Göteborgs Stad

Beslutsunderlag
Utfärdat 2022-02-15
Diarienummer 0001/22

Handläggare
Annika Forsgren
Telefon: 031-368 55 07
E-post: annika.forsgren@gotalejon.goteborg.se

Lekmannarevisorernas granskningsredogörelse 2021

Förslag till beslut

- Lekmannarevisorernas granskningsrapport för 2021 förklaras framlagd.

Bilagor

1. Granskningsrapport 2021
2. Lekmannarevisorernas granskningsredogörelse 2021

Granskningsrapport för 2021

Till årsstämman i Försäkrings AB Göta Lejon
Till kommunfullmäktige för kännedom

Org.nr: 516401-8185

Vi, lekmannarevisorer i Försäkrings AB Göta Lejon, har granskat bolagets verksamhet under 2021. Granskningen har utförts av sakkunniga som biträder lekmannarevisorerna.

Bolagets styrelse och verkställande direktör ansvarar för att verksamheten bedrivs i enlighet med lagar och föreskrifter, bolagsordning samt ägardirektiv. Vårt ansvar är att granska om bolagets verksamhet har skötts på ett ändamålsenligt och från ekonomisk synpunkt tillfredsställande sätt och om bolagets interna kontroll har varit tillräcklig.

Granskningen har utförts enligt försäkringsrörelselagen, kommunallagen, kommunens revisionsreglemente, god revisionssed i kommunal verksamhet och med beaktande av de beslut kommunfullmäktige och årsstämman har fattat.

En sammanfattning av granskningen har överlämnats till bolagets styrelse och verkställande direktör i en granskningsredogörelse. Granskningen har genomförts med den inriktning och omfattning som behövts för att ge rimlig grund för vår bedömning.

Vi bedömer att bolagets verksamhet har skötts på ett ändamålsenligt och från ekonomisk synpunkt tillfredsställande sätt och att bolagets interna kontroll har varit tillräcklig.

Göteborg den 9 februari 2022

Tom Heyman
Lekmannarevisor utsedd
av kommunfullmäktige

Alf Landervik
Lekmannarevisor utsedd
av kommunfullmäktige

Göteborgs Stad

Detta dokument är elektroniskt signerat.

Signed by: Tom Heyman
Date: 2022-02-10 10:12:17
BankID refno: 2cf69c39-8752-4875-ac9c-31a25920b085

Lekmannarevisor: Tom Heyman

Signed by: ALF LANDERVIK
Date: 2022-02-10 13:18:44
BankID refno: dac41b7c-80c4-4fcc-b600-a156b1f6173c

Lekmannarevisor: Alf Landervik

Granskning av verksamhetsåret 2021

Vi, lekmannarevisorer i Försäkrings AB Göta Lejon AB, har avslutat granskningen av bolaget avseende verksamhetsåret 2021. Våra iakttagelser och bedömningar framgår av granskningsredogörelsen som bifogas.

Vårt uttalande till årsstämman lämnas i en granskningsrapport. Granskningsrapporten skickar vi till bolaget efter det att styrelsen har beslutat att fastställa årsredovisningen. Uttalandet i granskningsrapporten grundar sig på granskningsredogörelsen.

Göteborg den 19 januari 2022

Tom Heyman
lekmannarevisor utsedd
av kommunfullmäktige

Alf Landervik
lekmannarevisor utsedd
av kommunfullmäktige

Granskningsredogörelse
Stadsrevisionen

Göteborgs Stad

Försäkrings AB Göta Lejon

– granskning av verksamhetsåret 2021

2022-01-19

Januari 2022

Titel: Försäkrings AB Göta Lejon – granskning av verksamhetsåret 2021

Diarienummer: 0173/21

Lekmannarevisorer: Tom Heyman och Alf Landervik

Yrkesrevisor: Susanne Grandin

www.goteborg.se/stadsrevisionen

Innehåll

1 Sammanfattning

Styrelse och vd ansvarar för att bolagets verksamhet bedrivs i enlighet med lagar och föreskrifter, bolagsordning samt ägardirektiv.

Lekmannarevisorernas uppdrag är att granska om bolagets verksamhet sköts på ett ändamålsenligt och från ekonomisk synpunkt tillfredsställande sätt samt om bolagets interna kontroll är tillräcklig.

