Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Förvaltnings AB Göteborgslokaler

2022-12-28

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 ett behov av att se över lagringstiden av inspelat material, säkerställa dokumentation av bedömningen kring rättslig grund och att säkerställa att upprättat personuppgiftsbiträdesavtal med leverantören

innehåller samtliga kriterier som ett personuppgiftsbiträdesavtal ska innehålla. Bolaget bör även bedöma om konsekvensbedömning bör utföras för de behandlingar där det inte har gjorts samt säkerställa att dataskyddsombudets rekommendationer inhämtas vid genomförande av konsekvensbedömningar eller tröskelanalyser.

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 Göteborgslokalers 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

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

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:

Bolaget har skattat sig betydligt högre på denna kontrollpunkt än föregående år. Samtliga påståenden har besvarats med alternativet *Ja, det stämmer helt*, vilket innebär att bolaget anser 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 med dataskyddsfrågor.

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

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Bolagets skattning är betydligt högre detta år än föregående. Skattningen indikerar att det inom ramen för kontrollpunkten inte föreligger några risker av betydelse och bolaget anser att de arbetar på ett systematiskt vis med personuppgiftsincidenter.

I och med att bolaget har svarat att samtliga påståenden stämmer helt, anser bolaget att arbetet med incidenthantering fungerar mycket väl.

Enligt avstämning med bolaget har det enbart skett en personuppgiftsincident under 2022. Incidenten anmäldes till Integritetsskyddsmyndigheten. Med hänsyn till att tröskeln för när en personuppgiftsincident har skett är låg och att personuppgiftsincidenter förekommer även i organisationer som har mycket väl

utvecklade rutiner för att förhindra att personuppgiftsincidenter sker, bedömer dataskyddsombudet det som osannolikt att enbart en incident har skett under 2022. Det kan snarare vara så att ett visst antal incidenter är ett slags ”friskhetstecken” och indikerar att den aktuella verksamheten har goda rutiner för att upptäcka incidenter och att medarbetare är medvetna om vad som utgör en incident och hur de ska rapportera den. Mot denna bakgrund rekommenderas bolaget att utvärdera om rutinerna och den allmänna medvetenheten hos medarbetarna ger tillräckligt goda förutsättningar för att hantera eventuella incidenter

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:

Skattningen indikerar att det inom ramen för kontrollpunkten inte föreligger några risker av betydelse och att bolaget arbetar på ett systematiskt vis. Skattningen är betydligt högre detta år än föregående och bolaget hamnar på nivå 4.

Bolaget anger att de har rutiner för att göra efterlevnadskontroller av leverantör som biträdesavtal har upprättats med, att det finns rutiner och kompetens att bedöma personuppgiftsansvar, samt att det finns rutiner och kompetens för att kontrollera hela kedjan av underbiträden till en leverantör. Bolaget anger också att biträdesavtal är upprättade för samtliga behandlingar där så krävs.

Dataskyddsombudet har inga invändningar mot bolagets skattning, men har heller inte kontrollerat bolagets rutiner inom ramen för denna kontrollpunkt i en fördjupad kontroll.

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:

Bolaget har skattat sig betydligt högre på denna kontrollpunkt än föregående år och hamnar nu på nivå 4. Enligt bolagets skattning föreligger alltså inga risker av betydelse inom ramen för kontrollpunkten och bolaget anser sig arbeta systematiskt med sitt personuppgiftsregister.

Bolaget har enligt skattningen rutiner på plats för tydlig ansvarsfördelning för registret och att uppdatera det. Bolaget anger också att den interna dataskyddsorganisationen använder registret som en del i det dagliga arbetet.

