Göteborgs Stad

Granskning av verksamhetsåret 2021

Vi, lekmannarevisorer i Business Region Göteborg 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 26 januari 2022

Alf Landervik
lekmannarevisor utsedd
av kommunfullmäktige

Susanne Zetterberg Jensen
lekmannarevisor utsedd
av kommunfullmäktige

Göteborgs Stad

Business Region Göteborg

– granskning av verksamhetsåret 2021

2022-01-26

Januari 2022

Titel: Business Region Göteborg – granskning av verksamhetsåret 2021

Diarienummer: 0182/21

Lekmannarevisorer: Alf Landervik & Susanne Zetterberg Jensen

Yrkesrevisor: Max Kvilling & Tim Sahlén

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.

- **Granskning av arbetet med informationssäkerhet:** Syftet med granskningen är att bedöma om bolaget bedriver ett ändamålsenligt informationssäkerhetsarbete. Med ändamålsenligt menar vi om bolaget följer de styrdokument för informationssäkerhet som kommunfullmäktige har beslutat om. Vår bedömning är att bolaget i allt väsentligt bedriver ett ändamålsenligt informationssäkerhetsarbete.

- **Uppföljning av ärendeberedning och beslutsunderlag:** Vår uppföljning visar att rekommendationen som lämnades föregående år är omhändertagen.

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 samt interna kontroll, en fördjupad granskning av bolagets arbete med informationssäkerhet samt uppföljning av tidigare års granskning.

2.1 Grundläggande granskning

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

- följsamhet mot tillämpliga delar av aktiebolagslagen
- följsamhet mot tillämpliga delar av kommunallagen
- följsamhet mot bolagsordningen
- följsamhet mot kommunfullmäktiges ägardirektiv
- följsamhet mot kommunfullmäktiges riktlinjer för ägarstyrning
- följsamhet mot kommunfullmäktiges budget
- följsamhet mot kommunfullmäktiges riktlinjer för styrning, uppföljning och kontroll
- följsamhet mot kommunfullmäktiges regler för ekonomisk planering, budget och uppföljning
- styrning och uppföljning av verksamhet och ekonomi
- beslutsunderlag
- hantering av särskilda uppdrag från kommunstyrelsen/ kommunfullmäktige.

2.1.1 Iakttagelser

Den grundläggande granskningen visar inte 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 Informationssäkerhet

2.2.1 Utgångspunkter i granskningen

Lekmannarevisorerna har granskat bolagets arbete med informationssäkerhet Syftet med granskningen har varit att bedöma om bolaget bedriver ett ändamålsenligt informationssäkerhetsarbete. Med ändamålsenligt menar vi att bolaget följer de styrdokument för informationssäkerhet som kommunfullmäktige har beslutat om.

En del av informationen som hanteras inom Göteborgs Stad är mycket värdefull, både för organisationer och för enskilda personer. Informationssäkerhet handlar om att skydda informationen så att:

- den alltid finns tillgänglig när den behövs.
- den är korrekt och inte manipulerad eller förstörd.
- endast behöriga personer kan ta del av den.

Arbetet med informationssäkerhet tar sin utgångspunkt i stadens säkerhetspolicy. Av policyn framgår bland annat att säkerhetsarbetet ska vara långsiktigt och kontinuerligt samt att arbetet ska bedrivas med utgångspunkt i kontinuerliga riskanalyser. Arbetet med informationssäkerhet konkretiseras i sin tur i Riktlinje för informationssäkerhet. Riktlinjen beskriver bland annat att samtliga bolag och nämnder ska:

- klassificera sin information utifrån stadens klassificeringsmodell.
- skapa en förteckning över samtliga informationssystem.
- besluta om en kontinuitetsplan.
- säkerställa att alla anställda har tillräckliga kunskaper om informationssäkerhet i förhållande till sina arbetsuppgifter.
- följa upp informationssäkerhetsnivån årligen och rapportera resultatet till nämnd/styrelse.

Vi har genomfört granskningen genom dokumentstudier samt intervjuer med ansvariga tjänstepersoner. Vi har också intervjuat systemansvariga och systemägare för systemen Hogia och Superoffice. Hogia är bolagets löne- och personalsystem och Superoffice är bolagets CRM-system (det system där bolaget samlar informationen om sina kunder).

2.2.2 Iakttagelser

2.2.2.1 Organisation

Bolaget har beskrivit sin organisation för informationssäkerhetsarbetet i dokumentet ”Systemförvaltning inom BRG”. Där står bland annat att varje system ska ha en utsedd systemägare och systemansvarig. Systemägaren har det övergripande ansvaret för hur systemet ska förvaltas. Systemansvarig har i sin tur ansvaret för den dagliga användningen av systemet. Dokumentet redogör

inte uttryckligen för vem som är informationsägare för informationen i systemen.