Lekmannarevisorernas sammanfattande bedömning är att bolaget har skött verksamheten på ett ändamålsenligt och från ekonomisk synpunkt tillfredsställande sätt samt att den interna kontrollen har varit tillräcklig.

Nedan redogör vi kort för respektive område som omfattas av årets granskning.

- **Grundläggande granskning:** Den grundläggande granskningen syftar till att översiktligt bedöma bolagets ledning och styrning samt interna kontroll. Vår översiktliga bedömning är att bolaget har en tillfredsställande ledning och styrning samt tillräcklig intern kontroll inom de områden som vi har granskat.
- **Avtalsuppföljning:** Syftet är att granska bolagets arbete med uppföljning av avtal och inköp. Som grund för bedömning av ändamålsenlig avtalsuppföljning har Upphandlingsmyndighetens vägledning för avtalsförvaltning tillämpats. Vår bedömning är att bolaget har rutiner och ett arbetssätt som säkerställer ett systematiskt och ändamålsenligt arbete med avtalsuppföljning.
- **Följsamhet dataskyddsförordningen:**
  Syftet är att bedöma om styrelsens dataskyddsarbete är ändamålsenligt organiserat. Fokus är följsamhet mot dels dataskyddsförordningen vad gäller verksamhetens organisatoriska förutsättningar för att bedriva ett kontinuerligt dataskyddsarbete och fullgöra kraven om skydd av personuppgifter. Dels kommunstyrelsens krav på dataskyddskontakter och samarbete med dataskyddsombud. Vår bedömning är att bolagets dataskyddsarbete är ändamålsenligt organiserat.

2 Granskning av verksamheten

Styrelse och vd ansvarar för att bolagets verksamhet bedrivs i enlighet med lagar och föreskrifter, bolagsordning samt ägardirektiv.

Lekmannarevisorernas uppdrag är att granska om bolagets verksamhet sköts på ett ändamålsenligt och från ekonomisk synpunkt tillfredsställande sätt samt om bolagets interna kontroll är tillräcklig.

Granskningen av verksamheten omfattar en grundläggande del som är en översiktlig granskning av bolagets ledning och styrning och interna kontroll, samt en del som avser specifika granskningar avseende bolagets följsamhet gentemot dataskyddsförordningen och bolagets arbete med avtalsuppföljning.

2.1 Grundläggande granskning

Den grundläggande granskningen syftar till att översiktligt bedöma bolagets ledning och styrning samt interna kontroll. Det innebär att lekmannarevisorerna löpande följer styrelsens protokoll och handlingar och informerar sig om verksamheten. Granskningen omfattar exempelvis följande:

- följsamhet mot kommunallagen
- följsamhet mot försäkringsrörelselagen
- följsamhet mot bolagets ägardirektiv och bolagsordning
- följsamhet mot kommunfullmäktiges budget
- följsamhet mot Göteborg Stad kommunfullmäktiges styrande dokument, särskilt:
  - kommunfullmäktiges riktlinjer för styrning, uppföljning och kontroll
  - följsamhet mot kommunfullmäktiges regler för ekonomisk planering, budget och uppföljning

2.1.1 Iakttagelser

Inom ramen för grundläggande granskning har vi särskilt granskat följsamhet gentemot ägardirektivet. Fullmäktige beslutade i maj 2020 om ett nytt ägardirektiv för bolaget vilket framför allt berörde ekonomi och effektivitet.

Enligt fullmäktige ska bolaget använda benchmarking för att utveckla verksamhetens effektivitet och produktivitet. Bolaget ingår, enligt uppgift, i ett nätverk med såväl privata som offentliga captives. Samarbete finns exempelvis avseende upphandling av aktuarier. Årligen hanterar styrelsen en omvärlds- och nulägesanalys i vilken bolagets arbete med benchmarking framgår. Lekmannarevisorerna har tagit del av Rapport om omvärlds- och nulägesanalys 2021/2022 som styrelsen antog i september 2021.

Vi har också granskat bolagets följsamhet gentemot fullmäktiges handlingsplan för hur inköps- och beställarkompetens kan förstärkas under år 2021. Enligt bolaget är handlingsplanen under omhändertagande och kommer att följas upp under 2022.