Skattningen visar dock att bolaget behöver fortsätta registrera sina behandlingar i registret då det anges att cirka 75% av bolagets behandlingar finns med. Eftersom det anges att 75% av de registrerade behandlingarna innehåller det som de ska enligt art. 30 GDPR, så behöver även detta arbete förbättras. Detta eftersom en personuppgiftsansvarigs samtliga behandlingar ska finnas med i registret och innehålla all information som krävs enligt art. 30 i GDPR.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Bolaget har besvarat samtliga påståenden utom ett med alternativet *Ja, det stämmer helt* eller *ja, det stämmer bra,* vilket innebär att bolaget anser sig bedriva ett mycket gott arbete kopplat till övergripande strategi för dataskydd och man hamnar på nivå 4. Skattningen innebär en stor förbättring från föregående år och indikerar att det inom ramen för kontrollpunkten inte förekommer några risker av betydelse inom ramen för kontrollpunkten.

Enligt skattningen finns det flera rutiner på plats för att säkerställa att styrande dokument som innehåller bestämmelser om personuppgifter uppdateras. Det finns också rutiner för att efterleva GDPR:s krav vid fysiska och digitala sammankomster och bolaget har såväl en informationssäkerhetspolicy som en övergripande strategi för arbetet med dataskydd och att integrera frågorna i det övriga informationssäkerhetsarbetet. Bolaget anger också att samtliga informationstillgångar har identifierats och värderats enligt *Konfidentialitet*, *Riktighet* och *Tillgänglighet* utifrån stadens riktlinjer.

Dataskyddsombudet har ingen anledning att göra en annan bedömning än bolaget, men har inte heller involverats i denna typ av frågor under 2022 eller kontrollerat bolagets rutiner inom ramen för en fördjupad kontroll.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Bolagets skattning detta år är betydligt högre än föregående och bolaget hamnar nu på nivå 4. Enligt bolagets skattning föreligger alltså inga risker av betydelse inom ramen för kontrollpunkten. I och med att samtliga påståenden har besvarats med alternativet *Ja, det stämmer helt* eller *Ja, det stämmer bra*, anser bolaget att de arbetar väl med att utbilda sin personal och att kunskapsnivån i bolaget är hög.

Bolagets svar på enkäten i denna punkt 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 kunskap om tillvägagångssätt när registrerade utövar sina rättigheter i förhållande till bolaget. Dataskyddsombudet har inte fått några direkta indikationer som medför en annan bedömning. I och med att det exempelvis enbart rapporterats en personuppgiftsincident under 2022, kan det dock föreligga utbildningsbehov inom vissa områden som bör ses över.

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 på en hög nivå (4). Skattningen är högre än föregående år. Samtliga påståenden har besvarats med alternativet *Ja, det stämmer helt* eller *Ja, det stämmer bra*. Enligt bolagets skattning föreligger alltså inga risker av betydelse inom ramen för kontrollpunkten.

Efter att ha sett över bolagets externa integritetspolicy på en övergripande nivå bedömer dataskyddsombudet att det finns skäl att se till att utövandet av informationsplikten 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. 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 tredjelandsöverföringar som sker.

Även om mycket av ovanstående finns med i policyn så bör bolaget se över exempelvis hur man informerar om rättslig grund och ändamål med behandlingarna och de rättigheter som den registrerade har kopplat till en specifik behandling. Idag används en del bestämningsord såsom ”exempelvis” och liknande ord, vilket risker medföra en otydlighet. Integritetspolicyn bör vara så specifik som möjligt och dataskyddsombudet rekommenderar därför att bolaget ser över sin policy utifrån lagkrav, praxis och vägledningar. Dataskyddsombudet kan såklart bistå med rådgivning.

Sammantaget gör dataskyddsombudet bedömningen att bolagets skattning avseende att bolagets informationsplikt är uppfylld är för hög.

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:

Enligt bolagets skattning föreligger alltså inga risker av betydelse inom ramen för kontrollpunkten och bolaget anser sig arbeta systematiskt med e-post och dokumenthantering. Bolagets skattning är betydligt högre än föregående år.

