Beslutsunderlag
Styrelsen 2023-01-23
Diarienummer 0015/22

Handläggare: Karin Lange, administrativ chef
Telefon: 031 – 368 54 59
E-post: karin.lange@gshab.goteborg.se

Dataskyddsenhetens årsrapport för dataskyddsarbetet 2022

Förslag till beslut

I styrelsen för Göteborgs Stadshus AB:

Information avseende dataskyddsenhetens årsrapport för dataskyddsarbetet 2022 enligt bilaga 1 antecknas.

Ärendet

Ärendet avser anmälan till styrelsen av dataskyddsenhetens årsrapport för datasskyddsarbetet 2022 för Göteborg Stadshus AB.

Det är stadens nämnder och styrelser som har det yttersta ansvaret för att dess verksamhet följer dataskyddslagstiftningen. Dataskyddsenheten är dataskyddsombud för verksamheterna i Göteborgs Stad och enheten har arbetat fram en modell för sitt kontrollarbete som utgår från en gemensam kontrollplan för stadens verksamheter. 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.

Kontrollarbetet under 2022 för Göteborgs Stadshus AB (Stadshus) har resulterat i bilagda årsrapport, vilken innehåller resultatet av granskningen 2022 för en fördjupad kontrollpunkt, granskning enligt kontrollplan samt uppföljning av tidigare års kontroller.

Stadshus kommer i sitt dataskyddsarbete beakta dataskyddsombudets rekommendationer. Stadshus och kommunstyrelsen har samma huvudansvarigt dataskyddsombud och bolaget samverkar med stadsledningskontoret i sitt dataskyddsarbete.

Enligt dataskyddsenhetens systematik för sitt kontrollarbete kan årsrapporten komma att presenteras av representant från enheten efter överenskommelse.

Styrelsen föreslås att anteckna årsrapporten.

Bedömning ur ekonomisk, ekologisk och social dimension

Ärendet avser anmälan av den årsrapport som dataskyddsenheten lämnat. Bolaget har inte funnit några särskilda aspekter på frågan utifrån dessa dimensioner.

Bilaga

1. Dataskyddsenhetens årsrapport för dataskyddsarbetet 2022

Eva Hessman

Vd, Göteborgs Stadshus AB

Dataskyddsenheten

Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Stadshus AB

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 GDPR
[2] Artikel 38.3 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 hantering av personuppgiftsincidenter, 2022

Den fördjupade kontrollen har bestått av en kontroll av bolagets hantering av inträffade personuppgiftsincidenter under 2021 samt vilka förutsättningar som bolaget har att hantera dessa, utifrån rutiner och stöddokument. Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

Dataskyddsombudet har i rapporten avseende den fördjupade kontrollen haft vissa synpunkter och förslag på förbättringar och har därför lämnat ett antal rekommendationer till verksamheten.

Sammanfattade rekommendationer:

- Bolaget rekommenderas att komplettera mall/checklista med konkret information om hur medarbetare ska hantera personuppgiftsincidenter om dataskyddskontakterna inte är på plats
- Mall/checklista bör kompletteras med instruktioner i hur en bedömning av personuppgiftsincidenter ska bedömas samt instruktioner om när och hur information till registrerade ska ges.
- I mall/checklista tydliggöra vilka andra personer/roller som kan behöva involveras vid utredning av incidenter
- Bolaget rekommenderas att utreda behov av ytterligare utbildning av medarbetare

2.2.2 Uppföljning av tidigare genomförda kontroller

Dataskyddsombudet har under året följt upp vilka åtgärder som vidtagits avseende tidigare års lämnade rekommendationer av gjorda kontroller.

Kontroll (2021): Personuppgiftsregister

Verksamheten gavs följande rekommendationer:

- Klargöra roller, ansvar och arbetssätt i bolagets rutin.
- Se över rättslig grund för de behandlingar som utförs hos bolaget.

Kommentarer och rekommendationer:

Av uppföljningen framgår att arbetet med personuppgiftsregistret är pågående och att uppdateringar sker löpande där rättsliga grunder ses över. Bolaget anger också att det fortsatt arbetas med rutinen. Arbetet är överlag sammankopplat med arbetet med den ändring som sker av bolagets klassificeringsstruktur varför det framåt kommer att behöva ske en samlad insats.

Eftersom arbetet är pågående och strukturen i förändring kommer dataskyddsombudet framåt att följa upp arbetet.

