Framtiden Byggutveckling
Vi bygger det hållbara samhället för framtiden

Styrelsehandling nr 11
Styrelsedatum: 2023-02-10
Diarienummer: FBU2023-0004

Handläggare: Jenny-Maria Ericsson-Deogan
Telefon: 031-719 31 56
E-post: jenny-maria.ericsson@framtiden.se

Årsrapport för dataskyddsarbete 2022

Informationsärende

Styrelsen för Framtiden Byggutveckling AB:

Årsrapport för dataskyddsarbetet 2022 antecknas.

Ärendet

På sammanträdet 2022-02-11 antecknade styrelsen en kontrollplan för dataskyddsarbetet 2022 som bolaget har följt.

Ärendet innehåller en årsrapport över verksamhetens dataskyddsarbete för 2022. Rapporten innehåller information om verksamhetens samarbete med dataskyddsombudet, genomförda kontroller, lämnade rekommendationer samt en övergripande bedömning av status på verksamhetens personuppgiftshantering utifrån fasta kontrollpunkter.

För att möjliggöra en direkt kommunikation mellan dataskyddsombud och personuppgiftsansvarig styrelse ska årsrapporten presenteras i möte med styrelsen. Föreliggande rapport kommer att presenteras för styrelsen för Framtiden Byggutveckling AB av Markus Ternblad, som är Göteborgs Stads dataskyddsenhets utsedda kontaktperson för Framtiden Byggutveckling AB.

Rapporten från DSO omfattar en fördjupad kontroll avseende kameraövervakning och en årlig kontroll med 12 punkter.

Rapporten ger följande rekommendationer:

Den fördjupade kontrollen av kameraövervakning visar att rutin för framtida hantering behöver upprättas. Rekommendationerna avser bland annat behov av att säkerställa den rättsliga grunden för behandlingen, att se över lagringstiden av inspelat material, teckna personuppgiftsbiträdesavtal med leverantören och att säkerställa att information till de registrerade lämnas på korrekt sätt.

Bolaget rekommenderas även bedöma om en konsekvensbedömning behöver utföras för behandlingen i enlighet med bestämmelserna för när så ska ske enligt GDPR.

Årlig kontroll baseras på en enkät där påståenden och/eller självskattning ger en bild av bolagets dataskyddsarbete inom 12 områden. Alla kontrollpunkter spänner från hög (nivå 1) till låg risk (nivå 4). Även för verksamheter med låga risker krävs kontinuerliga insatser för att denna risknivå ska bibehållas. De risker som bolaget har identifierat spänner alla inom låga nivåer.

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

• **Kontrollpunkt 5: Övergripande strategi för dataskydd**

(nivå 3) Risker identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.

• **Kontrollpunkt 7: Integritetspolicy**

(nivå 4) Inga direkta risker av betydelse identifierade. Indikerar att verksamheten har ett systematiskt dataskyddsarbete.

• **Kontrollpunkt 9: Konsekvensbedömning/samråd**

(nivå 3) Risker identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.

Bedömning ur ekonomisk dimension

Ärendet är av administrativ karaktär och bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Bedömning ur ekologisk dimension

Ärendet är av administrativ karaktär och bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Bedömning ur social dimension

Ärendet är av administrativ karaktär och bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Samverkan

Ärendet har inte varit föremål för samverkan

Bilagor

1. Årsrapport dataskyddarbete 2022

Göteborgs Stad

Styrelsehandling nr 11
Bilaga 1
FBU2023-0004
2023-02-10

Årsrapport för dataskyddsarbetet 2022

Framtiden Byggutveckling

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.

Dataskyddsombudet har i rapporten avseende den fördjupade kontrollen haft vissa anmärkningar och har därför lämnat ett antal rekommendationer till verksamheten för att förbättra sitt arbete och säkerställa följsamhet mot GDPR.

Rekommendationerna avser bland annat behov av att säkerställa rättslig grund för behandlingen, att se över lagringstiden av inspelat material, teckna personuppgiftsbiträdesavtal med leverantören och att säkerställa att information till de registrerade lämnas på rätt sätt. Bolaget rekommenderas även bedöma om en

konsekvensbedömning behöver utföras för behandlingen i enlighet med bestämmelserna för när så ska ske enligt GDPR.

Vid avstämning med bolaget i december 2022 framgår att kamerabevakningen på Titteridammsvägen är avslutad. Dataskyddsombudets rekommendationer bör därför ses som vägledande för framtida bevakningar.

