevakningslagen, med fokus på dokumenterade bedömningar, om tillräcklig information lämnas till de registrerade och i förekommande fall om tillstånd finns.

Tillvägagångssätt

Den fördjupade kontrollen kommer att genomföras i två delar. I del ett ombeds ni att skicka in dokumenterade instruktioner/rutiner samt besvara ett antal frågor. I del två kommer uppföljande frågor att ställas.

Dataskyddsombudet kommer sedan att sammanställa underlaget i en delårsrapport som lämnas till er i juni.

Fördjupad kontroll 2022

Kontrollpunkt 11: Kamerabevakning (del 1)

Ni ombeds besvara följande frågor samt skicka in dokumenterade rutiner, instruktioner, styrande dokument eller liknande avseende er användning av kamerabevakning.

1. Vilka platser kamerabevakar ni? Detta ska beskrivas även utifrån vilka områden/ytor på platsen som kamerabevakas tex. entrén utvändigt, entrén invändigt, trapphus, specifika rum.
    a. Ange ändamålet och rättslig grund för behandlingen/behandlingarna.
    b. Har ni sökt tillstånd för den kamerabevakning som ni utför? Om inte ange varför.
2. Har ni utfört konsekvensbedömningar eller andra typer av dokumenterade bedömningar/analyser för er kamerabevakning? Om ja, skicka även in denna dokumentation.
3. Vilken teknik använder ni och vilka leverantörer använder ni?
    a. Finns personuppgiftsbiträdesavtal upprättade med de leverantörer som ni använder? Bifoga dessa avtal.
4. Hur informerar ni de registrerade om kamerabevakningen som utförs? Bifoga den information som ni tillhandahåller de registrerade och ange hur den tillgängliggörs.

Obs! Det är mycket viktigt att frågorna besvaras av eller i samråd med rätt befattningar/roller inom förvaltningen/bolaget för att resultatet ska bli korrekt. Säkerställ även en lämplig förankring av svaren inom organisationen innan de översänds till dataskyddsombudet.

Underlaget ska ha inkommit till dataskyddsombudet **senast den 15 mars 2022.**

Har du frågor, kontakta ditt huvudansvarige dataskyddsombud.

Fördjupad kontroll 2022

Kontrollpunkt 11: Kamerabevakning (del 2)

Ni ombeds besvara följande **uppföljande/förtydligande frågor** samt skicka in viss dokumentation avseende er användning av kamerabevakning.

1. Vilka platser kamerabevakar ni? Detta ska beskrivas även utifrån vilka områden/ytor på platsen som kamerabevakas tex. entrén utvändigt, entrén invändigt, trapphus, specifika rum.

a. Ange ändamålet och rättslig grund för behandlingen/behandlingarna.
b. Har ni sökt tillstånd för den kamerabevakning som ni utför? Om inte ange varför.
    - **Uppföljande fråga: Ni har enbart angett nej på frågan om tillstånd, finns det en bedömning i varje enskilt fall?**

2. Har ni utfört konsekvensbedömningar eller andra typer av dokumenterade bedömningar/analyser för er kamerabevakning? Om ja, skicka även in denna dokumentation.
    - **Uppföljande fråga:** För de bevakningar där konsekvensbedömningar inte har gjorts, ange varför så inte har skett.

3. Vilken teknik använder ni och vilka leverantörer använder ni?

a. Finns personuppgiftsbiträdesavtal upprättade med de leverantörer som ni använder? Bifoga dessa avtal.
    - **Uppföljande fråga:** Svaret har lämnats blankt avseende två bevakningar på Stackmolnsgatan och Väderilsgatan, komplettera eller motivera varför svar inte lämnas. Utveckla också svaret och beskriv tekniken avseende CCTV Milestone, sker inspelningen t.ex. med ljudupptagning? Lagras inspelningen i molntjänst?
    - **Uppföljande fråga:** Enbart PUB-avtal med SafeTeam har bifogats. Varför finns inte PUB-avtal?

Kompletterande förtydligande fråga:
Beskriv i breda drag hur kamerabevakningen på de olika platserna används. Är det t.ex. enbart inspelat material som bolaget tittar på vid behov i efterhand eller sker realtidsövervakning?

Obs! Det är mycket viktigt att frågorna besvaras av eller i samråd med rätt befattningar/roller inom förvaltningen/bolaget för att resultatet ska bli korrekt. Säkerställ även en lämplig förankring av svaren inom organisationen innan de översänds till dataskyddsombudet. Om ni inte vet hur frågan ska besvaras, fråga t.ex. dataskyddskontakten eller dataskyddsombudet.

Underlaget ska ha inkommit till dataskyddsenheten **senast den juni 2022.**

Har ni frågor, kontakta dataskyddsenheten (dso@intraservice.goteborg.se).