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 Stadshus 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 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 avseende påståenden om dataskyddsorganisationen genomgående angett det näst högsta eller högsta värdet. Det medför en placering inom riskområde fyra vilket indikerar ett systematiskt och välfungerande dataskyddsarbete.

Dataskyddsombudet har inte genomfört någon granskning avseende bolagets organisation och har därför ingen djupare insikt i hur den fungerar. Det har dock inte heller framkommit indikationer som medför en annan bedömning. Dataskyddsombudet rekommenderar att bolaget fortsätter att arbeta för att

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

dataskydd ska vara en integrerad och naturlig del i alla delar av verksamheten. Det rekommenderas också att bolaget kontinuerligt utvärderar den interna organisationen och säkerställer att den har rätt förutsättningar för att bedriva ett effektivt dataskyddsarbete.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Bolaget har inom denna kontrollpunkt angett genomgående höga värden i sin skattning av hur väl arbetet med personuppgiftsincidenter fortlöper inom verksamheten.

Trots bolagets egen skattning och placeringen inom risknivå fyra finns det enligt dataskyddsombudet förbättringar att genomföra. Dataskyddsombudet har inom denna punkt utfört en fördjupad kontroll av incidenthanteringen under 2021 och sett att visst förbättringsarbete bör genomföras. Rekommendationer avseende kontrollen finns sammanfattade under avsnitt 2.2.1 samt i sin helhet i bilaga 2.

Dataskyddsombudet vill också skicka med, vilket kan te sig något motsägelsefullt, att ju fler upptäckta personuppgiftsincidenter desto bättre. Antalet rapporterade incidenter kan utgöra ett mått på hur väl medarbetare är införstådda med vad en incident är (även ett felskickat mejl kan utgöra en incident) och hur den ska hanteras. Dataskyddsombudet rekommenderar att bolaget kontinuerligt utvärderar antalet rapporterade incidenter och säkerställer att medarbetare får regelbunden information och utbildning i incidenthantering.

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:

Svaren inom denna kontrollpunkt indikerar att bolaget har god överblick och kontroll över sina personuppgiftsbiträdesavtal samt överlag goda förutsättningar för att bedöma biträden och underbiträden.

Dataskyddsombudet har under det gångna året inte involverats i någon större utsträckning i frågor gällande biträden och biträdesavtal men gör heller ingen avvikande bedömning avseende bolagets arbete i denna del. Bolaget rekommenderas att fortsätta med efterlevnadskontroller och säkerställa att biträdena uppfyller och följer de krav och instruktioner som framgår av avtalen.

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:

Av skattningen utläser dataskyddsombudet att bolaget i hög utsträckning anser sig efterleva kraven i GDPR i denna del. Utifrån att bolaget anger att ca 75 % av behandlingarna finns upptagna i registret rekommenderar dataskyddsombudet att bolaget gör en översyn för att säkerställa att inga behandlingar har missats i registret.

I övrigt rekommenderas bolaget att fortsätta arbeta med att hålla registret aktuellt och uppdaterat samt säkerställa att det finns fördelat ansvar för de olika behandlingarna.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Bolagets svar i denna del indikerar att det finns en övergripande strategi för dataskyddsarbetet, att det finns en informationssäkerhetspolicy och att man arbetar riskbaserat. Enligt skattningen finns det också styrande dokument som säkerställer att styrande dokument hålls uppdaterade, att informationstillgångar har värderats i relativt stor utsträckning och att det utförs interna kontroller för att säkerställa följsamheten mot GDPR.

Dataskyddsombudet utläser av skattningen att bolaget behöver se över sina rutiner för att efterleva kraven enligt GDPR vid fysiska/digitala sammankomster. Bolaget rekommenderas att ta fram och dokumentera sådana rutiner.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Bolagets svar inom denna kontrollpunkt indikerar att det överlag finns goda förutsättningar i dataskyddsarbetet men att vissa förbättringar kan ske. Placeringen inom risknivå tre indikerar att vissa risker finns men i och med att man ändå gränsar till nivå fyra är det ingen punkt som särskilt sticker ut.

Bolaget rekommenderas att utvärdera utbildningsnivån för att säkerställa att den är tillräcklig för att bedriva ett effektivt dataskyddsarbete.