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 Framtiden Byggutveckling AB:s 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 likadant på denna kontrollpunkt som föregående år, vilket innebär att bolaget även i år hamnar på nivå 4. Skattningen innebär att bolaget anser sig ha mycket goda organisatoriska förutsättningar för att kunna bedriva ett effektivt och fungerande dataskyddsarbete. Skattningen indikerar att det inom ramen för kontrollpunkten inte föreligger några risker av betydelse och bolaget arbetar på ett systematiskt vis.

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

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Bolaget har skattat sig något högre på denna kontrollpunkt än föregående år och hamnar på nivå 4. Skattningen indikerar att det inom ramen för kontrollpunkten inte föreligger några risker av betydelse och att bolaget arbetar på ett systematiskt vis med personuppgiftsincidenter.

Det enda dataskyddsombudet vill lyfta under denna kontrollpunkt är att bolaget bör se över om man verkligen har tillräckliga rutiner för att upptäcka personuppgiftsincidenter. Detta då bolaget under 2022 enbart har haft en personuppgiftsincident. 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:

Bolagets skattning på denna kontrollpunkt ligger kvar på samma nivå som föregående år (3), med en marginell förbättring av kontrollpunktens medelvärde. Resultatet indikerar att det förekommer risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga. Det är positivt att det bland annat förefaller finnas biträdesavtal tecknade för samtliga personuppgiftsbiträdesrelationer.

På frågan om bolaget har rutiner för att kontinuerligt genomföra efterlevnadskontroller av anlitade personuppgiftsbiträden i syfte att säkerställa att dessa uppfyller villkoren i biträdesavtalet, har dock bolaget svarat att det inte stämmer. Då efterlevandskontroller är en viktig del i att uppfylla ansvarsprincipen i dataskyddsförordningen bör bolaget införa rutiner för detta. Bolaget behöver också, enligt skattningen, säkerställa att det finns rutiner för att bedöma om en personuppgiftsbiträdesrelation uppstår vid anlitande av nya leverantörer.

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 på denna kontrollpunkt ligger kvar på samma nivå (3) som föregående år, med en mindre försämring av kontrollpunktens medelvärde.

Resultatet indikerar att det förekommer risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga. Ett par av frågorna har dock besvarats med alternativet *Nej, det stämmer inte bra*. Bolaget behöver exempelvis säkerställa att det finns rutiner för att uppdatera registret när behandlingar har tillkommit eller förändrats. Det kan också vara fördelaktigt att försöka använda registret som en del i det dagliga dataskyddsarbetet.

Dataskyddsombudet vill också belysa att bolaget har svarat att cirka 75 % av bolagets behandlingar finns registrerade i registret och att cirka 75 % av dessa innehåller den information som ska finnas med enligt art. 30 GDPR. I och med att samtliga behandlingar ska finnas registrerade i registret och att samtliga ska innehålla den information som art. 30 GDPR säger, rekommenderas bolaget att säkerställa att så sker.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Bolaget har förbättrat sitt resultat på denna kontrollpunkt jämfört med föregående år och ligger nu på nivå 3. Resultatet 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. Två av de frågor som bolaget inte kunde besvara föregående och som därmed drog ned resultatet för kontrollpunkten har besvarats detta år, vilket bidrar till förbättringen.

Svaren på flera av frågorna under kontrollpunkten indikerar dock att det finns risker som bolaget behöver arbeta med. Bolaget behöver, likt föregående år, arbeta med klassificeringen (konfidentialitet, riktighet, och tillgänglighet) av sina informationstillgångar utifrån stadens styrande dokument. Detta då bolaget angett att enbart cirka 25 % av informationstillgångarna har klassificerats.

Vid avstämning med bolaget uppges det att en intern kontroll för att säkerställa följsamheten mot GDPR nyligen har genomförts. Dataskyddsombudet rekommenderar att bolaget säkerställer att detta är något som sker regelbundet för att kontinuerligt kontrollera följsamheten mot GDPR. Vid avstämning med bolaget

uppges att man nyligen har genomfört en intern kontroll för att säkerställa följsamhet till GDPR.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Likt föregående år har bolaget skattat sig högt på denna kontrollpunkt och ligger kvar på nivå 4. Skattningen indikerar att det inte finns några direkta risker och att bolaget arbetar systematiskt med utbildning inom dataskydd.

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

Likt föregående år har bolaget skattat sig mycket högt på denna kontrollpunkt och besvarat samtliga påståenden med alternativet *Ja, det stämmer helt*. Detta gör att skattningen indikerar att det inte finns några direkta risker kopplat till kontrollpunkten.

