Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Familjebostäder

2022-12-23

Innehåll

1 Dataskydd i kommunal verksamhet

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

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

1.1 Göteborgs Stads dataskyddsombud

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

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

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

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

2 Granskning av dataskyddsarbetet 2022

2.1 Dataskyddsombudets kontrollfunktion

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

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

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

2.2 Fördjupad kontroll

2.2.1 Kontroll av kamerabevakning 2022

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

Dataskyddsombudets övergripande intryck efter kontrollen är att bolaget har god koll på sin kamerabevakning överlag och förståelse för att det är två separata regelverk som ska tillämpas. I rapporten har dataskyddsombudet dock haft några anmärkningar och har därför lämnat rekommendationer till verksamheten för att förbättra sitt arbete och säkerställa följsamhet mot GDPR.

Rekommendationerna avser bland annat behov av att se över och förtydliga lagringstiden av inspelat material och säkerställa att bolaget inhämtar

dataskyddsombudets rekommendationer i samband med utförande av konsekvensbedömningar.

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 Familjebostäders dataskyddsarbete 2022

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

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

2.4.1 Kontrollpunkt 1: Dataskyddsorganisation

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

Dataskyddsombudets kommentarer:

Bolagets skattning ligger kvar på ungefär samma nivå som föregående år, men med en marginell förbättring av medelvärdet, vilket gör att bolagets skattning nu ligger precis på gränsen till nivå 4. Skattningen indikerar att det inom ramen för kontrollpunkten har identifierats risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga.

En förbättring kan ses avseende att bolaget nu angivit att dataskydd är en naturlig och integrerad del av det dagliga arbetet för alla medarbetare.

Utifrån de kontakter som dataskyddsombudet har haft med bolaget under 2022, instämmer dataskyddsombudet i bolagets skattning. Bolaget förefaller ha flera rutiner på plats och arbeta för att driva dataskyddsarbetet framåt.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Bolagets skattning är något högre detta år jämfört med föregående och man ligger kvar på nivå 4. Sammantaget indikerar skattningen att det inom ramen för kontrollpunkten inte bedöms föreligga några risker av betydelse och indikerar att bolaget arbetar systematiskt med personuppgiftsincidenter.

Enligt skattningen har bolaget i stort ett välfungerande arbete med personuppgiftsincidenter, men behöver arbeta vidare med att följa upp inträffade incidenter för att på så vis identifiera riskområden.

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

2.4.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

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

Dataskyddsombudets kommentarer:

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

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

2.4.4 Kontrollpunkt 4: Personuppgiftsregister

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

Dataskyddsombudets kommentarer:

Bolagets skattning visar på en förbättring inom ramen för kontrollpunkten. Bolaget ligger kvar på nivå 3 överlag, men ligger precis på gränsen till nivå 4. Sammantaget indikerar skattningen att det inom ramen för kontrollpunkten har identifierats risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga.

Det är positivt att bolaget har förbättrat sig avseende hur stor del av behandlingarna som nu innehåller all den information som krävs enligt art. 30 GDPR och ligger nu

på 75 %. Bolaget har också förbättrat sig avseende att följa upp och kontinuerligt uppdatera registret med behandlingar som antingen har tillkommit eller förändrats. En liten försämring ses avseende bolagets skattning av hur många av bolagets behandlingar som finns med i registret, från ca 100 % förra året till ca 75 % detta år. Eftersom samtliga behandlingar som en personuppgiftsansvarig utför ska finnas i registret och detta ska innehålla komplett information rekommenderas bolaget att fortsätta sitt arbete inom detta område.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

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

Enligt skattningen verkar bolaget arbeta på bra med styrningen av dataskyddsfrågorna och att systematiskt integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet. Bolaget anger att flera rutiner finns på plats för att säkerställa dataskyddet och att man har en policy för att hantera IT-system och verktyg osv.

Bolagets informationstillgångar bör fortsätta klassificeras utifrån *Konfidentialitet, Riktighet* och *Tillgänglighet* i enlighet med stadens styrande dokument då det anges att det är gjort för ca 75 % av informationstillgångarna. Bolaget bör också genomföra interna kontroller för att säkerställa följsamhet mot GDPR.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

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

Bolaget förefaller arbeta bra med utbildningar och informationsinsatser samt att följa upp kunskapsnivån hos medarbetarna. För att bli ännu bättre och säkerställa att resurser sätts in där det främst behövs bör bolaget kartlägga vilken nivå av dataskyddskunskaper som olika befattningar bör ha och utbilda därefter.

