Styrelsehandling nr 9
Datum 2023-03-23
Diarienummer: BB2023-0184
Diarienummer: BB2023-0196

Handläggare
Sara Fischer
Telefon: 031-731 50 10
E-post: sara.fischer@bostadsbolaget.se

Årsrapport för dataskyddsarbete 2022 (DSO)

Informationsärende

Styrelsen Göteborgs stads bostadsaktiebolag föreslås

Årsrapport för Bostadsbolagets dataskyddsarbete antecknas.

Sammanfattning

Varje år genomför dataskyddsenheten på Intraservice en kontroll över bolagets dataskyddarbete. Kontrollen består av ett antal fasta kontrollpunkter samt utvalda fördjupade kontroller. Den fördjupade kontrollen 2022 omfattade kamerabevakning (CCTV). I årsrapporten presenteras resultat av kontrollen för 2022 och rekommendationer om hur bolaget ska förbättra arbetet med dataskydd enligt Dataskyddsförordningen (GDPR) samt resultatet av den fördjupade granskningen inom kamerabevakning.

Bedömning ur ekonomisk dimension

Bolaget har inte funnit några aspekter på frågan utifrån denna dimension.

Bedömning ur ekologisk dimension

Bolaget har inte funnit några aspekter på frågan utifrån denna dimension.

Bedömning ur social dimension

Bolaget har inte funnit några aspekter på frågan utifrån denna dimension.

Samverkan

Ärendet har inte bedömts vara föremål för samverkan.

Bilagor

1. Årsrapport för dataskyddsarbetet 2022

Dataskyddsenheten

Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Göteborgs Bostads AB (Bostadsbolaget)

2022-12-23

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 har god kontroll på sin kamerabevakning i stort och förståelse för att det är två separata regelverk som ska tillämpas. 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 se över och förtydliga lagringstiden av inspelat material samt att förtydliga underlagen till respektive

bevakning så att det tydligt framgår på vilken grund som bevakningen inte är tillståndspliktig.

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.	

2.4 Bostadsbolagets 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.

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

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 (3) som föregående år, men med en marginell försämring av medelvärdet. Skattningen indikerar att det inom ramen för kontrollpunkten har identifierats risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga. Med hänsyn till att fyra av sex frågor har besvarats med alternativet *Nej, det stämmer inte bra*, rekommenderar dataskyddsombudet att arbetet med denna kontrollpunkt prioriteras.

Bolaget behöver, utifrån skattningen, säkerställa att den interna dataskyddsorganisationen ges ett ökat stöd och mer resurser för att kunna få rätt förutsättningar att utföra arbetet. Olika befattningshavares ansvar och mandat att fatta beslut i olika typer av dataskyddsfrågor behöver också förtydligas.

Bolaget behöver vidare arbeta för att dataskydd ska bli en naturlig och integrerad del av det dagliga arbetet för alla medarbetare. Det behöver även finnas rutiner för att säkerställa att dataskyddsombudet involveras i de frågor som rör dataskydd inom verksamheten.

Vid avstämning med bolaget framgår att ett ambitiöst arbete redan påbörjats inom ramen för kontrollpunkten. Bolaget har exempelvis upprättat en organisation med utpekade personer i bolagets olika verksamheter som ska kunna lite extra om dataskydd, hålla koll på verksamhetens olika behandlingar och bistå bolagets dataskyddskontakt/informationssäkerhetssamordnare. Dataskyddsombudet ser mycket positivt på detta. Dataskyddsombudet anser också att bolaget har skattat sig ärligt på kontrollpunkten, vilket i sig indikerar att bolaget har en utpräglad förståelse för vad som faktiskt krävs för att ett bolag som behandlar ett stort antal personuppgifter ska ha en ändamålsenlig och fungerande dataskyddsorganisation.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Bolagets skattning är något högre detta år jämfört med föregående och man ligger nu 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 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 att systematisk följa upp incidenter som en naturlig del i dataskyddsarbetet.