Utifrån hur den externa integritetspolicyn är formulerad uppmanar dataskyddsombudet bolaget att säkerställa att integritetspolicyn uppfyller kraven på

information. För att informationsplikten ska anses vara uppfylld ska det bland annat tydligt framgå ändamål och rättslig grund, hur länge uppgifterna lagras eller vara 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 bolagets externa policy så bör bolaget exempelvis se över 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 tveksamt om hänvisning till dokumenthanteringsplan som den registrerade inte har tillgång till kan anses tillräckligt.

Avseende överföring till tredjeland anger bolaget att bolaget strävar efter att alltid behandla personuppgifterna inom EU/EES, vilket också bör tydliggöras. Antingen behandlar bolaget personuppgifterna inom EU/EES och kan ange att så sker eller så gör bolaget inte det och då ska information i enlighet med art. 13.1 f och 14.1 f GDPR lämnas.

När det kommer till de registrerades rättigheter bör bolaget beskriva dessa tydligare, vad de innebär och koppla dem till respektive behandling. Det ska också framgå hur den registrerade kan gå till väga för att utöva en specifik rättighet och vilka begränsningar som rättigheten eventuellt omfattas av.

Sammantaget instämmer inte dataskyddsombudet i bolagets skattning avseende att bolagets integritetspolicy säkerställer att informationsplikten uppfylls.

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 sig något på denna punkt jämfört med föregående år, men ligger kvar på samma övergripande nivå (3). Detta gör att det inom ramen för kontrollpunkten finns risker identifierade, men dessa bedöms inte vara brådskande, omfattande eller allvarliga. Det är positivt att bolaget jämfört med föregående år nu

anger att de informerar registrerade om hur deras personuppgifter behandlas vid första kontakt via e-post.

Bolaget behöver, enligt skattningen, arbeta vidare med klassificeringen av sina personuppgiftsbehandlingar enligt stadens styrande dokument eftersom det angivits att så har skett för cirka 50 % av bolagets behandlingar. Bolaget har också angett att de inte vet/inte kan besvara frågan om klassificeringarnas aktualitet har kontrollerats det senaste året. Bolaget bör därför säkerställa att tidigare klassificeringar är aktuella. Bolaget behöver också säkerställa att det finns rutiner och anvisningar för hantering av personuppgifter i e-post.

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:

Bolaget har förbättrat sig något på denna punkt jämfört med föregående år, men ligger kvar på samma övergripande nivå (3). Detta gör att det inom ramen för kontrollpunkten finns risker identifierade, men dessa framstår ej som brådskande, omfattande eller allvarliga.

Dataskyddsombudet utläser dock att det finns vissa motstridiga uppgifter i bolagets svar. Bland annat har angivits *Ja, det stämmer helt* vad gäller om verksamheten har rutiner för att identifiera personuppgiftsbehandlingar med hög risk för de registrerades fri- och rättigheter, medan det också anges att cirka 0 % av bolagets behandlingar har kontrollerats utifrån höga risker för de registrerades fri- och rättigheter. Bolaget har också angett att det finns rutiner för att säkerställa att konsekvensbedömningar genomförs innan riskfyllda behandlingar påbörjas. Med hänsyn till att bolaget angett att cirka 0 % av bolagets behandlingar har kontrollerats och att konsekvensbedömningar enbart har utförts för cirka 25 % av de behandlingar då det krävs, verkar det föreligga behov av att säkerställa att eventuella rutiner följs. Det är dock positivt att det förefaller finnas en planering för utförandet av konsekvensbedömningar där så krävs. Det innebär ju dock att bolaget har identifierat vilka behandlingar som behöver konsekvensbedömas.

Sammanfattningsvis rekommenderar dataskyddsombudet att bolaget prioriterar arbetet med denna kontrollpunkt och säkerställer att det finns tillräckliga rutiner samt att konsekvensbedömningar utförs för samtliga behandlingar som innebär en hög risk för de registrerades fri- och rättigheter.

Dataskyddsombudet vill också lyfta att det pågår ett positivt och intensivt arbete med konsekvensbedömningar på koncerngemensam nivå, vilket dataskyddsombudet tror kommer gynna bolaget utveckling inom ramen för denna kontrollpunkt.

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, likt föregående år, skattat sig högt på denna kontrollpunkt och svarat *Ja, det stämmer bra* på samtliga frågor. Skattningen indikerar att det inte föreligger några risker och att bolaget arbetar systematiskt med dataskyddsperspektivet i IT-projekt och upphandling.