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 innebär en försämring jämfört med föregående år, men som helhet ligger bolaget kvar på nivå 3, vilket innebär att det föreligger risker som behöver åtgärdas, men som ej anses vara brådskande, omfattande eller allvarliga.

Försämringen består i att bolaget nu anger att integritetspolicyn inte uppfyller kraven på information enligt GDPR och att det saknas rutiner för att kontinuerligt se över och uppdatera den policyn. Efter att ha sett över bolagets externa integritetspolicy på en övergripande nivå anser dataskyddsombudet att årets skattning är mer korrekt än föregående års skattning och att det finns skäl att se till att utövandet av informationsplikten förbättras. För att informationsplikten ska anses vara uppfylld ska det bland annat tydligt framgå ändamål och rättslig grund, hur länge uppgifterna lagras eller vara väldigt tydligt för den registrerade hur lagringstiden bedöms. Det ska även framgå vilka som är mottagare, vad som gäller när det kommer till de registrerades rättigheter samt vara tydligt om och i så fall vilka tredjelandsöverföring som sker. Om personuppgifterna inte samlas in direkt från den registrerade så ska även kategorierna av personuppgifter framgå.

Även om mycket av ovanstående finns med i policyn så bör bolaget se över exempelvis hur man informerar om lagringstid. Det kan vara okej att hänvisa till kriterierna för hur lagringstiden bedöms om exakt lagringstid inte anges. Den registrerade ska dock, utifrån sin egen situation, i så fall kunna bedöma lagringstiden utifrån kriterierna. Dataskyddsombudet bedömer det som tveksamt om hänvisning till dokumenthanteringsplan som den registrerade inte har tillgång till kan anses tillräckligt. Bolaget bör även säkerställa att den registrerades rättigheter förtydligas för respektive behandling. En ordentlig översyn av helheten bör genomföras kontinuerligt, inte minst med hänsyn till den praxis som nu finns kopplat till informationsplikten och som kontinuerligt fortsätter att komma.

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 ligger kvar på samma resultat på denna kontrollpunkt som föregående år (3). Skattningen indikerar att det finns risker, men att de inte bedöms vara brådskande, omfattande eller allvarliga. Flera av påståendena har dock besvarats med alternativet *Nej, det stämmer inte bra*, varför det sannolikt ändå finns risker som bör prioriteras inom ramen för kontrollpunkten.

Bolaget behöver bland annat se till att det finns en aktuell, uppdaterad och fastställd dokumenthanteringsplan så att det finns tydlighet kring när och hur personuppgifter gallras. Kopplat till detta behövs också möjlighet att kontrollera att personuppgifter gallras enligt gällande gallringsbeslut och framförallt att man medvetandegör bolagets medarbetare om dokumenthantering och gallring kopplat till GDPR. Utan en dokumenthanteringsplan är det svårt för en personuppgiftsansvarig att uppfylla principerna om lagringsminimering och uppgiftsminimering. Vid avstämning med bolaget framgår att arbetet med att ta fram dokumenthanteringsplan hela tiden fortlöper, men att det tar lång tid att få till samtliga delar i samråd med Regionarkivet. Bolaget står dock inte helt utan gallringsbeslut för samtliga handlingar. Det har också fattats vissa delbeslut som möjliggör såväl bevarande som gallring.

Vidare bör bolaget, utifrån skattningen, arbeta vidare med informationsklassificering av sina personuppgiftsbehandlingar och utifrån klassningarna informera medarbetare om hur information ska hanteras och lagras.

2.4.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

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

Dataskyddsombudets kommentarer:

Bolagets skattning är lägre på denna kontrollpunkt än föregående år. Det övergripande resultatet ligger kvar på nivå 3, men börjar närma sig nivå 2, vilket innebär att det inom ramen för kontrollpunkten kan finnas risker som behöver åtgärdas inom en snar framtid.