Enligt skattningen har bolaget ordning på sin hantering av personuppgifter i e-post och man har fungerande rutiner för gallring och övrig dokumenthantering, samt informerar sina medarbetare om korrekt dokumenthantering och gallring kopplat till GDPR.

Enligt skattningen är cirka 50% av bolagets personuppgiftsbehandlingar klassificerade i enlighet med stadens styrande dokument och cirka 100% av dessa är kontrollerade för aktualitet det senaste året. Bolaget bör fortsätta med klassificeringen så att samtliga personuppgiftsbehandlingar klassificeras.

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 hamnar detta år på nivå 3. Detta indikerar att det inom ramen för kontrollpunkten föreligger risker som behöver åtgärdas, men som ej bedöms brådskande, omfattande eller allvarliga.

Bolagets skattning innebär att många efterfrågade rutiner finns på plats. Det finns, enligt skattningen, rutiner för att identifiera behandlingar med hög risk, inhämta dataskyddsombudets synpunkter vid konsekvensbedömning, genomföra och dokumentera konsekvensbedömningar innan behandlingarna påbörjas, uppdatera konsekvensbedömningar vid förändringar i behandlingen och för att bedöma risker för de registrerade. Det finns även rutiner för hur beslut inom ramen för en konsekvensbedömning ska fattas och dokumenteras. Bolaget anger också att det finns rutiner för att säkerställa att identifierade behov av åtgärder i en konsekvensbedömning genomförs.

Skattningen visar dock att bolaget bör arbeta vidare med bedömningar av om deras personuppgiftsbehandlingar behöver konsekvensbedömas, även om det är ett gott betyg att 75% av behandlingarna har bedömts. Eftersom bolaget anger att konsekvensbedömningar har utförts för cirka 75% av de behandlingar där det bedömts behövas, bör även detta arbete fortlöpa för att säkerställa att konsekvensbedömningar genomförs för samtliga behandlingar med höga risker.

Bolaget bör även säkerställa att det finns rutiner för att inhämta de registrerades synpunkter vid en konsekvensbedömning (där det bedöms lämpligt) och att involvera dataskyddsombudet redan i bedömningen av om en konsekvensbedömning bör genomföras eller ej.

Dataskyddsombudet har under 2022 inte involverats i någon konsekvensbedömning som är specifik för Göteborgslokaler, men däremot i konsekvensbedömningar för koncerngemensamma behandlingar.

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 ligger enligt sin skattning på nivå 4, vilket är en stor förbättring jämfört med föregående år då bolaget inte kunde besvara frågorna i 2021 års kontroll. Enligt bolagets skattning föreligger alltså inga risker av betydelse inom ramen för kontrollpunkten och bolaget anser sig arbeta systematiskt med dataskydd kopplat till IT-projekt och upphandling.

Enligt skattningen finns dataskyddsperspektivet 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. Bolaget saknar däremot rutin för att involvera dataskyddsombudet från start i dessa processer.

Dataskyddsombudet har inte blivit involverad i frågor kopplade till kontrollpunkten under 2022 och kan därför inte avgöra om bolagets skattning är korrekt, förutom i just den del som avser att dataskyddsombudet inte involveras. Bolaget bör säkerställa att dataskyddsombudet involveras i dessa frågor.

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 mycket högre än föregående år då bolaget inte kunde besvara frågorna i 2021 års kontroll. Bolaget ligger nu på nivå 4. Bolagets skattning antyder alltså att man arbetar systematiskt med dataskydd kopplat till IT-system och digitala tjänster och att inga risker av betydelse finns inom ramen för kontrollpunkten.

Bolaget har, enligt skattningen, goda rutiner för sin behörighetsstyrning. Det finns också dokumentation över samtliga IT-system, digitala tjänster och kommunikationskanaler. Bolaget har, enligt skattningen, väl fungerande rutiner för användningen av gratisappar och sociala medier.