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:

Skattningen inom denna punkt genererar en placering inom risknivå fyra med inga direkta risker identifierade. Svaren indikerar att bolagets policy i stor utsträckning uppfyller kraven enligt GDPR, att den är tydlig och lättillgänglig samt kontinuerligt uppdateras. Efter en snabb genomgång av den information/policy som finns tillgänglig via bolagets hemsida på goteborg.se gör dataskyddsombudet i viss mån en annan bedömning än den som framgår via bolagets skattning.

Utifrån de krav som ställs på personuppgiftsansvariga att tillhandahålla, konkret, enkel, exakt och tydlig information anser dataskyddsombudet att den lämnade informationen inte uppfyller kraven enligt GDPR i denna del och att informationen behöver ses över. T.ex. anges det att bolaget ibland får personuppgifter från annan än den registrerade själv, det framgår emellertid inte vilken personuppgiftsbehandling det skulle röra sig om eller vad den har för rättslig grund. Det framgår inte heller konkret information om lagring per behandling och vad gäller tredjelandsöverföringar anges detta endast i generella ordalag. Utifrån bolagets personuppgiftsregister framgår ett större antal personuppgiftsbehandlingar som, såvitt dataskyddsombudet kan se, inte täcks in av informationen. Dataskyddsombudet vet dock inte om information om dessa behandlingar lämnas på annat vis.

Dataskyddsombudet rekommenderar att bolaget kartlägger vilka behandlingar som är tänkta att täckas in av policyn via websidan och tydligt redogör för den

obligatoriska informationen där. I detta rekommenderas det att bolaget informerar i lager (skikt) för att säkerställa att de registrerade får fullständig information medan det samtidigt säkerställs att den är lättläst och lättillgänglig. För de behandlingar som eventuellt inte är tänkta att ingå i policyn på hemsidan behöver bolaget säkerställa att fullständig information lämnas på annat vis till de registrerade.

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:

Den sammantagna skattningen i denna del indikerar att bolagets e-post och dokumenthantering sker i enlighet med dataskyddsförordningen.

Dataskyddsombudet gör ingen annan bedömning än den som görs via bolagets skattning. Eftersom principerna om lagring- och uppgiftsminimering är grundläggande i dataskyddsförordningen rekommenderar dataskyddsombudet att bolaget kontinuerligt informerar medarbetarna hur dokumenthantering och gallring ska gå till. Utifrån skattningen rekommenderas också bolaget att säkerställa att den klassade informationen är aktuell och att anvisningar om hur informationen får hanteras är uppdaterade.

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 inom denna kontrollpunkt angett främst medelhöga och höga värden i sin skattning. Det anges bland annat att ca 75 % av alla behandlingar har bedömts utifrån höga risker och att det uppskattningsvis finns genomförda och fastställda konsekvensbedömningar i ca 75 % av fallen där detta krävs. Vid genomgång med bolaget angavs att de två konsekvensbedömningar som dataskyddsombudet har varit involverad i är de två konsekvensbedömningar som bolaget har arbetat med/arbetar med. Mot bakgrund av bolagets storlek och typ av verksamhet är det sannolikt relativt få behandlingar som bolaget behöver genomföra konsekvensbedömningar för. Även med denna omständighet i beaktande anser dataskyddsombudet att den höga skattningen i viss mån kan ifrågasättas, särskilt

eftersom arbetet med den ena konsekvensbedömningen är pågående och alltså ännu inte är fastställd. Det bör även finnas behandlingar inom HR-området, t.ex. vad gäller utbetalning av lön och hantering av rehabiliteringsärenden, där kriterierna för när en konsekvensbedömning behöver genomföras kan tänkas vara uppfyllda. Dataskyddsombudet rekommenderar att förvaltningen kartlägger vilka behandlingar som genomförs där kriterierna för när en konsekvensbedömning är uppfyllda och tar fram en konkret plan för hur arbetet på sikt ska kunna genomföras.

Utifrån den egna skattningen rekommenderas bolaget också att säkerställa att beslutade åtgärder i genomförda konsekvensbedömningar följs upp samt ta fram rutiner för att, när det är lämpligt, inhämta registrerades synpunkter.

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:

Skattningen inom denna punkt genererar en placering inom risknivå fyra, med inga direkta risker identifierade.

Dataskyddsombudet har inte varit involverad i någon upphandling eller IT-projekt hos bolaget vilket är rimligt eftersom projekt och upphandlingar där dataskydd är en faktor sker mycket sällan.