Resultatet av skattningen på de 14 frågorna under kontrollpunkten är relativt splittrat, då det förvisso anges att ett flertal rutiner finns på plats, såsom för att identifiera behandlingar med hög risk, inhämta dataskyddsombudets synpunkter efter utförd tröskelanalys och konsekvensbedömning och att genomföra och dokumentera konsekvensbedömningar samt genomföra dem innan nya behandlingar påbörjas. Däremot anges också att det saknas rutiner för att säkerställa att konsekvensbedömningar uppdateras vid förändringar i behandlingen, att inhämta de registrerades synpunkter, att följa upp att de åtgärder som konsekvensbedömningen har identifieras behöver vidtas faktiskt också genomförs samt att säkerställa hur beslut om accepterande av risker i en konsekvensbedömning ska fattas och dokumenteras. Det saknas också metodstöd för att bedöma riskerna för de registrerade i samband med en behandling. Vidare anges att bolaget har bedömt om en konsekvensbedömning behöver utföras för cirka 50% av sina personuppgiftsbehandlingar och att konsekvensbedömningar utförts för cirka 50% av de behandlingar där det sannolikt behöver utföras en sådan.

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

2.4.10 Kontrollpunkt 10: IT-projekt och upphandling

Kontrollpunkten avser verksamhetens organisation och rutiner för hantering av dataskyddsfrågor inom IT-projekt och upphandling. I detta ingår till exempel hur verksamheten integrerar dataskyddsfrågor i arbetet med upphandling av nya, samt utvecklingen av, befintliga system och tjänster.

Dataskyddsombudets kommentarer:

Bolaget har skattat sig ungefär likadant som förra året på denna kontrollpunkt, om än något lägre. Det innebär att man landar på nivå 3, men ganska nära 2. Skattningen indikerar att det finns risker, men att de inte bedöms vara brådskande, omfattande eller allvarliga.

Samtliga av påståendena utom ett har dock besvarats med alternativet *Nej, det stämmer inte bra*, vilket innebär att bolaget fortsatt har behov av att säkerställa att dataskyddsperspektivet finns med i arbetet med nya IT- och digitaliseringslösningar samt vid utvecklingen av redan befintliga system och tjänster. Vid upphandlingen av nya system/tjänster så behöver det även tas med i kravställningen att det finns en anpassning till inbyggt dataskydd och dataskydd som standard.

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

2.4.11 Kontrollpunkt 11: IT-system och digitala verktyg

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

Dataskyddsombudets kommentarer:

Bolaget har skattat sig ungefär likadant som förra året på denna kontrollpunkt. Det innebär att man landar på nivå 3, liksom föregående år. Sammantaget indikerar skattningen att det inom ramen för kontrollpunkten har identifierats risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga.

Bolaget har enligt skattningen goda rutiner för tilldelning och uppföljning av behörigheter i IT-system för att säkerställa att medarbetare enbart har tillgång till det som de behöver för utförandet av sina arbetsuppgifter. Bolaget har också en tydlig överblick av sina kommunikationskanaler och säkerställer att de används i enlighet med bestämmelserna i GDPR. Detsamma gäller att bolaget har heltäckande och uppdaterad dokumentation över samtliga IT-system och digitala verktyg som används i organisationen.

Bolaget behöver fortsatt utföra kontroller så att IT-system och digitala verktyg används på rätt sätt. Därför är det även nödvändigt att verksamheten ser till att informera medarbetarna om korrekt användning av systemen/verktygen. Bolaget behöver även säkerställa att dataskyddsperspektivet beaktas vid införandet och användandet av kostnadsfria tjänster, såsom gratisappar och sociala medier.

Bolaget har skattat sig lågt 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 information om cookies framgår att såväl nödvändiga som icke-nödvändiga cookies samlas in. Nödvändiga cookies kräver inget samtycke enligt lagen (2022:482) om elektronisk kommunikation för att få samlas in (tidigare SFS 2003:389) för att få samlas in, däremot krävs det för icke nödvändiga cookies. Det ska vara lika lätt för den enskilde att tacka nej till icke-nödvändiga cookies som att tacka ja. Bolagets cookie-ruta är därför inte i enlighet med lagkraven. Bolagets information om cookies anger inte heller hur besökaren går till väga för att tacka nej till cookies. Bolagets rekommenderas därför att uppdatera cookierutan. Dataskyddsenheten bistår gärna med rådgivning så att utformning blir korrekt.