Bolaget har också 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. Enligt bolagets policy används såväl nödvändiga cookies för hemsidans funktionalitet som icke-nödvändiga cookies såsom för statistik. För att få samla in nödvändiga cookies krävs inget samtycke enligt lagen (2022:482) om elektronisk kommunikation (tidigare SFS 2003:389), men det krävs däremot för insamling av icke nödvändiga. Bolaget har en cookie-ruta som gör det lika lätt att avvisa cookies som att godkänna dem, vilket dataskyddsombudet finner positivt. Bolaget bör dock se över den informationstext som anges i anslutning till cookie-rutan, eftersom det där anges att besökaren anses godkänna användningen av cookies om denne fortsätter använda hemsidan. Detta riskerar bli motstridigt, då det för icke nödvändiga cookies krävs ett aktivt samtycke.

Vid kontroll av bolagets hemsida förekommer dock ett flertal 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 och Instagram som LinkedIn.

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 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. Bolaget bör vidta åtgärder för att inte bryta mot förordningens bestämmelser användningen av Facebook, Instagram och LinkedIn. Dataskyddsombudet noterar att personuppgifter, bland annat i form av bilder på personer, 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 på nivå 4 enligt årets skattning, vilket är en betydande förbättring från föregående år. Samtliga påståenden har besvarats med alternativet *Ja, det stämmer helt*, förutom ett som har besvarats med *Ja, det stämmer bra.* Enligt bolagets skattning föreligger alltså inga risker av betydelse inom ramen för kontrollpunkten och bolaget anser sig arbeta systematiskt med hanteringen av registrerades rättigheter.

Dataskyddsombudet har ingen anledning att göra en annan bedömning än bolaget, 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:

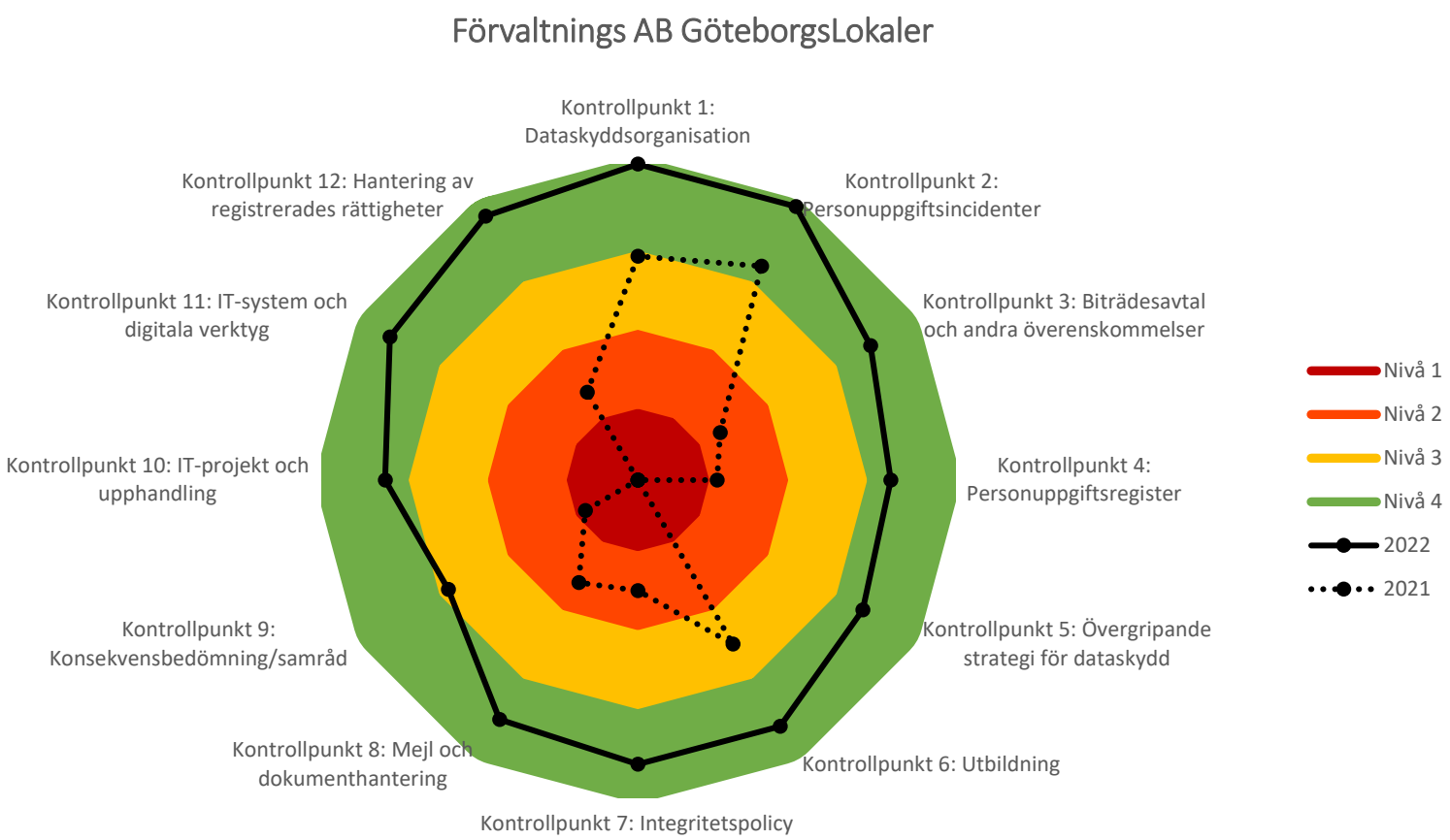
- Kontrollpunkt 7: Integritetspolicy.
- Kontrollpunkt 9: Konsekvensbedömning/samråd.
- Kontrollpunkt 11: IT-system och digitala verktyg.