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

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 något högre på denna kontrollpunkt jämfört med tidigare år och bolaget ligger nu på nivå 3. Sammantaget indikerar skattningen att det inom ramen för kontrollpunkten har identifierats risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga.

Bolaget behöver däremot säkerställa att man har rutiner för att kontinuerligt genomföra efterlevnadskontroller av anlitade personuppgiftsbiträden och för att bedöma om andra överenskommelser/avtal behöver upprättas avseende gemensam/delad hantering av personuppgifter när en leverantör anlitas eller när samarbeten sker. Med hänsyn till att det har tecknats personuppgiftsbiträdesavtal med ca 75% av de som har bedömts utgöra personuppgiftsbiträden till bolaget, bör bolaget fortsätta att teckna dessa så att man når en nivå på 100%.

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 förbättring inom ramen för kontrollpunkten, men bolaget ligger överlag kvar på nivå 3. Sammantaget indikerar skattningen att det inom ramen för kontrollpunkten har identifierats risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga.

Det är positivt att bolaget har förbättrat sig avseende ansvarsfördelning angående uppdatering av behandlingarna i registret och att man nu anger att man använder registret som en del i det löpande dataskyddsarbetet. Eftersom bolaget angett att cirka 50% av bolagets behandlingar finns registrerade i registret enligt skattningen och att 50% av dessa innehåller den information som ska finnas med enligt art. 30 i GDPR, rekommenderar dataskyddsombudet att bolaget prioriterar arbetet med registret. Detta eftersom det är ett krav enligt artikel 30 i GDPR att den personuppgiftsansvariges samtliga behandling finns upptagna i registret, med fullständig information.

Vid avstämning med bolaget anges att förhoppningen är att den utvecklade dataskyddsorganisationen, med medarbetare ”långt ut” i verksamheten, ska förbättra bolagets användning av registret eftersom man då kan fånga upp samtliga av bolagets behandlingar på ett bättre sätt.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Bolagets skattning är oförändrad sedan föregående års skattning på denna kontrollpunkt och bolaget ligger kvar på nivå 3. Sammantaget indikerar skattningen att det inom ramen för kontrollpunkten har identifierats risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga.

Med hänsyn till hur flera av frågorna har besvarats bedömer dataskyddsombudet att det förefaller finnas risker inom ramen för kontrollpunkten. Bland annat bör det finnas skäl till att ha en övergripande strategi för arbetet med dataskydd och att systematiskt integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet. Det bör även finnas skäl att aktivt och medvetet arbeta riskbaserat och att säkerställa att man har rutiner för att efterleva GDPR:s krav vid olika sammankomster, såväl digitala som fysiska. Bolagets informationstillgångar bör även klassificeras utifrån *Konfidentialitet, Riktighet* och *Tillgänglighet* i enlighet med stadens styrande dokument. Bolaget har angett att cirka 50% av bolagets informationstillgångar har klassificerats.

Vid avstämning med bolaget framgår att det pågår ett aktivt arbete för att få till ett systematiskt arbetssätt och att integrera dataskyddsarbetet i det övergripande

informationssäkerhetsarbetet. Bolaget har anställt en IT-chef och man arbetar tillsammans för att inkludera dataskydd och informationssäkerhet tidigt i sina processer, vid inköp av nya IT-system osv.

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 lägre detta år än föregående, men ligger kvar på samma övergripande nivå (3). Sammantaget indikerar skattningen att det inom ramen för kontrollpunkten har identifierats risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga.

Fler än hälften av påståendena har dock besvarats med alternativet *nej, det stämmer inte bra*, vilket likt ovanstående kontrollpunkt indikerar att det finns risker som bör hanteras inom ramen för kontrollpunkten. Bolaget bör säkerställa att den allmänna kunskapsnivån i verksamheten höjs, samt ta fram rutiner för att följa upp och säkerställa att medarbetarnas kunskapsnivå bibehålls. Man bör även kartlägga vilken nivå av dataskyddskunskaper som olika befattningar bör ha och utformar utbildningar därefter.