I den grundläggande granskningen har också noterats att styrelsen under året hemställt om ändring av bolagsordning. Anledningen var att möjliggöra för bolaget att själva, utan inblandning från Finansinspektionen, kunna hantera barn- och elevolycksfallsförsäkring för Göteborgs Stads barn och elever. Fullmäktige beslutade om reviderad bolagsordning i oktober månad.

Lekmannarevisorerna kan konstatera att den grundläggande granskningen inte visar på några väsentliga avvikelser.

2.1.2 Bedömning

Lekmannarevisorernas översiktliga bedömning är att bolaget har en tillfredsställande ledning och styrning samt tillräcklig intern kontroll inom de områden som vi har granskat.

2.2 Avtalsuppföljning

2.2.1 Utgångspunkter i granskningen

Lekmannarevisorerna har granskat bolagets arbete med avtalsuppföljning.

Stadsrevisionen har, genom särskilt uppdrag från kommunfullmäktige, ansvar för att löpande följa Stadens upphandlings- och inköpsverksamhet. I stadsrevisionens revisionsplan för år 2021 betonar de förtroendevalda revisorerna vikten av att nämnderna och bolagen har ändamålsenliga rutiner för att följa upp anlitade leverantörer. Med ändamålsenliga avses i sammanhanget rutiner som säkerställer att den upphandlade varan eller tjänsten levereras på ett korrekt sätt, vid rätt tid och i enlighet med avtal.

Syftet är att granska bolagets arbete med uppföljning av avtal och inköp. Som grund för bedömning av ändamålsenlig avtalsuppföljning tillämpas Upphandlingsmyndighetens vägledning för avtalsförvaltning och SKR:s uppföljning av upphandlingskontrakt. Även följsamhet gentemot fullmäktiges riktlinje för inköp och upphandling samt regler för attest granskas.

Metod har utgjorts av intervjuer med ansvariga, dokumentanalys samt tre stickprov på avtal som är av verksamhetskritisk karaktär. Valda avtal rör aktuarie, internrevision och regelefterlevnad.

2.2.2 Iakttagelser

Iakttagelserna är strukturerade utifrån ändamålsenlighet enligt Upphandlingsmyndighetens vägledning, följsamhet mot fullmäktiges riktlinje för inköp och upphandling samt regler för attest.

2.2.2.1 Bolagets arbete med avtalsuppföljning och dess systematik

Avtalsklassificering

Bolaget har gjort en avtalsprioritering för att säkerställa att resurser prioriteras till rätt avtal i sitt uppföljningsarbete. Totalt har bolaget omkring 100 avtal som även innefattar interna avtal och inköp på stadsgemensamma ramavtal. Bolagets verksamhetskritiska avtal utgörs av de utlagda kontrollfunktionerna i verksamheten, det vill säga de som avser återförsäkring, skadereglering, aktuariefunktionen, regelefterlevnad, riskhantering, internrevision och it. Dessa avtal följs, enligt rutin, upp minst två gånger per år. Lekmannarevisorerna har tagit del av styrelsens beslut, i november 2021, över sammanställningen av den utlagda verksamheten och uppdragsavtal med molntjänstleverantör år 2021.

Systemstöd

Vad gäller systemstöd för ärendehantering av avtalen hanteras de i dagsläget i diariet i avvaktan på inrättandet av den staden-gemensamma avtalsdatabasen/ leverantörsdatabasen. Nämnden för inköp och upphandling leder det arbetet som syftar till att öka ordning och reda bland stadens avtal samt skapa bättre överblick och uppföljning av leverantörsdatabasen. Planen är att arbetet ska vara klart under 2022.

Struktur för planering

För de verksamhetskritiska avtalen, det vill säga de avtal som avser bolagets utlagda kontrollfunktioner i verksamheten, upprättas aktivitetsplaner/ granskningsplaner för uppföljning över vad som ska genomföras och av vem och med vilken frekvens samt när. Det är försäkringsrörelselagen och Solvens II-förordningen som reglerar avtalsuppföljning av kontrollfunktionerna. Lekmannarevisorerna har tagit del av aktivitetsplan och agenda. Vad gäller övriga avtal som bolaget ansvarar för, ska dessa följs upp av avtalsansvariga en gång per år, enligt uppgift.