Även om det är sällan förekommande behöver det säkerställas att en beredskap finns när det väl inträffar. Bolaget rekommenderas att vid uppkomna IT-projekt och upphandlingar där dataskydd och skyddet för personuppgifter är aktuellt säkerställa dataskyddsperspektivet samt involvera dataskyddsombudet i ett tidigt skede.

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 inom denna kontrollpunkt angett varierande värden i sin skattning som sammanslaget genererar en placering i riskområde tre. Detta innebär att det finns risker identifierade men dessa bedöms inte vara allvarliga eller omfattande.

Utifrån den egna skattningen rekommenderas det att bolaget tar fram rutiner för att systematiskt följa upp att användning av system och digitala verktyg följer uppsatta regler/riktlinjer. Det rekommenderas också att det tas fram en anskaffningsprocess för att säkerställa att nya verktyg och tjänster uppfyller kraven enligt GDPR.

Bolaget anger att Brysselkontoret har behov av att använda sociala medier, vilket också görs i form av Facebook och LinkedIn. Ett ställningstagande finns för denna användning där det bl.a. redogörs för åtgärder som vidtas för, vad dataskyddsombudet antar är, att minska riskerna för de registrerade. Dataskyddsombudet anser det vara positivt att bolaget har arbetat aktivt med frågan och sett över sin användning. Dataskyddsombudet vill dock ändå lyfta att denna användning är dataskyddsmässigt problematisk. Det går att ifrågasätta om det för de tredjelandsöverföringar som sker av personuppgifter för vilka bolaget är personuppgiftsansvarig finns ett tillämpligt överföringsverktyg enligt kapitel 5.

I enlighet med tidigare rekommendationer från dataskyddsenheten om tredjelandsöverföringar efter Schrems II-domen avråder dataskyddsombudet från alla överföringar av personuppgifter till tredjeland där kraven i GDPR inte kan uppfyllas. Bolaget rekommenderas att dokumentera sin bedömning av behandlingarna som sker i sociala medier och huruvida lagenlighet kan säkerställas. Om detta inte är möjligt rekommenderar dataskyddsombudet, utifrån rådande rättsläge, att behandlingarna avbryts.

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 på denna punkt angett medelhöga och höga värden i sin skattning. Dataskyddsombudet har inte involverats i någon fråga kopplad till rättigheter under året och bolaget har angett att det generellt sett är ovanligt att de kontaktas av registrerade i detta avseende.

Bolaget uppmanas att säkerställa att det även framåt finns en beredskap och förutsättningar för att hantera inkomna frågor och begäranden från registrerade rörande deras 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 bolaget under 2023 prioriterar följande delar av dataskyddsarbetet:

- Kontrollpunkt 4: Personuppgiftsregister
- Kontrollpunkt 11: IT-system och digitala verktyg