Dataskyddsombudet har inte anledning att ifrågasätta resultatet i stort, men har inte heller blivit involverad i frågor som rör uppstart av nya IT-projekt eller införande av nya tjänster där personuppgifter kommer att hanteras det senaste året. Med hänsyn till vad som framgår under kontrollpunkt 9 om konsekvensbedömningar/samråd bör bolaget dock säkerställa att man verkligen arbetar systematisk och kontinuerligt med att bedöma risker för personuppgiftsbehandlingar i arbetet med upphandling av nya system och tjänster eller vid utveckling av befintliga verksamhetssystem.

Vid avstämning med bolaget framgår att bolagets samtliga upphandlingar sker via stadengemensamma rutiner och via förvaltningarna för Intraservice och inköp och upphandling. Bolaget anger därför att de ofta hamnar i en situation där de anges som ansvariga för en personuppgiftsbehandling som de har mycket liten eller ingen möjlighet att påverka. Dataskyddsombudet instämmer i att personuppgiftsansvarsfrågan behöver tydliggöras i staden och inte minst i de fall där det upphandlas tjänster centralt som bolag och förvaltningar inte har möjlighet att välja bort. Utifrån hur upplägget ser ut idag anges dock bolag och förvaltningar som personuppgiftsansvariga och dataskyddsombudet anser att bolaget borde ha belyst de svårigheter och brister som man upplever i centrala upphandlingar i sin skattning.

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, likt föregående år, skattat sig högt på denna kontrollpunkt och ligger kvar på nivå 4. Skattningen indikerar att det inom ramen för kontrollpunkten inte finns några risker av betydelse och att bolaget arbetar systematiskt med frågan.

Enligt skattningen behöver bolaget dock arbeta vidare med att säkerställa dataskyddsperspektivet vid införandet och användandet av kostnadsfria tjänster såsom gratisappar och sociala medier.

Avseende sociala medier anger bolaget att de använder plattformen LinkedIn, men att det utförts analys av användningen efter att Schrems II-domen kom.

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 har genomfört en analys av användningen, bör bolaget vidta ytterligare åtgärder för att följsamhet mot förordningen ska kunna säkerställas vid användningen av LinkedIn.

Bolaget har skattat sig högt avseende användningen av cookies och informationen om dessa till de registrerade. Vid avstämning med bolaget framgår att bolaget helt avbrutit sin användning av cookies. Då det fortsatt finns information om bolagets användning av cookies i bolagets integritetspolicy (såväl nödvändiga som icke nödvändiga cookies) bör bolaget ändra denna så den överensstämmer med vad som faktiskt sker. Dataskyddsombudet har inte kunnat kontrollera bolagets cookies då de verktyg som finns tillgängliga för dessa inte kan läsa av bolagets hemsida på grund av för många omdirigeringar, rekommenderar dataskyddsombudet att bolaget säkerställer att all cookieanvändning är borttagen samt att det inte föreligger risk för överföring av personuppgifter till tredjeland på grund av tredjepartsförfrågningar. Dataskyddsombudet lyfter detta då det vid kontroll av flera av de övriga bolagen i koncernens hemsidor föreligger sådan risk.

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 har, enligt skattningen, gjort en ordentlig förbättring inom ramen för denna kontrollpunkt jämfört med tidigare år och ligger nu på nivå 4. De allra flesta påståenden har besvarats med alternativet Ja, det stämmer helt, vilket indikerar att bolaget anser att det finns mycket god kunskap och rutiner för att hantera de fri- och rättigheter som GDPR anger att de registrerade har. Det finns goda rutiner för att hantera begäran om registerutdrag i tid och på rätt sätt.

Bolaget har angett att det inte finns rutiner för att hantera om en registrerad drar tillbaka ett lämnat samtycke. Vid avstämning med bolaget anges att samtycke aldrig används som rättslig grund inom bolaget, varför några rutiner kopplat till detta inte heller finns. Dataskyddsombudet anser det som rimligt och har inga invändningar. Skulle bolaget använda sig av samtycken framöver bör bolaget då säkerställa att aktuell rutin finns.