I dagsläget finns ingen övergripande dokumenterad rutin för arbetet med uppföljning av bolagets samtliga avtal som de förfogar över. Enligt vd finns behov av översyn av dokumenterade rutiner och ansvariga, i samband med omorganisationen på bolaget, i syfte att stärka den interna kontrollen och öka kontinuiteten i bolagets arbete.

Uppföljning av krav

Vad gäller kontinuerlig uppföljning av verksamhetskritiska avtal och leverantörers ekonomiska status och skattestatus under avtalsperioden, sker

enligt uppgift, dels kontroll mot Creditsafe, dels en ratingkontroll av återförsäkring en gång per månad via finans-avdelningen på stadsledningskontoret.

Uppföljning av verksamhetskritiska avtal omfattar, enligt rutiner, krav på leverantör (kvalificeringskrav), krav på varan/tjänsten samt utvärderingskriterier (LOU). Dessa krav följs upp vid två tillfällen per år. Kvalificeringskrav som exempelvis särskild yrkeskompetens (CV/kompetens) följs upp genom att granska personella förändringar. Utöver krav enligt upphandlingsavtal granskas avvikelser och förändringar i regelverk. Inkommer klagomål hanteras de som avvikelse.

Enligt uppgift följer bolaget löpande upp volym och pris för avtal genom att attestanten ska kontrollera att fakturor stämmer med avtal.

Bolaget följer upp, eller genomför revision av kvalitet genom att granska kvalitet på skadereglering (verksamhetskritisk) och betalningars korrekthet. Det är, enligt uppgift, avtalsansvarig som tillser detta.

Nämnas ska också att bolaget har en checklista för uppföljning av utlagd verksamhet gällande kritiska eller viktiga operativa funktioner eller verksamheter som följer av försäkringsrörelselagen och Solvens II-förordningen. Lekmannarevisorerna har tagit del av checklistan och av rutin för tecknande av uppdragsavtal innehållande utvärdering av leverantörsavtal.

Sanktioner vid avvikelser

Avvikelser och/eller brister dokumenteras, enligt uppgift, löpande. Lekmannarevisorerna har tagit del av rutin för hantering och rapportering av incidenter/avvikelser/brister samt riktlinje för hantering och rapportering av händelse av väsentlig betydelse. Med händelse av väsentlig betydelse avses sådan som ska rapporteras till Finansinspektionen. Ett exempel är om förmåga att uppfylla åtaganden mot försäkringstagare och andra ersättningsberättigade äventyras. Ett annat är om bolagets stabilitet eller skyddet av försäkringstagares tillgångar äventyras.[1]

Avvikelser/brister kommuniceras, enligt rutin, minst två gånger per år med leverantörer för de verksamhetskritiska avtalen.

Avtalen innehåller bestämmelser om såväl vitesklausuler som uppsägningsklausuler.

Riskanalys

En del av bolagets riskanalys utgörs, enligt uppgift, av en kontinuerlig omvärldsbevakning av branschen liksom risken för oegentligheter.

[1] Finansinspektionens föreskrifter och allmänna råd om tillsynsrapportering för försäkringsrörelse FFFS 2015:13 och IKT enligt EIOPA-BoS 20/600 riktlinje 15.

Dokumentation

Uppföljning av de verksamhetskritiska avtalen dokumenteras, enligt uppgift, i diariet.

2.2.2.2 Fullmäktiges riktlinje för inköp och upphandling

Styrelse arbetar löpande, enligt uppgift, med att följa upp bolagets avrop på staden-gemensamma ramavtal. Det innebär att det är beställaren som kontrollerar att exempelvis beställda varor är av den kvalitet och till det pris som gäller enligt avtal. I annat fall sker en reklamation.

Enligt uppgift tillser bolaget att underrätta förvaltningen för inköp- och upphandling om väsentliga avtalsbrott eller andra allvarliga brister hos en leverantör via deras inrapporteringssystem Arthur.

2.2.2.3 Fullmäktiges regler för attest i Göteborgs Stad

Leverantörsfakturor

Fullmäktiges regler för attest innehåller ett antal kontrollmoment för vad kontrollattestant, beslutsattestant och betalningsattestant ska analysera när det gäller leverantörsfakturor. Exempelvis att varan är mottagen och att fakturan är rätt beräknad.