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 Göteborgslokaler

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.

Göteborgslokalers användning av kamerabevakning

Bolaget bedriver kamerabevakning på sju adresser i staden i syfte att förebygga brott och öka tryggheten. Tillstånd för övervakningen har sökts och erhållits för två av de sju platserna. Tre av platserna var tidigare anmälningspliktiga till Länsstyrelsen.

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 tillstånd har sökts och erhållits för kamerabevakningen på Vårväderstorget (ute) och Tuve Torg. Bevakningen på Vårväderstorget (inne), Höstvädersgatan och Blåsvädersgatan omfattades i tidigare lagstiftning av anmälningsplikt till Länsstyrelsen. Med nuvarande lagstiftning är detta krav borttaget och bevakningen är enligt bolaget inte heller tillståndspliktig. Även bevakningen i Rannebergen och Selma Lagerlöfs torg bedöms vara icke tillståndspliktig.

Vid avstämning med bolaget framgår att kamerabevakningen i Rannebergen är borttagen.

Dataskyddsombudet tolkar det underlag som översänts som att bolaget bedömer att bevakningarna på Vårväderstorget (inne), Höstvädersgatan och Blåsvädersgatan inte är tillståndspliktiga utifrån undantaget till tillståndsplikten i 9 § 8 p. kamerabevakningslagen. Undantaget innebär 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. Bestämmelsen tar sikte på just parkeringshus där det finns parkeringsplatser som är upplåtna för allmänheten. Den omfattar inte parkeringsplatser i byggnader dit allmänheten inte har tillträde. Sådana parkeringar blir snarare inte tillståndspliktiga utifrån bestämmelsen i 7 § kamerabevakningslagen. Bolagets bedömning kring tillstånd för Selma Lagerlöfs torg är inte lika tydlig som för ovanstående bevakningar. Bolaget anger dock att omständigheterna kring bevakningen i parkeringshuset på Selma Lagerlöfs torg i stort är desamma som för Vårväderstorget, Höstvädersgatan och Blåsvädersgatan. Det framgår också i underlaget att allmänheten förefaller ha tillträde till parkeringshuset.