Vid avstämning med bolaget framgår att åtgärder vidtas för att höja den allmänna kunskapsnivån. Det har nyligen genomförts utbildning för de personer som kommer ha ett större ansvar för bolagets dataskyddsarbete framåt. Bolaget har identifierat ett större utbildningsbehov för dessa, men kommer också att vidta åtgärder framöver för att höja den generella kunskapsnivån i bolaget.

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 ligger fortsatt på en hög nivå (4), men kontrollpunktens medelvärde har sjunkit något jämfört med tidigare år.

Efter att ha sett över bolagets externa integritetspolicy på en övergripande nivå anser dataskyddsombudet att årets skattning bättre speglar de faktiska omständigheterna än föregående års skattning och att det finns skäl att se till att

utövandet av bolagets informationsplikt förbättras. 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. Om personuppgifterna inte samlas in direkt från den registrerade så ska kategorierna av personuppgifter framgå, mottagare ska framgå och så även tydlighet kring tredjelandsöverföring och vad som gäller när det kommer till de registrerades rättigheter. 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. Dataskyddsombudet bedömer det som mycket tveksamt om hänvisning till dokumenthanteringsplan som den registrerade inte har tillgång till kan anses tillräckligt. Bolaget bör även säkerställa att rättslig grund framgår för respektive behandling. En ordentlig översyn av helheten bör genomföras kontinuerligt, inte minst med hänsyn till den omfattande praxis som nu finns kopplat till informationsplikten och som kontinuerligt fortsätter att komma.

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 mycket positivt att bolaget jämfört med föregående år nu anger att de informerar registrerade om hur deras personuppgifter behandlas vid första kontakt via e-post. Bolaget behöver dock arbeta vidare med informationsklassificeringen av sina personuppgiftsbehandlingar (dock bra att man säkerställt att tidigare klassificeringar är aktuella). Bolaget behöver också säkerställa att det finns rutiner och anvisningar för hantering av personuppgifter i e-post, se till att personuppgifter gallras enligt gällande gallringsbeslut och att man informerar medarbetare om dokumenthantering och gallring i förhållande till kraven i GDPR.

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. Resultatet ligger dock väldigt nära nivå 2, vilket innebär att det inom ramen för kontrollpunkten kan finnas risker som behöver åtgärdas inom en snar framtid.

Resultatet av skattningen på de 14 frågorna under kontrollpunkten är splittrat, bolaget anger att ett flertal rutiner finns på plats. Exempelvis för att identifiera behandlingar med hög risk, inhämta dataskyddsombudets synpunkter efter utförd tröskelanalys och konsekvensbedömning, genomföra och dokumentera konsekvensbedömningar och för att bedöma risker för de registrerade. Bolaget uppger samtidigt att det saknas rutiner för att säkerställa att konsekvensbedömningar genomförs innan riskfyllda behandlingar påbörjas och för att hålla konsekvensbedömningar uppdaterade vid förändringar i behandlingen, samt för hur beslut om accepterande av risker i en konsekvensbedömning ska fattas och dokumenteras. Vidare anges att bolaget enbart har bedömt om en konsekvensbedömning behöver utföras för cirka 25% av sina personuppgiftsbehandlingar och att konsekvensbedömningar utförts för cirka 0% av de behandlingar där det sannolikt behöver utföras en sådan.

Med hänsyn till ovanstående rekommenderar dataskyddsombudet att arbetet med denna kontrollpunkt prioriteras.

Vid avstämning med bolaget anges att en genomgång av genomförda konsekvensbedömningar har gjorts, men att de i flera fall är genomförda på ett sätt som gör att bolaget inte kan anse att de uppfyller kraven på vad en konsekvensbedömning ska innehålla. På en koncerngemensam nivå där bolagens dataskyddskontakter arbetar gemensamt med konsekvensbedömningar pågår ett intensivt arbete för att utföra och komma i kapp med konsekvensbedömningsarbetet. Dataskyddsombudet instämmer i bedömningen att arbetet med konsekvensbedömningar går framåt. En viktig fråga som både bolaget och dataskyddsombudet ser behöver åtgärdas är den om beslutsmandat och att det är tydligt vem som får fatta beslut om inledning av behandling osv.