På frågan om vilka rutiner bolaget har för kontrollattestant, beslutsattestant och betalningsattestant anges att fullmäktiges regler för attest finns att tillgå för var och en på bolagets intranät samt i bolagets attestinstruktion. Proceedo styr kontroll- och beslutsattest och Agresso styr utbetalning två i förening. Belopp över 5 mnkr ska attesteras av styrelseordförande. På bolaget kan samtliga beställa, men det är endast två, utöver vd, som tillåts attestera, enligt uppgift.

På frågan om vilka rutiner bolaget har för att dokumentera och hantera brister såsom exempelvis fel i belopp, underlag, antal eller kvalitet, som upptäcks vid attest, anges att avvikelser rapporteras och följs upp i Stratsys inom vilken bolaget har en egen plattform för uppföljningsrapporter.

2.2.3 Bedömning

Utifrån genomförd granskning kan lekmannarevisorerna konstatera att bolaget har rutiner och ett arbetssätt som säkerställer ett systematiskt och ändamåls-enligt arbete med avtalsuppföljning. Vad gäller följsamhet gentemot fullmäktiges riktlinje för inköp och upphandling samt regler för attest visar granskningen på att dessa styrande dokument följs av bolaget.

2.3 Följsamhet dataskyddsförordningen

2.3.1 Utgångspunkter i granskningen

Lekmannarevisorerna har granskat styrelsens följsamhet gentemot dataskyddsförordningen

Syftet med granskningen är att bedöma om styrelsens dataskyddsarbete är ändamålsenligt organiserat. Fokus är hur styrelsen säkerställer följsamhet mot dels dataskyddsförordningen vad gäller verksamhetens organisatoriska förutsättningar för att bedriva ett kontinuerligt dataskyddsarbete och fullgöra kraven om skydd av personuppgifter. Dels kommunstyrelsens krav på dataskyddskontakter och samarbete med dataskyddsombud.

När det gäller eventuell överföring av personuppgifter till ett tredje land kommer det området inte att beröras inom ramen för denna granskning. Orsaken är att rättsläget i fråga om räckvidden och effekterna av aktuell rättspraxis avseende främst tredjelandsöverföring till USA inte är helt klart i dagsläget.

Metod utgörs av dokumentanalys och intervjuer med ansvariga tjänstepersoner.

2.3.2 Iakttagelser

Granskningens iakttagelser är strukturerade utifrån dataskyddsförordningens krav som avser dataskyddsombud, personuppgiftsansvarig och personuppgiftsbiträde. Vad gäller Göteborgs Stads organisering av dataskyddsombuden finns också krav i beslut från kommunstyrelsen.

2.3.2.1 Dataskyddsombud

Enligt dataskyddsförordningen ska personuppgiftsansvariga som är offentliga organ utse dataskyddsombud vars uppgift är att kontrollera att dataskyddsförordningen följs inom verksamheten genom att bland annat utföra kontroller och informationsinsatser. För personuppgiftsansvariga som ingår i en koncern får gemensamt dataskyddsombud utses, vilket har gjorts i Göteborgs Stad. Stadens dataskyddsombud är organisatoriskt placerade på Intraservice och dess dataskyddsenhet.[2]

Respektive nämnd och styrelse ska, i sin tur, ha minst en utsedd dataskyddskontakt som dataskyddsombudet har som sin huvudkontakt. Dock är möjligt att ha flera dataskyddskontakter. De ska vara kontaktpersoner till dataskyddsombudet och har i uppgift att kanalisera frågor från verksamheten till dataskyddsombudet. Dataskyddskontakter ska ha goda kunskaper i dataskyddsförordningen och annan relevant lagstiftning.[3]

[2] Kommunstyrelsen 2017-08-23 Förslag till ny kommungemensam intern tjänst – organisation för dataskyddsombud enligt EU:s dataskyddsförordning.
[3] Dataskyddsenheten 20180406 Tjänstebeskrivning dataskyddsombud (DSO).

När det gäller dataskyddsombuden ska de enligt dataskyddsförordningen ha följande uppgifter:

• informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar personuppgifter

• följa upp efterlevnaden av lagstiftningen, verksamheternas strategier för skydd av personuppgifter samt ansvarsfördelning

• informera och utbilda i dataskyddsförordningen

• ge råd om risk- och konsekvensbedömningar avseende dataskydd

• samarbeta med och vara kontaktperson till Integritetsskyddsmyndigheten som är tillsynsmyndighet.