Vid kontroll av bolagets hemsida framgår att det finns flera tredjepartsförfrågningar som riskerar medföra risk för tredjelandsöverföring, vilket bolaget bör se över.

Avseende sociala medier så använder bolaget såväl Facebook som LinkedIn och Instagram. Vid avstämning med bolaget framgår att det pågår en

koncerngemensam översyn av de sociala medierna, inte minst med hänsyn till domen i Schrems II-målet.

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

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

Bolagets skattning är lägre än förra året och bolaget ligger nu på nivå 3 istället för 4. Det är positivt att bolaget, enligt svaren på frågorna, fortsatt har efterfrågade rutiner avseende hantering av de registrerades rättigheter. Enligt skattningen behöver bolaget dock arbeta vidare med att medvetandegöra medarbetarna i bolaget om de registrerades rättigheter.

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 ~~b~~olaget under 2023 prioriterar följande delar av dataskyddsarbetet:

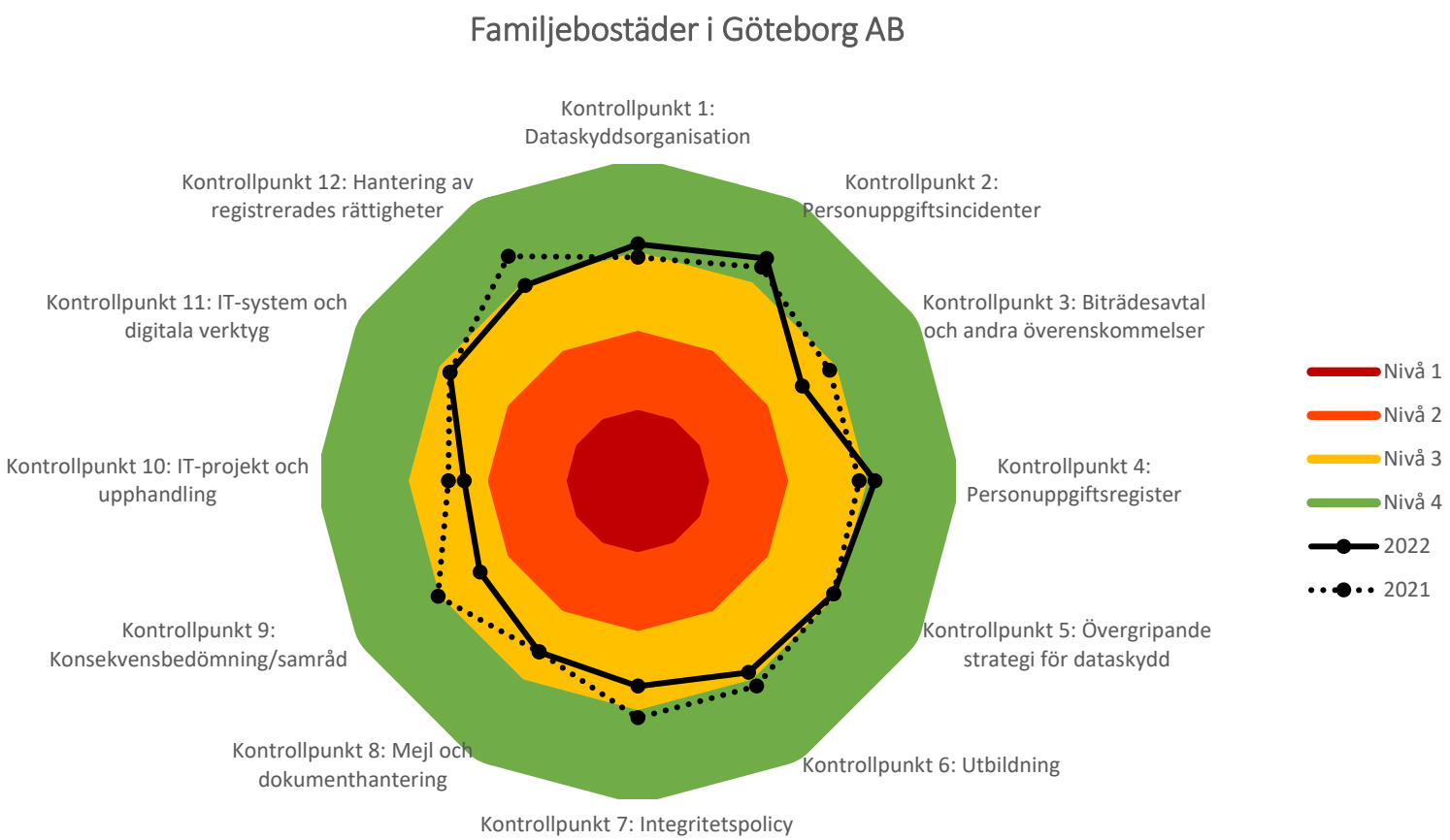
- Kontrollpunkt 8: Mejl- och dokumenthantering
- Kontrollpunkt 9: Konsekvensbedömning/samråd
- Kontrollpunkt 10: IT-projekt och upphandling
- Kontrollpunkt 11: IT-system och digitala verktyg