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. Det innebär att man landar på nivå 2, men mycket nära nivå tre. Resultatet indikerar att det inom ramen för kontrollpunkten finns risker identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder. Samtliga av påståendena har besvarats med alternativet *Nej, stämmer inte bra*, vilket innebär att bolaget fortsatt har ett behov av att säkerställa 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 behöver det även tas med i kravställningen att det finns en anpassning till inbyggt dataskydd och dataskydd som standard.

Verksamheten bör även ha som rutin att dataskyddsombudet involveras från start i dessa processer.

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 något högre än föregående år, men ligger ändå kvar på nivå 3. Sammantaget indikerar skattningen att det inom ramen för kontrollpunkten har identifierats risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga.

Bolaget behöver fortsatt 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. Bolaget behöver även säkerställa att dataskyddsperspektivet beaktas vid införandet och användandet av kostnadsfria tjänster, såsom gratisappar och sociala medier.

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 bolaget policy anges att enbart nödvändiga cookies för hemsidans funktionalitet samlas in. Nödvändiga cookies kräver inget samtycke enligt lagen (2022:482) om elektronisk kommunikation för att få samlas in (tidigare SFS 2003:389). Bolaget efterfrågar dock besökarens

samtycke/godkännande för användningen av cookies, vilket riskerar bli missvisande.

Vid kontroll av bolagets hemsida framgick att det låg en del tredjepartsförfrågningar som riskerade medföra risk för tredjelandsöverföring, bland annat Google Analytics.

Vid avstämning med bolaget angavs att bolaget snarast skulle se över såväl sin cookie-banner och användningen av tredjepartsförfrågningar, vilket dataskyddsombudet uppfattar nu är gjort och åtgärdat.

Avseende sociala medier så använder bolaget såväl Facebook som LinkedIn. 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 i 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 och LinkedIn.

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. Det är positivt att bolaget, enligt svaren på frågorna, nu har en rutin för att hantera ett tillbakadraget samtycke från en registrerad. Enligt skattningen behöver bolaget enbart arbeta vidare med att ta fram en rutin för att bedöma om när en invändning mot en personuppgiftsbehandling från en registrerad är uppenbart ogrundad eller orimlig.

Dataskyddsombudet har ingen anledning att ifrågasätta bolagets skattning, men har inte heller kontrollerat arbetet särskilt i en fördjupad kontroll eller liknande.

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 förvaltningen/bolaget under 2023 prioriterar följande delar av dataskyddsarbetet:

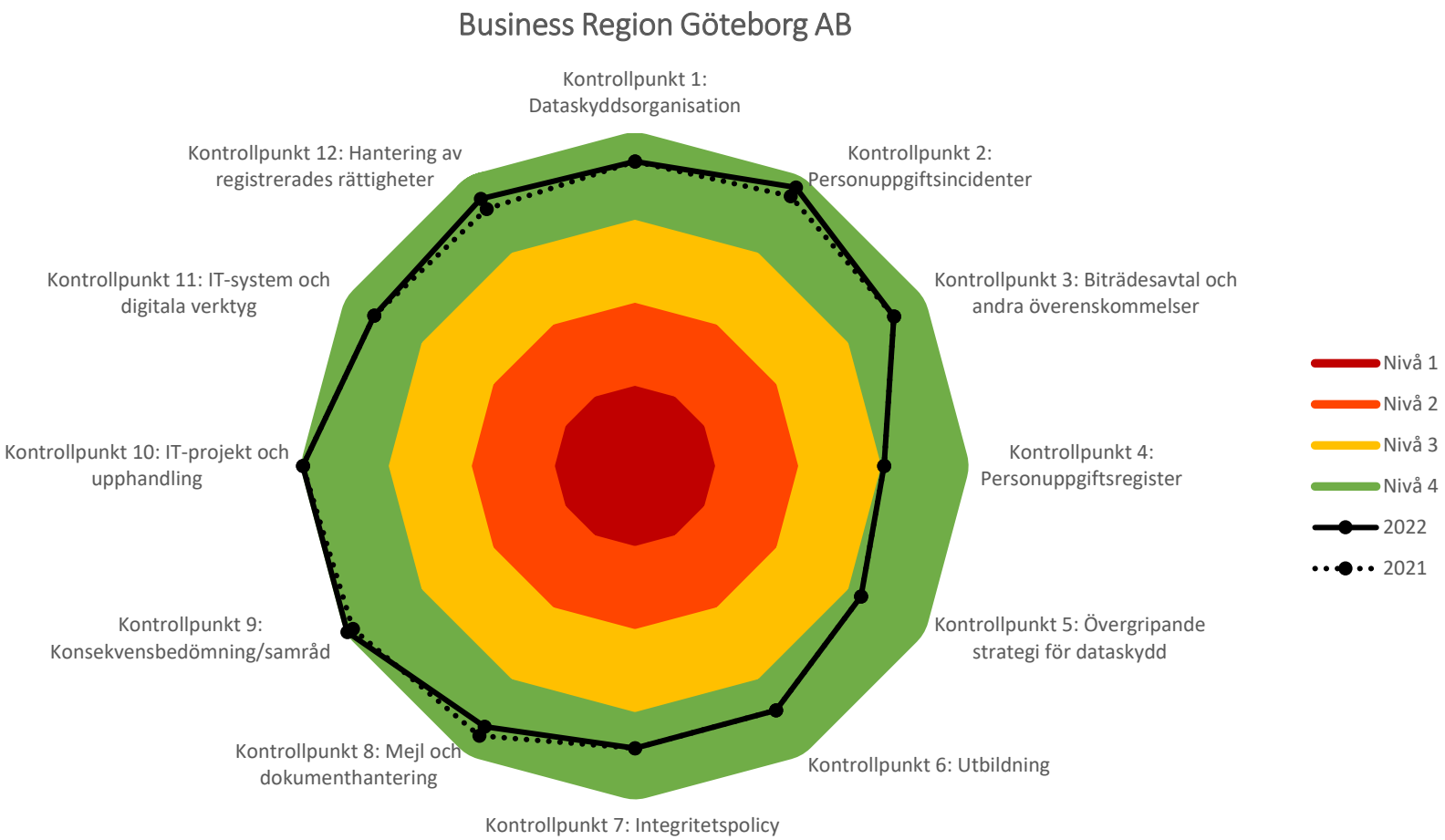
- Kontrollpunkt 1: Dataskyddsorganisation
- Kontrollpunkt 9: Konsekvensbedömning/samråd
- Kontrollpunkt 10: IT-projekt och upphandling

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 Göteborgs Bostads AB (Bostadsbolaget)

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.

Bostadsbolagets användning av kamerabevakning

Bolaget bedriver kamerabevakning i anslutning till tre garage i staden i syfte att verka brottsförebyggande och upprätthålla allmän ordning. Något tillstånd för övervakningen har inte sökts.