Bolaget har utsett en IT-ansvarig som har det övergripande ansvaret för att systemen håller den tekniska och funktionella kvalitet som systemägarna efterfrågar. Enligt stadens säkerhetspolicy ska varje bolag även ha en säkerhetschef som ska driva och hålla ihop, initiera och genom stöd och uppföljning utveckla säkerhetsarbetet. BRG har utsett HR-chefen till säkerhetsansvarig, men inom området informationssäkerhet är det i praktiken IT-ansvarig som genomför de uppgifter som i stadens säkerhetspolicy är ålagda säkerhetschefen. Den säkerhetsansvariges ansvar framgår inte i dokumentet ”Systemförvaltning inom BRG”.

I november 2020 genomförde Göteborgs Stad en undersökning av samtliga nämnders och bolags digitala mognad. Syftet var att mäta stadens förmåga att tillgodogöra sig nyttorna med digitalisering. Undersökningen gjordes med metoden DiMiOS (Digital mognad i offentlig sektor) som har tagits fram av ett forskningskonsortium på uppdrag av Regeringskansliet. Den mäter digital mognad baserad på ett flertal parametrar så som informationssäkerhet, infrastruktur, styrning och organisation. BRG blev med ett resultat på 80 % rankade som den verksamhet i staden med högst digital mognad. Näst bäst resultat av stadens bolag och nämnder fick ett annat bolag på 66 %.

2.2.2.2 Följsamhet mot riktlinjen för informationssäkerhet

Ett första steg i arbetet med informationssäkerhet är att klassa sin information utifrån hur skyddsvärd den är. I stadens riktlinje står det att informationsklassning ska göras kontinuerligt och att klassningen ska ligga till grund för hur informationen ska hanteras i verksamheten. I riktlinjen finns även en modell som bolag och nämnder ska använda när de klassar sin information. Bolaget har i granskningen visat att de arbetar enligt stadens riktlinje och att informationsklassningen utgår ifrån stadens modell.

Den information som bolaget har gett högsta säkerhetsklassning är de personuppgifter som bolaget hanterar i löne- och HR-systemet. Bolaget uppger i intervju att all övrig information också hanteras enligt de säkerhetskrav som staden har på information med den högsta säkerhetsklassningen. Detta eftersom all information finns lagrad lokalt hos bolaget och inte i någon molntjänst.

Enligt stadens riktlinje för informationssäkerhet ska bolaget ha en förteckning över samtliga informationssystem. Förteckningen ska visa ändamålet med systemet samt hur ansvaret för systemet är fördelat. Bolaget har publicerat en sådan förteckning på sitt intranät. Förteckningen anger vem som är systemägare respektive systemansvarig men det framgår inte alltid vad som är systemets användningsområde eller vem som är informationsägaren.

Riktlinjen för informationssäkerhet beskriver också hur bolaget ska arbeta med åtkomst och behörigheter. Riktlinjen anger bland annat att åtkomst och behörighet ska ges restriktivt och styras utifrån de krav som ställs på den anställdes roll. Hos bolaget behöver en anställd ansöka om behörighet till ett system. Ansökan ska godkännas av medarbetarens chef. I intervju framgår att samtliga som anställs får en standardbehörighet till Superoffice. En sådan behörighet ger möjlighet till att läsa all öppen information i systemet. Bolaget beskriver att samtliga anställda ska kunna ha tillgång till de aktiviteter bolaget har haft tillsammans med kunden. Dels för att förbättra kundens upplevelse, dels för att kunna arbeta mer effektivt. Bolaget har gjort bedömningen att nyttan är större än den risk det innebär att ge samtliga anställda behörighet. Granskningen visar att bolaget uppfyller övriga krav vad gäller åtkomst och behörigheter.

Enligt riktlinjen för informationssäkerhet i Göteborgs Stad ska det finnas en formellt fastlagd rutin för hur informationssystemets användare ska agera vid incidenter. Det ska också finnas rutiner för rapportering, loggning, åtgärdande, informationsspridning, eskalering, uppföljning och analys av incidenter. Av intervjuer framgår att det inte finns någon formellt fastlagd rutin för hur bolagets anställda ska agera vid incidenter.

Göteborgs Stad ställer även krav på att bolaget ska ha en kontinuitetsplanering, det vill säga en plan för att säkerställa bolagets verksamhet vid allvarliga störningar av IT-miljön. Bolaget har en kontinuitetsplan som är beslutad av bolagets IT-strategigrupp. I intervjuer framgår också att planen testas årligen samt att en parallell IT-miljö har satts upp för att genomföra återstartstester.