Utifrån det material som dataskyddsombudet tagit del av instämmer dataskyddsombudet i bolagets bedömning att kamerabevakningen där det i dag saknas tillstånd sannolikt inte är tillståndspliktig i enlighet med 9 § 8 p. kamerabevakningslagen.

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 bolaget kan visa att ett behov finns.

Göteborgslokaler bedriver kamerabevakning på sju platser i staden, Vårväderstorget, Vårvärderstorget (inne), Tuve torg, Höstvädersgatan, Blåsvädersgatan, Rannebergen och Selma Lagerlöfs torg. Bevakningarna på Höstvädersgatan (ute) och Tuve torg sker utomhus och är placerade på portiker respektive fasader. Bevakningarna på Höstvädersgatan (inne), Blåsvädersgatan och Selma Lagerlöfs torg sker i parkeringshus (in- och utfart samt del av parkeringsplatser). Kamerabevakningen sker dygnet runt i parkeringshusen på Selma Lagerlöfs torg och på Vårväderstorget. För övriga platser sker bevakningen mellan kl. 18:00 och 06.00 och i ett fall mellan kl. 20.00 och 08.00.

Utifrån den information som dataskyddsombudet har tagit del av förefaller det inte orimligt, med hänsyn till ändamålet med kamerabevakningen, att bevakningen sker på så vis som anges.

Avseende lagringstid har bolaget uppgett att lagring sker i 30 dagar. För den bevakning som sker med tillstånd bestäms lagringstiden av tillståndet. Underlaget för tillståndet har dock inte översänts till dataskyddsombudet. Huvudregeln för inspelat material är att det får lagras i 72 timmar, vilket gör att bolagets lagringstid 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 i vissa underlag angivit att semestertider och därmed svårighet att få ut materialet genom den person eller de personer som har tillgång till materialet, bidrar till den längre lagringsperioden.

Dataskyddsombudet förstår att en längre lagringstid än huvudregeln på 72 timmar kan vara berättigad. 30 dagar är dock ett stort avsteg från huvudregeln. Framför allt bör bolaget dokumentera och argumentera för sin bedömning av lagringstiden mer utförligt. Även om semesterperioder såklart kan ha viss betydelse så bör det inte vara avgörande för bedömningen. Enligt dataskyddsombudet kan det, på grund av semesterperioder inte anses nödvändigt att ha en så pass lång generell lagringstid som bolaget har. 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 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 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.

Göteborgslokaler har angett att ändamålet med behandlingen är att förebygga brott och öka tryggheten. Ändamålet anges också vara att fullgöra ett brottsbekämpande uppdrag. Dataskyddsombudet har i stort inga invändningar mot de ändamål som anges, men vill förtydliga att bolaget mycket väl kan använda ändamål som trygghetsskapande och brottsförebyggande, men bör vara försiktiga med att uttrycka att de har ett *brottsbekämpande* uppdrag.

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, men det framgår också att tillsynsmyndigheten har bedömt att bolaget utför en uppgift av allmänt intresse i samband med de tillståndspliktiga bevakningarna. Dataskyddsombudet har idag inga invändningar mot bolagets bedömning, men bolaget bör säkerställa att de noggrant har dokumenterat den intresseavvägning som ligger till grund för bedömningen av den rättsliga grunden för respektive kamerabevakning. I underlaget som dataskyddsombudet tagit del av finns en intresseavvägningsbedömning för kamerabevakningen i parkeringshusen på Vårväderstorget, Blåsvädersgatan och Höstvädersgatan. Om det inte redan finns bör bolaget säkerställa att det finns för samtliga bevakningar.

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.

Konsekvensbedömning har utförts för kamerabevakningen i parkeringshusen på Vårväderstorget, Blåsvädersgatan och Höstvädersgatan. Bolaget har angett att behovs- och riskanalys har gjorts av leverantören när det kommer till bevakningen av parkeringshuset på Selma Lagerlöfs torg samt att ovanstående konsekvensbedömning bör vara tillämplig även för Selma Lagerslöfs torg då omständigheterna i stort är desamma.