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 då bolagets övervakning inte är tillståndspliktig. 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 hur bolagets underlag (som i övrigt är väldigt bra) för kamerorna är utformade är det dock otydligt för läsaren på vilken grund bolaget bedömer att bevakningen inte kräver tillstånd. Sammantaget förstår och instämmer dataskyddsombudet i att de bevakningar bolaget har idag sannolikt inte är tillståndspliktiga, men i underlaget blev det otydligt på vilken grund. Detta då det hänvisas dels till att allmänheten inte har tillgång, vilket skulle innebära att bevakningen inte är tillståndspliktig enligt 7 § kamerabevakningslagen, och dels till att undantaget till tillståndskravet i 9 § 8 kamerabevakningslagen är tillämpligt. Bolaget rekommenderas förtydliga detta och dataskyddsombudet vill även skicka med att undantaget i 9 § 8 p. kamerabevakningslagen om att bevakning i ett parkeringshus, om bevakningen har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott, ej är tillståndspliktig, enbart gäller för parkeringshus med plats för bilar och andra fordon som är upplåtna för allmänheten. Bestämmelsen tar inte sikte på kamerabevakning i inomhusparkeringar, till vilka allmänheten inte har tillträde, exempelvis garage för boende i en bostadsrättsförening. Utifrån detta överväger dataskyddsombudet om undantaget verkligen är tillämpligt för bevakningen på Rundbäcksgatan och Gamla Tuvevägen, men däremot för Landala då det delvis finns platser för besökare där. Däremot är ju kamerabevakningen sannolikt inte tillståndspliktig för Rundbäcksgatan eller Gamla Tuvevägen heller, men på grund av att allmänheten inte har tillträde dit.

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.

Bostadsbolaget bedriver kamerabevakning på tre platser i Staden, Rundbäcksgatan, Gamla Tuvevägen och i Landala, samtliga i anslutning till parkeringsgarage. Områden

som övervakas är in och utfart, garageport samt P-ytor. på Gamla Tuvevägen övervakas också ett cykelrum. Områdena bevakas dygnet runt.

Utifrån den information som dataskyddsombudet har tagit del av förefaller det rimligt, med hänsyn till ändamålet med kamerabevakningen, att bevakningen sker dygnet runt och på det sätt som sker.

Avseende lagringstid har bolaget uppgett att lagring sker i 21 dagar. Huvudregeln för inspelat material är att det får lagras i 72h, vilket gör att bolagets lagringstid klart överstiger huvudregeln. Det är dock möjligt att frångå huvudregeln om det finns skäl för det, men man 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 angett att det kan dröja några veckor innan bolaget får vetskap om att en incident har inträffat eftersom bevakningen sker i en miljö där personer rör sig mindre frekvent och under kortare tidsperioder. Även semestertider eller långhelger kan medföra fördröjd upptäckt. Vid upptäckt tar det ca 1-2 dagar för behörig personal att ta fram det inspelade materialet och överlämna det till polisen. Polisen kan dessutom ha lång handläggningsperiod för händelser i parkeringshus. Bolaget har sammantaget bedömt att 21 dagar är en väl avvägd tid för lagring av materialet.

Dataskyddsombudet instämmer delvis i bolagets bedömning och anser att en längre lagringstid än huvudregeln på 72h får anses vara berättigad. 21 dagar är dock ett stort avsteg från huvudregeln och även om dataskyddsombudet har förståelse för att det kan ta tid att upptäcka incidenter så bör de ytor som kamerabevakningen sker på (infart/utfart och p-ytor) trots allt beträdas relativt frekvent. Polisens handläggningstid bör inte ha någon relevans för den allmänna lagringstiden. Att särskilja och omhänderta det material som visar en incident och att lagra detta material en längre tid får dock anses befogat.

Sammantaget rekommenderar dataskyddsombudet att den generella lagringstiden ses över ytterligare för att säkerställa att den verkligen är befogad i förhållande 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.

Bostadsbolaget har angett att ändamålet med behandlingen är dels att den ska verka brottsförebyggande och därvid leda till att bolagets kostnader för exempelvis skadegörelse eller inbott ska minska, dels att allmän ordning ska kunna upprätthållas och att kamerabevakningen ska utgöra en trygghetsskapande åtgärd för de boende i fastigheterna.

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 och har även tillhandahållit de intresseavvägningar som genomförts. Dataskyddsombudet har inga invändningar mot bolagets bedömning.

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 inte genomfört någon konsekvensbedömning avseende den kamerabevakning som man bedriver. Bolaget uppger dock att det har utförts en inventering av samtliga anläggningar för att kontrollera dem enligt Framtidenkoncernens anvisning för kamerabevakning och har nyligen färdigställt dokumentation för samtliga anläggningar i drift.