Slutligen är en viktig punkt i riktlinjen för informationssäkerhet att personer som ska få tillgång till information och informationssystem ska ha tillräckliga kunskaper om informationssäkerhet. Bolaget genomför kontinuerligt utbildningar för att stärka personalens kunskap i informationssäkerhet. Under våren 2021 har bolaget haft obligatoriska utbildningar för samtliga anställda i informationshantering av dokument och e-post.

2.2.2.3 Riskanalyser och rapportering till styrelsen

Enligt stadens säkerhetspolicy ska säkerhetsarbetet utgå från kontinuerliga riskanalyser och tyngdpunkten ska ligga på förebyggande aktiviteter. Hur riskanalyser ska genomföras framgår dock inte av stadens styrande dokument. Däremot finns stöddokumentet ”Rådet för riskanalys avseende informationssäkerhet” för vägledning. Rådet beskriver en metod som bygger på genomförd informationsklassning och att de tre skyddsaspekterna konfidentialitet, riktighet och tillgänglighet ska beaktas vid analys och utvärdering.

Bolaget framför i intervjuer att riskanalys och riskhantering avseende informationssäkerhet sker löpande kopplat till förändringar i system och i omvärlden. Bolaget har även ett övergripande systematiskt riskhanteringsarbete

där informationssäkerhet ingår. I det arbetet har bolaget brutit ned informationssäkerhet till olika riskområden. Till respektive riskområde finns åtgärder och kontrollaktiviteter. Bolagets egen bedömning är att riskerna kopplade till informationssäkerhet är hanterade med tillräckliga åtgärder. Det övergripande riskhanteringsarbetet resulterar i en samlad riskbild som tillsammans med en internkontrollplan årligen beslutas av styrelsen. Där rapporterar bolaget den övergripande risken informationshantering där bland annat risken för informationssäkerhet ingår. Det rapporteras även hur bolaget har hanterat risken.

Av intervjuer framgår även att bolaget gör riskanalyser vid införskaffandet av nya system, samt vid utveckling av befintliga system. Detta bekräftas av intervju med bolagets dataskyddsombud som även skriver i sin delårsrapport att bolaget har en rutin som säkrar att informationssäkerhet omhändertas i de upphandlingar som bolaget utför samt att bolaget då använder de styrande och rådgivande dokument som finns i staden gällande informationsklassning och riskanalys.

2.2.3 Bedömning

Det är lekmannarevisorernas bedömning att bolaget i huvudsak följer de styrdokument för informationssäkerhet som kommunfullmäktige har beslutat om och att bolaget därmed bedriver ett ändamålsenligt informationssäkerhetsarbete. Bolaget har klassificerat sin information i enlighet med riktlinjen för informationssäkerhet, tagit fram en kontinuitetsplan som innehåller de delar riktlinjen kräver samt utfört regelbundna utbildningar kopplade till informationssäkerhet. Bolaget genomför även årligen riskanalyser av informationssäkerheten och styrelsen får en återrapportering av att säkerhetsnivån är acceptabel.

Granskningen visar också att bolagets informationssäkerhetsarbete har en tyngdpunkt på förebyggande aktiviteter, ett arbetssätt som följer stadens säkerhetspolicy. Då bolaget är relativt litet har de anställda ofta ett brett ansvarsområde. Detta gäller även arbetet med informationssäkerhet. Lekmannarevisorerna ser därför positivt på att bolaget fortsätter dokumentera arbetet med informationssäkerhet. Bolaget behöver komplettera dokumentationen med en fastlagd rutin för hantering av incidenter.

2.3 Uppföljning av ärendeberedning och beslutsunderlag

Lekmannarevisorerna granskade år 2020 bolagets arbete med ärendeberedning och beslutsunderlag. Granskningen resulterade i att vi riktade följande rekommendation till styrelsen:

Lekmannarevisorerna rekommenderar styrelsen att säkerställa att ärendeberedningen sker i enlighet med Stadshus anvisning.

Vi har i år följt upp denna rekommendation genom att ställa frågor till bolagets företrädare, genom att ta del av bolagets omarbetade mall och rutin samt genom stickprov.

2.3.1 Iakttagelser

Av bolagets yttrande till stadsrevisionen, daterat 2021-06-14, framgår att bolaget har utvecklat sin rutin avseende ärenden av principiell beskaffenhet som ska underställas kommunfullmäktige för ställningstagande. Bolagets vd ansvarar för att säkerställa att sådana ärenden identifieras i god tid så att kommunfullmäktiges ställningstagande hinner inhämtas i tid.

Vi har tagit del av bolagets omarbetade mall för beslutsunderlag och noterat att denna följer Stadshus anvisning avseende bedömning av om ärendet är av principiell beskaffenhet.

Vårt stickprov av fem beslutsärenden visar inte på några avvikelser i förhållande till den nya beslutsmallen.

2.3.2 Bedömning

Rekommendationen är omhändertagen.

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 i regel 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 brister 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 bolaget 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