2.5 Sammanfattande rekommendationer

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

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

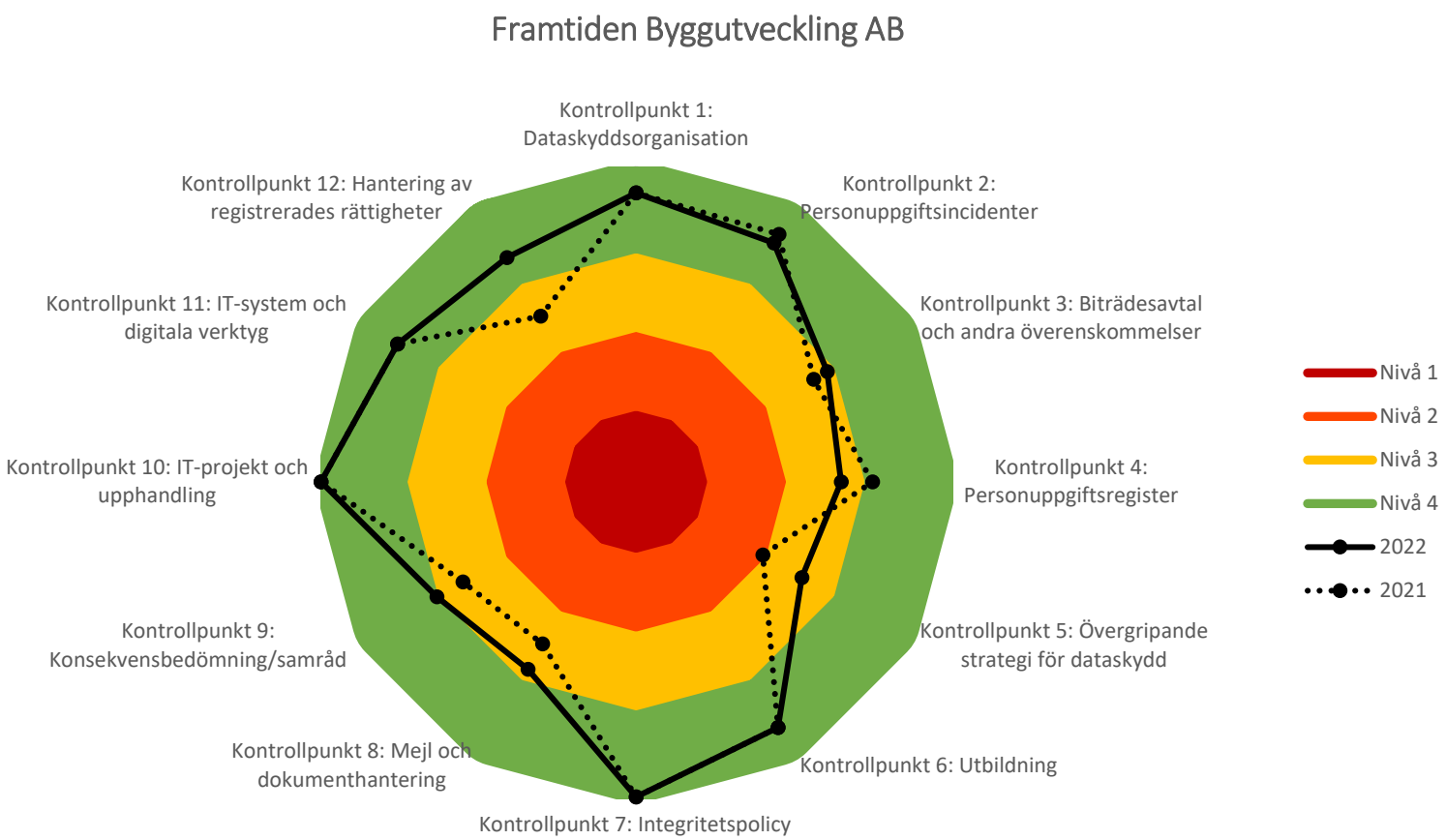
- Kontrollpunkt 5: Övergripande strategi för dataskydd
- Kontrollpunkt 7: Integritetspolicy
- Kontrollpunkt 9: Konsekvensbedömning/samråd

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 Framtiden Byggutveckling AB (FBU)

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.

Sammanfattning av FBU:s användning av kamerabevakning

Enligt inkomna svar från FBU har bolaget enbart kamerabevakning på en plats, nämligen vid byggutvecklingsprojektet vid Titteridammsvägen. Bolaget har fyra kameror i det inhägnade området, med fokus på yttre entréer till den färdigställda obebodda byggnation man uppfört. En kamera är riktad mot det staket som vetter mot Titteridammsvägen. Syftet med kamerabevakningen är att förhindra stöld, inbrott och olaga intrång samt att kunna kontrollera att staketet inte blåser ner. Bolaget har inte sökt tillstånd för kamerabevakningen då den uppges ske på en plats dit allmänheten inte har tillträde. Personuppgiftsbiträdesavtal saknas med den anlitade leverantören av kameror.