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 Familjebostäder

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.

Familjebostäders användning av kamerabevakning

Bolaget bedriver kamerabevakning på sju adresser i Göteborg Stad i syfte att verka brottsförebyggande och underbygga rättsliga anspråk. Tillsammans med Gärdsås torg KB (som bolaget är delägare i) bevakas 14 ställen på utsidan runt affärshuset Gärdsås torg. Något tillstånd för övervakningen har inte sökts för de sju adresserna, men däremot har det sökts och delvis beviljats för kamerabevakningen på Gärdsås torg. Bevakningen på Gärdsås torg kommer inte ingå i kontrollen eftersom den trots allt genomförs av ett annat bolag som är personuppgiftsansvarigt.

Dataskyddsombudets rekommendationer

Tillstånd

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

Bolaget uppger att man inte sökt något tillstånd för kamerabevakningen av de sju adresserna i staden då bolagets övervakning inte är tillståndspliktig. Under förutsättning att den information som bolaget inkommit med är korrekt instämmer dataskyddsombudet i att majoriteten av kamerabevakningarna inte är av en sådan art att den kräver ett tillstånd för att få genomföras. För adresserna Lisa Sass gata 16 och 18 framgår dock att kamerabevakning sker i entré och trapphus. Omständigheter såsom bevakning av entré skulle kunna medföra tillståndsplikt om det är yttre entré som avses. IMY anger just bevakning av yttre entré som exempel på när kommunala bostadsbolags bevakning är tillståndspliktig.[1] Vid muntlig avstämning med bolaget framgår att det enbart är inre entré som bevakas. Dataskyddsombudet instämmer därför med bolaget i att bevakningen inte är tillståndspliktig.

Tider och platser som kamerabevakas

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

Familjebostäder bedriver kamerabevakning på Ostindiegatan 20, Slottsskogsgatan 18, Klareborgsgatan 5, Opalgatan/Bronsåldersgatan, Siriusgatan 78 och Lisa Sass gata 16 och 18. De fem första bevakningarna sker av parkeringsgarage, medan bevakningarna på Lisa Sass gata 16 och 18 sker i entré/trapphus. Kamerabevakningen sker dygnet runt på dessa adresser, men aktiveras först vid rörelse.

Utifrån den information som dataskyddsombudet har tagit del av förefaller det inte orimligt, med hänsyn till ändamålet med kamerabevakningen, att bevakningen i stort sker dygnet runt och på det sätt som sker. Bolaget bör dock överväga om bevakningen på i

[1] Se Integritetsskyddsmyndighetens vägledning om kamerabevakning, rapport 2021:2, s. 40.

entréer och trapphus på Lisa Sass gata, bör ske dygnet runt. Detta eftersom det anses särskilt integritetskänsligt att bevaka denna typ av plats, i nära anslutning till de registrerades hem.

Avseende lagringstid har bolaget uppgett att lagring sker i max 21 dagar, men av vissa underlag framgår en kortare lagringstid om 14 dagar. Huvudregeln för inspelat material är att det får lagras i 72 h, vilket gör att bolagets lagringstid klart överstiger huvudregeln. Det är dock möjligt att frångå huvudregeln om det finns skäl för det, men man behöver då tydligt ange och bedöma hur lång tid det tar för verksamheten att upptäcka en incident och hur lång tid det tar att omhänderta materialet för att skicka det till polisen vid brott. Bolaget har i vissa underlag angivit att semestertider och därmed svårighet att få ut materialet genom den person eller de personer som har tillgång till materialet.