Dataskyddsombudet finner det positivt att det för flera bevakningar finns en genomförd konsekvensbedömning. Eftersom underlaget innehåller en bedömning att konsekvensbedömningen inte behöver stämmas av med dataskyddsombudet på grund av att dataskyddsförordningen inte hade trätt i kraft när kamerabevakningen inleddes, vill dock dataskyddsombudet påpeka att när dataskyddsombudet inte involveras i en konsekvensbedömning kan den inte anses fullständig eller färdigställd. Den personuppgiftsansvarige ska alltid involvera dataskyddsombudet vid utförandet av en konsekvensbedömning enligt art. 35.2 GDPR. Detta gäller oavsett om behandlingen av personuppgifter inleddes före eller efter att dataskyddsförordningen trädde i kraft. Dataskyddsombudet rekommenderar därför att bolaget säkerställer att dataskyddsombudets rekommendationer inhämtas. Bolaget bör även bedöma om konsekvensbedömning behöver utföras för bevakningen på Selma Lagerlöfs torg. Den behovs- och riskbedömning som genomförts av leverantören är inte en konsekvensbedömning och bolaget bör i stället uppta behandlingen i redan upprättade konsekvensbedömningar eller upprätta en egen för Selma Lagerlöfs torg (om bolaget bedömer att en konsekvensbedömning ska genomföras).

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 systemet som används på anläggningarna heter Avigilon Control Centre 5 (Milestone). All video lagras endast lokalt men driftas av leverantören Safeteam. Materialet raderas automatiskt efter 30 dagar. Endast bild spelas in. Enligt underlagen har enbart leverantören tillgång till och kan plocka ut materialet.

För bevakning som omfattas av kamerabevakningslagen gäller sekretess för uppgift om enskilds personliga förhållanden som inhämtats genom kamerabevakning i enlighet med 32 kap. 3 § offentlighets- och sekretesslagen (2009:400), OSL. Dataskyddsombudet vill därför göra ett medskick till bolaget om att det bör säkerställas att leverantörens tillgång till materialet är förenlig med OSL, om så inte redan gjorts.

Leverantörer för anläggningarna heter Vindico AB och Safeteam. Personuppgiftsbiträdesavtal har tecknats med Safeteam. Dataskyddsombudet noterar dock att det är ett äldre avtal och att det kan behöva ses över så att samtliga kriterier som ett personuppgiftsbiträdesavtal ska innehålla sedan GDPR trädde i kraft finns med. Avseende Vindico AB tolkar dataskyddsombudet det som att denna leverantör enbart levererar och underhåller utrustning, men inte behandlar några personuppgifter för bolagets räkning, varför personuppgiftsbiträdesavtal inte har upprättats.

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 informerar i ett första informationslager genom skyltning där kamerabevakningen sker. Bolaget har bifogat underlag som visar hur skyltarna utformas. Information finns också på bolagets hemsida och hänvisas till via skyltarna.

Dataskyddsombudet har inget att invända mot i utformningen av de skyltar som sätts upp, utan anser att de fungerar väl med hänseende till att den information som ska lämnas i det första informationslagret finns med.

Sammanfattade rekommendationer

- 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.
- Säkerställ att det finns dokumenterade intresseavvägningsbedömningar för samtliga bevakningar som baseras på den rättsliga grunden berättigat intresse.

- Bedöm om konsekvensbedömning bör utföras för de behandlingar där det inte har gjorts.
- Inhämta dataskyddsombudets rekommendationer vid genomförande av konsekvensbedömningar eller tröskelanalyser.
- Säkerställ att tecknat personuppgiftsbiträdesavtal med leverantören Safeteam innehåller samtliga kriterier som ett personuppgiftsbiträdesavtal ska innehålla sedan GDPR trädde i kraft.

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**:

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.

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 8 juli 2022.**

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