Styrelsen har utsett en dataskyddskontakt inom bolaget. Enligt uppgift arbetar bolagets dataskyddsombud från dataenheten på Intraservice med årliga utbildningar till såväl personal som till styrelsen. Därutöver informerar ombudet dataskyddskontakten fyra gånger per år om nyheter och ger råd vilka även meddelas till bolagets övriga anställda. Dataskyddskontakten, i sin tur, rådfrågar dataskyddsombudet å bolagets vägnar. Vidare genomförs regelbundna workshops med dataskyddsombudet och andra dataskyddskontakter i staden. Nätverket kallas cirka en gång per år och senast gällde frågan informationssäkerhet.

Enligt dataskyddsförordningen ska personuppgiftsansvarig och personuppgiftsbiträdet säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter. De ska lämna stöd i utförandet av ovan angivna uppgifter, genom att tillhandahålla de resurser som krävs för att fullgöra uppgifterna och ge tillgång till personuppgifter och behandlingsförfaranden, samt stödja upprätthållandet av dataskyddsombudets sakkunskap.

Enligt uppgift säkerställs och stödjs dataskyddsombudets arbete genom att bolaget utsett en dataskyddskontakt som kommunicerar med ombudet vid behov, exempelvis vid konsekvensbedömning och rådgivning i samband med personuppgiftsincidenter. Enligt uppgift bedöms stödet vara tillräckligt. Enligt uppgift har också personuppgiftsansvarig/personuppgiftsbiträde offentliggjort dataskyddsombudets kontaktuppgifter och meddelat dessa till tillsynsmyndigheten.

Lekmannarevisorerna har tagit del av dataskyddsombudets årsrapport för bolaget 2020, kontrollplan för bolagets dataskyddsarbete år 2021 och delårsrapport i maj 2021. I kontrollplanen för år 2021 framgår att dataskyddsombudet lämnat rekommendationer vid fördjupad kontroll av personuppgiftsbiträdesavtal.

Med anledning av rekommendationerna har bolaget, enligt uppgift, arbetat fram nya personuppgiftsbiträdesavtal i samverkan med deras regelefterlevnadsfunktion på grund av ny lagstiftning. Den nya lagstiftningen avser IKT som är

ett EU-direktiv kring InternKommunikationsTeknik och molntjänster och gäller från år 2020.

2.3.2.2 Personuppgiftsansvarig

Personuppgiftsansvariges ansvarsskyldighet

I dataskyddsförordningen anges personuppgiftsansvariges ansvarsskyldighet som omfattar fem punkter och som vederbörande ska ansvara för och kunna visa att de efterlevs.

Lekmannarevisorerna har tagit del av bolagets integritetsskyddspolicy som är beslutad av styrelsen i april 2021. Av den framgår dataskyddsförordningens krav på att personuppgifter ska 1) behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. 2) Att de ska vara riktiga och uppdaterade. 3) Att felaktiga uppgifter raderas eller rättas utan dröjsmål. 4) Att radera personuppgifterna när de ej längre behövs. 5) Att uppgifter ska skyddas så att ej obehöriga får tillgång till dem och så att de inte förloras eller förstörs.

Tillhandahållande av uppgifter till den registrerade

Av dataskyddsförordningen framgår att information ska tillhandahållas om personuppgifter samlas in från den registrerade.

Lekmannarevisorerna har tagit del av ovan nämnda integritetsskyddspolicy av vilka framgår att information ska ges till den registrerade. Av dokumentet framgår vidare förordningens krav på kontaktuppgifter till personuppgifts-ansvarig, ändamålet med behandlingen, personuppgifter som behandlas och hur länge, vilka som får ta del av personuppgifterna, rätten att inge klagomål till en tillsynsmyndighet, hur och varifrån uppgifterna erhållits.

Motsvarande information ska också tillhandahållas om personuppgifter inte har erhållits ifrån den registrerade, vilket framgår av styrelsens integritets-skyddspolicy. Enligt uppgift erhåller bolaget uppgift från andra men då utifrån fullmakt. Det kan gälla exempelvis sjukvårdsjournaler vid skador och dylikt.