Dataskyddsombudet förstår att en längre lagringstid än huvudregeln på 72 h kan vara berättigad. Såväl 14 som 21 dagar är dock ett stort avsteg från huvudregeln. Bolaget rekommenderas dokumentera och motivera 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.

Familjebostäder har angett att ändamålet med behandlingen är att förebygga brott och att underbygga rättsliga anspråk.

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. 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 med för vissa av kamerabevakningarna, men det bör säkerställas att det finns en tydlig intresseavvägning 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.

Konsekvensbedömningar har utförts för Lisa Sass gata, Opalgatan, Bronsåldersgatan 56 samt för Klareborgsgatan och Siriusgatan. Dataskyddsombudet finner det positivt att konsekvensbedömning har genomförts för flera av bolagets bevakningar.

Bolaget har angett att konsekvensbedömningarna ska ses över framåt, vilket dataskyddsombudet anser är positivt. Underlagen innehåller en bedömning om att konsekvensbedömningen inte behöver stämmas av med dataskyddsombudet. När dataskyddsombudet inte involveras i en konsekvensbedömning kan en konsekvensbedömning inte anses fullständig. Den personuppgiftsansvarige ska alltid involvera dataskyddsombudet vid utförandet av en konsekvensbedömning enligt art. 35.2 GDPR. Dataskyddsombudet rekommenderar därför att bolaget i samband med översynen av utförda konsekvensbedömningar, säkerställer att dataskyddsombudets rekommendationer inhämtas.

Säkerhet för bevakningen

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

Bolaget uppger att tekniken som används är lagrad video, systemet som används på anläggningarna heter Milestone Express+ och Avigilon Control Centre 5. All video lagras endast lokalt med begränsade behörigheter och raderas automatiskt efter aktuell tidsbegränsning. Endast bild spelas in. Leverantörer för anläggningarna heter Låsteam och Safeteam. Personuppgiftsbiträdesavtal har tecknats med Låsteam och sedermera även för Safeteam avseende behandlingen kamerabevakning.

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. Ytterligare information finns på bolagets hemsida avseende personuppgiftsbehandlingen 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 tillämpningen av information i flera lager. Informationen på hemsidan kan med fördel förtydligas avseende lagringstid då den informationen är mycket allmänt hållen, vilket kan innebära svårighet för den registrerade att avgöra vad som är korrekt information. I och med att det finns flera bevakningar med olika lagringstid har dataskyddsombudet förståelse för att det är svårt att ange specifik lagringstid på hemsidan. I sådana fall kan det räcka att tydligt ange att lagringstiden anges vid aktuell bevakning och att den kan variera mellan exempelvis 72 timmar och fem dagar beroende på de bedömningar som har gjorts för olika bevakningar.

Sammanfattade rekommendationer

- Se över den generella lagringstiden ytterligare för att säkerställa att den verkligen är befogad i förhållande till ändamålen och omständigheterna kring hur lång tid det tar att upptäcka och hantera en incident.
- I samband med översynen av utförda konsekvensbedömningar, inhämtar dataskyddsombudets rekommendationer.
- Förtydliga informationen om lagringstid på hemsidan.

Bilagor

- Frågor och informationsutskick

Information om fördjupad kontroll 2022

Kontrollpunkt 11: Kamerabevakning

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

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

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

Tillvägagångssätt

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

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

Fördjupad kontroll 2022

Kontrollpunkt 11: Kamerabevakning (del 1)

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

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

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

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

Har du frågor, kontakta ditt huvudansvarige dataskyddsombud.

Fördjupad kontroll 2022

Kontrollpunkt 11: Kamerabevakning (del 2)

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

1. 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.

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

   - **Uppföljande frågor:** Utveckla svaret och beskriv tekniken avseende Milestone och Avigilon, sker inspelningen t.ex. med ljudupptagning? Lagras inspelningen i molntjänst?

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

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

Underlaget ska ha inkommit till dataskyddsombudet **senast den 8 juni 2022.**

Har du frågor, kontakta huvudansvarigt dataskyddsombud.