Vidare uppges att i samband med att en kamerabevakningsanläggning ska tas i drift utförs en analys för att se att det finns en tydlig problembild som inte blivit avhjälp av andra mindre integritetskänsliga åtgärder, vilka ytor som kommer övervakas, vilken typ av teknik som kommer användas och hur omfattande övervakningen kommer att vara. I den analysen bedömer bolagets dataskyddskontakt om det vore lämpligt att genomföra en konsekvensbedömning. Denna bedömning, om konsekvensbedömning ska göras, dokumenteras i analysmallen. Befintliga anläggningar är värderade utifrån ovanstående analysmall/beslutsmall.

Dataskyddsombudet finner det positivt att en bedömning av om en konsekvensbedömning bör genomföras eller ej görs inför att en kamerabevakningsanläggning ska tas i drift och att det också noteras. Det enda medskick dataskyddsombudet vill göra är att det kan vara fördelaktigt att dokumentera bedömningen ytterligare än vad som redan görs utifrån de kriterier som avgör om en konsekvensbedömning ska göras eller inte enligt art. 35 GDPR. Detta för att på så vis kunna påvisa på vilka grunder bedömningen görs. Bolaget bör särskilt bedöma om kamerabevakningen i Landala medför behov av konsekvensbedömning, då allmänheten till viss del förefaller vistas där.

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, systemet som används på samtliga anläggningar heter Milestone, all video lagras endast lokalt på inlåsta servrar och raderas automatiskt efter aktuell tidsbegränsning. Endast bild spelas in. Leverantör för samtliga anläggningar är Låsteam (tidigare Vindico). Personuppgiftsbiträdesavtal har tecknats med 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 varningsskylt 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. I samband med att man inventerar sina behandlingar kommer också nya skyltar med information att sättas upp i anslutning till de platser som kamerabevakas. Bolaget har bifogat underlag som visar hur dessa kommer att utformas.

Dataskyddsombudet har inget att invända mot i utformningen av de skyltar som sätts upp, utan anser att de fungerar väl med hänseende till information i flera lager. Informationen på hemsidan kan med fördel förtydligas avseende lagringstid då informationen är mycket allmänt hållen, vilket kan innebära svårighet för den registrerade att avgöra vad som är korrekt information. Om det finns flera bevakningar med olika lagringstid har dataskyddsombudet förståelse för att det är svårt att ange specifik lagringstid på hemsidan. I sådana fall kan det räcka att tydligt ange att lagringstiden anges vid aktuell bevakning och kan variera mellan exempelvis 72 timmar och fem dagar beroende på de bedömningar som har gjorts för olika bevakningar. I och med att Bostadsbolaget enbart har tre bevakningar och att samtliga har samma lagringstid bör informationen på hemsidan kunna specificeras.

Sammanfattade rekommendationer (punktform)

- Förtydliga bedömningen kring varför bevakningen inte är tillståndspliktig i bolagets underlag.
- Se över den generella lagringstiden ytterligare för att säkerställa att den verkligen är befogad i förhållande ändamålen och omständigheterna kring hur lång tid det tar att upptäcka och hantera en incident.
- Förtydliga informationen om lagringstid på hemsidan.

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.

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.
    - **Uppföljande fråga:** Har bolaget genomfört en bedömning av om personuppgiftsbehandlingarna som sker genom kamerabevakning uppfyller kraven för när en konsekvensbedömning ska utföras? Om ja, bifoga bedömningen. Om nej, varför inte?
3. Vilken teknik använder ni och vilka leverantörer använder ni?
    a) Finns personuppgiftsbiträdesavtal upprättade med de leverantörer som ni använder? Bifoga dessa avtal.
        - **Uppföljande frågor:** Är det enbart bild som spelas in? Förekommer även ljudupptagningar?
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 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 10 juni 2022.**

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