Rätt till rättelse

Av förordningen framgår att den registrerade har rätt att av den personuppgifts-ansvarige att utan onödigt dröjsmål få felaktiga personuppgifter rättade. Lekmannarevisorerna har tagit del av styrelsens integritetsskyddspolicy i vilken framgår en sammanställning över vilka rättigheter den registrerade har, enligt förordningen, och är vägledande vid bedömning av den registrerades begäran.

2.3.2.3 Personuppgiftsbiträde

Personuppgiftsbiträde

I bolagets bilaga till mall för personuppgiftsbiträdesavtal framgår instruktioner. De syftar till att säkerställa att personuppgiftsansvarig ger personuppgiftsbiträde

tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas. Lekmannarevisorerna har tagit del av instruktioner som framgår i avtal mellan personuppgiftsbiträde och aktuariefunktionen.

Avtal mellan personuppgiftsansvarig och personuppgiftsbiträde och krav på avtalets innehåll

Bolagets mall för personuppgiftsbiträdesavtal och bilaga med instruktioner följer dataskyddsförordningens krav på formalia avseende exempelvis föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, att den personuppgiftsansvariges skyldigheter och rättigheter anges, samt hantering av personuppgifter efter det att behandlingen har avslutats.

Vidare reglerar avtalsmallen att personuppgiftsbiträdet endast får behandla personuppgifter på dokumenterade instruktioner från personuppgiftsansvarig, samt att överföring av personuppgifter till tredjeland eller internationell organisation även inbegrips – om tillämpligt.

Därtill innehåller mallen för avtal och bilaga med instruktioner för personuppgiftsbiträdesavtal de krav som framgår av dataskyddsförordningen och vilka åligger personuppgiftsbiträdet. Exempelvis att bistå personuppgiftsansvarig med att se till att skyldigheter om säkerhet för personuppgifter och konsekvensbedömning avseende dataskydd och samråd fullgörs.

Register över behandling

För att säkerställa att personuppgiftsansvarig eller dennes företrädare för ett register för behandling används Draftit som är ett staden-gemensamt register för personuppgiftsbehandlingar.

Enligt dataskyddsförordningen ställs ett antal krav på vilka uppgifter som registret ska innehålla. Exempelvis namn och kontaktuppgifter för personuppgiftsansvarig eller företrädare samt dataskyddsombud, ändamålen med behandlingen, beskrivning av kategorierna av registrerade och kategorierna av personuppgifter, samt kategorier av behandling som har utförts för varje personuppgiftsansvarig.

Revisionen har tagit del av Draftit på plats samt erhållit ett utdrag som innehåller ovanstående krav. Enligt uppgift fungerar Draftit så att registrering låter sig först göras efter det att ett antal obligatoriska uppgifter har angetts.

Säkerhet i samband med behandlingen

Enligt dataskyddsförordningen ska personuppgiftsansvarig och personuppgiftsbiträde arbeta med att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken för fysiska personers rättigheter och friheter. Särskild hänsyn ska tas till risker

såsom oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till personuppgifter.

Enligt uppgift har en riskbedömning gjorts tillsammans med Intraservice av befintliga system i samband med införandet av dataskyddsförordningen utifrån ovanstående aspekter. Vidare sker, enligt uppgift, samarbete mellan personuppgiftsansvarig, personuppgiftsbiträde och leverantörer av it-system.

Som en löpande del av driften av systemet är det Intraservice rutiner som gäller för de krav som återfinns i dataskyddsförordningen vad gäller säkerhet i samband med behandling. Enligt uppgift handlar det exempelvis om pseudonymisering och kryptering av personuppgifter samt förmåga att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystem och -tjänsterna enligt kraven i dataskyddsförordningen.

Enligt uppgift har Intraservice också rutiner för att säkerställa att särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats, vid bedömning av lämplig säkerhetsnivå. Back-up finns, enligt uppgift, vilken kontrolleras årligen.

Anmälan av en personuppgiftsincident till tillsynsmyndigheten och information till den registrerade om en personuppgiftsincident

I dataskyddsförordningen anges regler för att hantera anmälan av personuppgiftsincident samt regler för att informera berörd om incident.