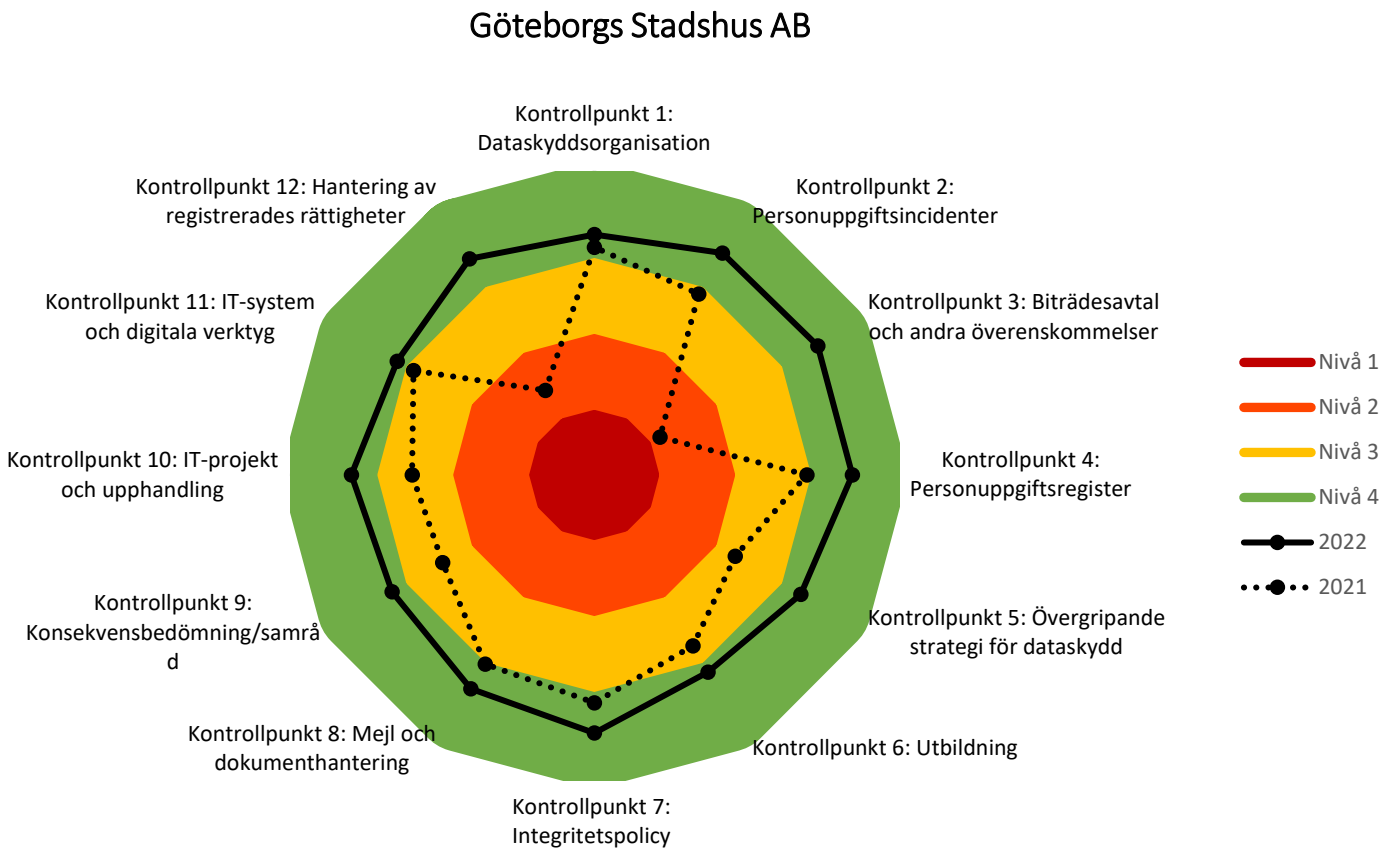
3 Bilagor

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

Bilaga 2: Fördjupad kontroll 2022, hantering av personuppgiftsincidenter under 2021

Bilaga 1

Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.



Fördjupad kontroll 2022

Kontrollpunkt 2: Hantering av personuppgiftsincidenter under 2021

Bakgrund

Den fördjupade kontrollen gällande personuppgiftsincidenter har haft till syfte att undersöka om det finns förutsättningar för verksamheten att hantera personuppgiftsincidenter på ett korrekt sätt som följer dataskyddsförordningen och om förvaltningens rutiner/handlingsplaner får önskat genomslag i praktiken. Kontrollen har genomförts i två delar där del ett har bestått av att verksamheten har ombetts att skicka in dokumentation av rutiner/handlingsplaner för hanteringen av incidenter och dokumentation över inträffade incidenter under 2021. Del två har bestått av frågor kopplade till organisationens incidenthantering.

lakttagelser från kontrollen

Personuppgiftsincidenter kan leda till allvarliga konsekvenser för registrerade personer och det är av stor vikt att de hanteras på ett korrekt sätt. Enligt dataskyddsförordningen ska vissa typer av personuppgiftsincidenter anmälas till tillsynsmyndigheten och i vissa fall ska även de registrerade informeras. Även de personuppgiftsincidenter som inte behöver anmälas till tillsynsmyndigheten ska dokumenteras.

IMY:s checklista vid personuppgiftsincidenter

Integritetsskyddsmyndigheten (IMY) har på sin hemsida publicerat en checklista för personuppgiftsansvariga att använda i sitt arbete med personuppgiftsincidenter. Den består dels av vilka åtgärder personuppgiftsansvariga kan vidta i sitt proaktiva arbete med personuppgiftsincidenter, dels vad som behöver göras vid redan inträffade incidenter. IMY lyfter bl.a. att de som behandlar personuppgifter behöver veta hur man identifierar en personuppgiftsincident och vikten av att rutiner och handlingsplaner finns på plats för att kunna begränsa och hantera en redan inträffad incident. Av rutinerna bör det framgå hur en bedömning av riskerna för de registrerade går till och i förlängningen om det behöver upprättas en anmälan till tillsynsmyndigheten och om de registrerade ska informeras.