Vid avstämning med bolaget i december 2022 framgår att kamerabevakningen på Titteridammsvägen är avslutad. Dataskyddsombudets rekommendationer bör därför ses som vägledande för framtida bevakningar.

Dataskyddsombudets rekommendationer

Tillstånd

Bolaget uppger att man inte sökt något tillstånd för kamerabevakningen då bolagets övervakning sker på en plats dit allmänheten inte har tillträde. I de fall kameror är riktade mot en plats dit allmänheten har tillträde är avståndet sådant att det inte går att identifiera enskilda individer. Utifrån bolagets beskrivning instämmer dataskyddsombudet i att behandlingen inte är av en sådan art att den kräver ett tillstånd för att få genomföras.

Tider och platser som kamerabevakas

FBU bedriver kamerabevakning på en geografisk plats, Titteridammsvägen. Bolaget har fyra kameror i området. Kameraövervakningen sker inom inhägnat område, med fokus på yttre entréer till den färdigställda obebodda byggnation man uppfört. Vidare uppger man att en kamera även är riktad mot det staket som vetter mot Titteridammsvägen. Denna kamera uppges vara placerad på ett sådant sätt att det inte går att urskilja enskilda individer på grund av avståndet. Övervakningen sker dygnet runt då det är ett färdigställt bostadsbygge som väntar på att bli överlämnat till förvaltande bolag. Flera intrångsförsök har gjorts på platsen.

Inga anställda eller någon annan rör sig på området då bygget är avslutat och det bor inga personer i byggnaderna. Om någon befinner sig på platsen har vederbörande tagit sig in olovligen.

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 anges.

Avseende lagringstid bör bolaget se över denna då huvudregeln för lagring av inspelat material, om lagring behöver ske, är 72 h. Bolaget har angett att lagringstiden är 14 dagar, vilket bör ses över. I detta kan det t.ex. vägas in 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 lagringstidens längd beror på brottsutredande myndigheters långa handläggningstid, vilket dataskyddsombudet anser behöver förtydligas då den generella lagringstiden sannolikt inte påverkas av brottsutredande myndighets handläggningstid i och med att larmbolaget realtidsövervakar platsen i kombination med att materialet spelas in. Det material som visar en incident bör således kunna omhändertas snabbt och särskiljas från övrigt material som då inte behöver lagras en längre tid. Det som bolaget bör utgå ifrån är alltså hur lång tid det tar att upptäcka en incident och omhänderta materialet, inte utgå från brottsutredande myndigheters handläggningstid. Att det material som visar en incident som behöver utredas sparas för en längre tid får dock anses befogat.

Dataskyddsombudet rekommenderar att bolaget ser över lagringstiden och om en längre tid än 72 h bedöms vara nödvändig, tydligt motiverar och dokumenterar denna bedömning.

Ändamål och rättslig grund

FBU har angett att ändamålet med behandlingen dels är att den ska verka brottsförebyggande och därvid leda till att bolagets kostnader för exempelvis skadegörelse eller inbott ska minska, dels att brott ska kunna utredas av brottsbekämpande myndigheter.

Dataskyddsombudet bedömer att de ändamål som har angivits för kamerabevakningen i stort verkar vara berättigade. Med hänsyn till att platsen har varit utsatt för intrångsförsök framstår det som rimligt att platsen kamerabevakas för att minska risken för fler sådana försök.

Utöver ett berättigat ändamål måste det finnas stöd i en rättslig grund i dataskyddsförordningen för att kamerabevakningen ska få utföras. FBU har uppgett att den rättsliga grund som man stödjer sin behandling på är artikel 6 c GDPR. Dataskyddsombudet förutsätter att det som avses är den rättsliga grund som kallas rättslig förpliktelse eftersom det är den rättsliga grund som framgår av art. 6.1 c GDPR. Av det underlag som dataskyddsombudet har tagit del av finns dock inte någon motivering eller anvisning till vilken rättslig förpliktelse det skulle vara.

För att en personuppgiftsbehandling ska kunna baseras på den rättsliga grunden rättslig förpliktelse så ska det röra sig om att det i lag eller annan författning, kollektivavtal eller beslut fattat med stöd av lag, finns en rättslig förpliktelse som gör att den personuppgiftsansvarige måste behandla vissa personuppgifter i sin verksamhet. Behandlingen av personuppgifter måste också vara nödvändig för att kunna utföra den rättsliga förpliktelsen.