Av bolagets mall för avtal med bilaga framgår rutiner för att säkerställa att personuppgiftsbiträde underrättar personuppgiftsansvarig och att personuppgiftsansvarig anmäler incident som kan medföra risk för en persons rättigheter och friheter.

Lekmannarevisorerna har tagit del av bolagets rutin (mall för avtal med bilaga) för hantering av incident. Av den framgår de krav som anges i dataskyddsförordningen såsom beskrivning av personuppgiftsincidentens art, kontaktuppgifter till dataskyddsombud eller annan person, beskrivning av de sannolika konsekvenserna av incidenten samt beskrivning av åtgärder som vidtagits eller kommer att vidtas av personuppgiftsansvarig. Av rutin framgår också hur personuppgiftsansvarig även ska informera den registrerade om en incident om den leder till en hög risk för fysiska personers rättigheter och friheter.

Personuppgiftsincidenter diarieförs, enligt uppgift, vilket är ett led för dels personuppgiftsansvarig att säkerställa att de dokumenteras, dela att underlätta för tillsynsmyndighetens kontroll, det vill säga Integritetsskyddsmyndigheten.

2.3.3 Sammanfattning

Av genomförd granskning kan stadsrevisionen konstatera att styrelsen vidtagit åtgärder för att organisera arbetet med dataskydd utifrån dataskyddsförordningens föreskrifter.

Exempel på sådana åtgärder är att dataskyddskontakt utsetts för att skapa förutsättningar för ett kontinuerligt dataskyddsarbete. Bland dataskyddskontaktens arbetsuppgifter finns att vidta åtgärder för att omhänderta eventuella rekommendationer från dataskyddsombudet, vilket också har skett. Vidare har styrelsen antagit rutiner, riktlinjer och anvisningar för att säkerställa följsamhet gentemot dataskyddsförordningen och enskilds rätt till skydd av personuppgifter.

2.3.4 Bedömning

Lekmannarevisorernas bedömning är att bolagets dataskyddsarbete är ändamålsenligt organiserat.

3 Lekmannarevisorernas uppdrag och rapportering

Den kommunala revisionen är ett lokalt demokratiskt kontrollinstrument med uppdrag att granska den verksamhet som bedrivs i kommunen.

Lekmannarevisorer är förtroendevalda och utses av kommunfullmäktige ur gruppen förtroendevalda revisorer i kommunen. Lekmannarevisorerna har ett självständigt uppdrag att granska de bolag som helt eller delvis ägs av kommunen. I Göteborg utses två lekmannarevisorer för varje bolag. Revisorerna är oberoende och granskar på kommunfullmäktiges uppdrag och därigenom indirekt också för medborgarna.

Resultatet av lekmannarevisorernas granskning redovisas i granskningsrapporter och granskningsredogörelser.

Revisorerna genomför också särskilda granskningar som i regel rör flera bolag och nämnder. Dessa redovisas löpande under året till kommunfullmäktige i revisionsrapporter.

Revisorerna tar även varje år fram en årsredogörelse som sammanfattar den granskning som gjorts i kommunen under det aktuella året.

Revisorernas rapporter hittar du på www.goteborg.se/stadsrevisionen

4 Språkbruk och revisionstermer

När revisorerna har genomfört en granskning lämnar de ofta rekommendationer till de granskade nämnderna och bolagen. Ibland lämnar de även revisionskritik.

Rekommendationer lämnas när revisorerna ser förbättringsområden i verksamheten. Rekommendationerna syftar till att utveckla och förbättra verksamheten.

Revisionskritik lämnas när revisorerna ser brister i verksamheten som är av mer allvarlig karaktär. Revisionskritik graderas genom begreppen erinran eller anmärkning. Anmärkning är allvarligast. När det gäller nämnderna kan en anmärkning lämnas med eller utan tillstyrkan om ansvarsfrihet.

Under kommande år följer revisorerna upp vilka åtgärder som nämnden eller bolagsstyrelsen har gjort för att följa revisorernas rekommendationer.

Stadsrevisionen
Postadress: Box 2141, 403 13 Göteborg
Besöksadress: Stora Badhusgatan 6
Göteborgs Stads kontaktcenter: 031-365 00 00, kansli: 031-368 07 00
stadsrevisionen@stadsrevisionen.goteborg.se
www.goteborg.se/stadsrevisionen