Rutiner och handlingsplaner

Göteborgs Stadshus AB har en checklista och en mall för incidentrapportering. Checklistan innehåller exempel på vanliga anledningar till incidenter, vad en anmälan till tillsynsmyndigheten ska innehålla samt frågor som medarbetarna förväntas känna till (t.ex. vad en incident är, hur och till vem som de ska rapporteras).

Av rapporteringsmallen framgår att personuppgiftsincidenter ska anmälas till bolagets dataskyddskontakt som sedan har till uppgift att utreda och bedöma incidenten. Mallen innehåller ett antal frågor samt hjälptexter som tydliggör vad som efterfrågas. Av de inskickade svaren från bolaget framgår att det inte finns ett eget styrande dokument som utgör stöd för bedömningen av om en händelse är en personuppgiftsincident eller inte. Stöd finns emellertid att få via information på intranät samt att samverkan sker med stadsledningskontoret. Anställda är också instruerade att ta direkt kontakt med

dataskyddsombudet om dataskyddskontakt inte är tillgänglig. Utifrån bolagets storlek och antal anställda har detta bedömts vara en tillräcklig och rimlig nivå av stöd och styrning vid incidentrapportering.

Av det inskickade underlaget framgår att bolaget under år 2021 upptäckt en personuppgiftsincident. Denna incident har inte bedömts vara tillräckligt allvarlig för att kräva en anmälan till tillsynsmyndigheten och har därför enbart dokumenterats internt.

Dataskyddsombudets rekommendationer

Bolagets checklista redogör i breda drag för vad en personuppgiftsincident innebär och innehåller exempel på händelser som utgör en incident, vilket är positivt. Rapporteringsmallen innehåller en beskrivning av tillvägagångssätt vid en misstänkt incident. Det är positivt att det är tydligt utpekat vem som har ansvar vid en misstänkt incident. Mallen eller checklistan bör emellertid kompletteras med uttrycklig information om hur medarbetare ska gå till väga om dataskyddkontakterna inte är på plats.

Dataskyddsombudet rekommenderar också att checklistan eller mallen kompletteras med instruktioner i hur en bedömning av personuppgiftsincident ska göras. Även om bolaget är litet och har förhållandevis få medarbetare behöver det finnas tydliga underlag och stöd att få i arbetet med incidenter.

Med tanke på att personuppgiftsincidenter kan vara komplicerade och svårutredda kan det även vara klokt att ta fram instruktioner kring att, i de fall det är lämpligt, kontakta andra personer/roller för att på ett tillfredsställande sätt kunna utreda incidenten. Detta är något som antagligen ter sig självklart för dataskyddskontakter men kan behöva tydliggöras i en rutin för det fall att det faller på någon annan att utreda och rapportera incidenten. Det framgår inte heller några instruktioner om när eller hur registrerade ska informeras om en inträffad incident, vilket ska göras om risken för de registrerade har bedömts som hög. Dataskyddsombudet rekommenderar att bolagets stöddokument kompletteras med denna information, för att säkerställa att det finns en beredskap för det fall en allvarligare incident skulle inträffa.

Av frågeunderlaget framgår att bolagets medarbetare har fått information om dataskyddsförordningen och att utbildningsinsatser har genomförts. Medarbetare har också ombetts att gå den digitala utbildningen ”Dataskydd på jobbet” som dataskyddsenheten har tagit fram och som nås via utbildningsportalen. Mot bakgrund av att bolaget under 2021 endast identifierat en personuppgiftsincident och då till och med ett felskickat mejl kan utgöra en personuppgiftsincident rekommenderar dataskyddsombudet bolaget att utreda om inte ytterligare utbildning kan vara aktuellt.

I takt med att de anställdas kunskaper om dataskydd ökar kan det antas att även antalet identifierade incidenter kommer att öka, vilket bör ses som något positivt. Att helt eliminera risken för personuppgiftsincidenter är inte möjligt och även om ett stort antal personuppgiftsincidenter är en indikation på att något inte funkar som det ska kan det också visa på att anställda har tillräckliga kunskaper för att korrekt identifiera en incident.