För rättslig förpliktelse krävs att skälet till personuppgiftsbehandlingen framgår tydligt i bestämmelsen, exempelvis bestämmelser om att redovisa uppgifter i körjournaler till Skatteverket. Det ska vara tydligt redan av bestämmelsens utformning för både den vars personuppgifter behandlas och den personuppgiftsansvarige att behandling av personuppgifter krävs för att uppfylla förpliktelsen. Dataskyddsombudet har svårt att se vilken sådan förpliktelse kamerabevakningen skulle kunna vara aktuell, men kan såklart inte säga att det inte är möjligt då det inte redogjorts för av bolaget. Dataskyddsombudet rekommenderat att FBU utreder, motiverar och dokumenterar rättslig grund för behandlingen.

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. Vad som utgör hög risk framgår bland annat av IMY:s förteckning med kriterier för att avgöra om en behandling av personuppgifter innebär hög risk. Om två eller flera kriterier är uppfyllda ska en konsekvensbedömning som huvudregel utföras. 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, utan anger att eftersom bevakningen sker på en plats dit allmänheten inte har tillträde eller där personuppgiftsbehandling enbart sker om någon olovligen rör sig på området, har någon konsekvensbedömning inte ansetts nödvändig.

Dataskyddsombudet noterar att det mycket väl kan vara så att kamerabevakningen i detta fall inte föranleder att någon konsekvensbedömning behöver genomföras. Utifrån omständigheterna som har beskrivits så verkar det inte sannolikt att minst två kriterier i IMY:s förteckning är uppfyllda. Dataskyddsombudet rekommenderar dock att bolaget gör denna bedömning (en så kallad tröskelanalys) och därmed också får sina överväganden nedtecknade. Att bevakningen sker på en plats dit allmänheten inte har tillträde kan vara en sådan omständighet, bland flera, som medför att den slutliga bedömningen blir att någon konsekvensbedömning inte behöver genomföras, men bolaget behöver göra en helhetsbedömning.

Säkerhet för bevakningen

Om kamerabevakningen innebär en personuppgiftsbehandling och leverantören av bevakningen hanterar personuppgifter på verksamhetens uppdrag, är leverantören att betrakta som personuppgiftsbiträde. Den personuppgiftsansvarige ansvarar för att enbart anlita personuppgiftsbiträden som tillämpar tillräckliga tekniska och organisatoriska åtgärder för behandlingen av personuppgifter och man behöver upprätta ett så kallat personuppgiftsbiträdesavtal mellan sig. Avtalet reglerar bland annat vilka personuppgifter som får behandlas, vilka säkerhetsåtgärder som ska tillämpas, hur länge personuppgifterna får lagras osv. Självklart behöver båda parter också vara införstådda med vilken teknik som används för behandlingen.

FBU uppger att kamerorna tillhandhålls av leverantören Omninor AB som även står för de väktare som rycker ut till området. Bolaget har även uppgett att man använder sig av kameror med rörligt ofiltrerat material som spelas in på en lokalt placerad inspelningsenhet. Lagring sker med ca 14 dagars material, p.g.a. polisutredares höga arbetsbelastning för det fall att brott skulle behöva utredas. Såväl inspelning som övervakning sker i realtid och utförs av Omninor AB.

FBU uppger som svar på dataskyddsombudets frågor att man inte tecknat något personuppgiftsbiträdesavtal med Omninor då kamerabevakningen sker på ett område som allmänheten inte har tillträde till. Dataskyddsombudet vill här påpeka att huruvida de

personer som eventuellt filmas befinner sig på platsen olovligen eller ej saknar betydelse för frågan om huruvida det är personuppgifter som behandlas eller inte. Här är det viktigt att komma ihåg att det är två regelverk som styr, kamerabevakningslagen och GDPR, och att man som personuppgiftsansvarig eller ansvarig för kamerabevakning behöver tillämpa samtliga bestämmelser. FBU rekommenderas därför att teckna biträdesavtal med Omninor AB.

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.

FBU uppger att skyltar på området informerar om att kamerabevakning sker och att man i övrigt hänvisar till sin integritetspolicy på bolagets hemsida. Den information som lämnas på hemsidan är dock en översiktlig beskrivning av hur bolaget behandlar personuppgifter och det nämns inget om den kamerabevakning som bedrivs. Detta behöver åtgärdas. FBU behöver ta hänsyn till att man trots allt behandlar personuppgifter, även om området inte är avsett att beträdas. Det är ytterst osannolikt att någon personuppgiftsbehandling inte sker. Det har skett flera intrångsförsök, bolaget beskriver att väktare åker till området vid behov och att inspektion av området sker sannolikt då och då utan att kamerorna stängs av.

Bolaget rekommenderas att uppdaterar informationen till de registrerade. Dels genom den skyltning som sker på plats (den viktigaste informationen om bevakningen) och dels genom den information som lämnas via hemsidan (det andra informationslagret).

Sammanfattade rekommendationer

- Se över den generella lagringstiden av inspelat material.
- Utred, motivera och dokumentera rättslig grund för behandlingen.
- Bedöm och dokumentera bedömningen om konsekvensbedömning bör genomföras på behandlingen.
- Teckna personuppgiftsbiträdesavtal med leverantören.
- Uppdatera informationen till de registrerade.

Bilagor

- Frågor och informationsutskick

Information om fördjupad kontroll 2022

Kontrollpunkt 11: Kamerabevakning

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

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

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

Tillvägagångssätt

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

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

Fördjupad kontroll 2022

Kontrollpunkt 11: Kamerabevakning (del 1)

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

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

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

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

Har du frågor, kontakta ditt huvudansvarige dataskyddsombud.

Fördjupad kontroll 2022

Kontrollpunkt 11: Kamerabevakning (del 2)

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

1. Vilka platser kamerabevakar ni? Detta ska beskrivas även utifrån vilka områden/ytor på platsen som kamerabevakas tex. entrén utvändigt, entrén invändigt, trapphus, specifika rum.
    - **Uppföljande fråga:** Ange antal områden och platser där ni i dagsläget har kamerabevakning. Här önskas en specifikation av samtliga områden/platser.
        a. Ange ändamålet och rättslig grund för behandlingen/behandlingarna.
    - **Uppföljande fråga:** Svaret innehåller endast en redogörelse om bevakningens ändamål. Ange också rättslig grund enligt artikel 6 GDPR för respektive behandling.
        b. Har ni sökt tillstånd för den kamerabevakning som ni utför? Om inte, ange varför.
    - **Uppföljande fråga:** Hur säkerställer bolaget att kameran inte omfattar allmän plats vid de platser/områden där kameran riktas mot entréer eller staket (i anslutning till allmän plats)?
2. Har ni utfört konsekvensbedömningar eller andra typer av dokumenterade bedömningar/analyser för er kamerabevakning? Om ja, skicka även in denna dokumentation.
    - **Uppföljande fråga:** Utveckla bedömningen till varför konsekvensbedömningar inte har gjorts. Hur har bolaget resonerat i frågan? Bifoga eventuell dokumentation.
3. Vilken teknik använder ni och vilka leverantörer använder ni?
    - **Uppföljande frågor:** Utveckla svaret ”Videokameror” och beskriv tekniken som används. Hur säkerställs att inga personer kan identifieras? Om filter används, är detta permanent eller kan det lyftas bort av bolaget (eller biträdet)? Sker inspelningen med ljudupptagning? Lagras inspelningen i molntjänst eller onprem? Hur länge sparas filmerna (lagringstid) och vem/vilka har tillgång till filmerna? Etc.

    a. Finns personuppgiftsbiträdesavtal upprättade med de leverantörer som ni använder? Bifoga dessa avtal.

- **Uppföljande fråga:** Har bolaget gjort bedömningen att den leverantör som används inte är personuppgiftsbiträde till bolaget? Utveckla hur verksamheten har kommit till denna slutsats och bifoga eventuell dokumentation i frågan.

4. Hur informerar ni de registrerade om kamerabevakningen som utförs? Bifoga den information som ni tillhandahåller de registrerade och ange hur den tillgängliggörs.
    - **Uppföljande frågor:** Innebär svaret att bolaget inte tillhandahåller någon information överhuvudtaget om kamerabevakningen? Då varken via information på hemsidan eller genom skyltar i direkt anslutning till området som kamera bevakas?

Kompletterande förtydligande fråga:
Beskriv i breda drag hur kamerabevakningen på de olika platserna används. Är det t.ex. enbart inspelat material som bolaget tittar på vid behov i efterhand eller sker realtidsövervakning? Ange även när kamerabevakningen sker och, om denna sker dygnet runt, om anställda som arbetar på platserna därmed förekommer på filmerna.

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 5 augusti 2022.**

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