Dataskyddsombudet har inte några synpunkter angående de personuppgiftsincidenter som förvaltningen har hanterat under 2021 och instämmer i de riskbedömningar som har gjorts.

Sammanfattning

- Bolaget rekommenderas att komplettera mall/checklista med konkret information om hur medarbetare ska hantera personuppgiftsincidenter om dataskyddskontakterna inte är på plats
- Mall/checklista bör kompletteras med instruktioner i hur en bedömning av personuppgiftsincidenter ska bedömas samt instruktioner om när och hur information till registrerade ska ges.
- I mall/checklista tydliggöra vilka andra personer/roller som kan behöva involveras vid utredning av incidenter
- Bolaget rekommenderas att utreda behov av ytterligare utbildning av medarbetare

Bilagor

- Information om fördjupad kontroll 2022
- Frågeunderlag fördjupad kontroll, del 1 och 2

Fördjupad kontroll 2022

Kontrollpunkt 2: Hantering av personuppgiftsincidenter under 2021

Del 1: Dokumentation för er att skicka in till dataskyddsombudet:

1. Rutiner/handlingsplaner/instruktioner för att hantera personuppgiftsincidenter
2. Dokumentation av inträffade personuppgiftsincidenter
    a. Dokumentation av incidenter som har anmälts till tillsynsmyndigheten
    b. Dokumentation av incidenter som endast har dokumenterats internt
3. Dokumentation av utredningar kring potentiella personuppgiftsincidenter

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

Har du frågor, kontakta ditt huvudansvariga dataskyddsombud.

Fördjupad kontroll 2022

Hantering av personuppgiftsincidenter under 2021 (del 2)

Uppföljande frågor att besvara:

1. Vilken metod/vilket tillvägagångssätt används för att bedöma huruvida händelsen är en personuppgiftsincident eller ej?
    a. *Om det framgår av rutin/handlingsplan/instruktion, hänvisa till vilket dokument samt på vilken sida detta framgår.*
2. Vilken metod/vilket tillvägagångssätt används för att bedöma huruvida incidenten ska anmälas till tillsynsmyndigheten eller ej?
    a. *Om det framgår av rutin/handlingsplan/instruktion, hänvisa till vilket dokument samt på vilken sida detta framgår.*
3. Hur säkerställer ni att era anställda vet vad en personuppgiftsincident är och hur de ska gå tillväga vid inträffade personuppgiftsincidenter?

Svaren ska ha inkommit till ert dataskyddsombud **senast den 9 juni 2022.** Dataskyddsombudet kan komma att ställa kompletterande frågor i samband med sammanställande av rapporten.

Har ni frågor, kontakta huvudansvarigt dataskyddsombud.

Information om fördjupad kontroll 2022

Kontrollpunkt 2: Hantering av personuppgiftsincidenter under 2021

Personuppgiftsansvariga och personuppgiftsbiträden ska arbeta medvetet och proaktivt för att förhindra personuppgiftsincidenter. Om det ändå sker en incident ska det finnas förutsättningar för att hantera den snabbt och på rätt sätt. Den personuppgiftsansvarige är enligt artikel 33.5 GDPR skyldig att dokumentera samtliga inträffade incidenter, oavsett risknivå. Dokumentationsskyldigheten är kopplad till ansvarsskyldigheten i artikel 5.2 GDPR, som innebär att den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna för dataskydd efterlevs. Dokumentationen ska innefatta omständigheterna kring incidenten, dess effekter och de korrigerande åtgärder som vidtagits.

Om det inte är osannolikt att en inträffad personuppgiftsincident medför en risk för registrerades fri- och rättigheter ska, enligt artikel 33 GDPR, den personuppgiftsansvarige anmäla incidenten till Integritetsskyddsmyndigheten inom 72 timmar efter det att personuppgiftsansvarig fått vetskap om incidenten. Den personuppgiftsansvarige behöver vid varje inträffad incident bedöma i vilken utsträckning som den uppkomna incidenten påverkar de registrerades fri- och rättigheter.

Tillvägagångssätt

Den fördjupade kontrollen kommer att genomföras i två delar. I del ett ombeds ni att skicka in dokumentation av rutiner/handlingsplaner för att hantera incidenter samt er dokumentation avseende redan inträffade personuppgiftsincidenter. I del två ombeds ni att svara på ett antal frågor kopplade till er incidenthantering.

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