Göteborgs Stad

Göteborg & Co AB

– granskning av verksamhetsåret 2022

2023-01-18

Så kommunicerar vi våra granskningar

Varje år publicerar stadsrevisionen i Göteborgs Stad sina granskningsresultat på följande sätt:

Publikation	Innehåll
Revisionsredogörelse	Här presenterar stadsrevisionen granskningen av nämnderna. I redogörelserna framgår revisorernas iakttagelser, bedömningar och rekommendationer, i syfte att förbättra verksamheterna.
Revisionsberättelse	Revisorerna upprättar en revisionsberättelse per nämnd. I berättelserna uttalar de sig om nämndernas verksamhet har skötts på ett ändamålsenligt och från ekonomisk synpunkt tillfredsställande sätt, om räkenskaperna är rättvisande samt om nämndens interna kontroll har varit tillräcklig.
Granskningsredogörelse	Här presenterar stadsrevisionen granskningen av bolagen. I redogörelserna framgår iakttagelser, bedömningar och rekommendationer, i syfte att förbättra verksamheterna.
Granskningsrapport	Lekmannarevisorerna upprättar en granskningsrapport per bolag. I rapporterna uttalar sig lekmannarevisorerna om bolagen har skötts på ett ändamålsenligt och från ekonomisk synpunkt tillfredsställande sätt samt om bolagets interna kontroll har varit tillräcklig.
Revisionsrapport	Här presenterar stadsrevisionen särskilda granskningar som i regel rör flera nämnder och/eller bolag – så kallade projektgranskningar. I rapporterna framgår revisorernas iakttagelser, bedömningar och rekommendationer, i syfte att förbättra verksamheterna.
Rapportsammandrag	I rapportsammandragen sammanfattar stadsrevisionen sina revisionsrapporter.
Revisionsberättelse för Göteborgs Stad	Revisorerna upprättar en revisionsberättelse som omfattar kommunens samlade verksamhet. Berättelsen innehåller uttalanden i ansvarsfrågan samt uttalanden om Göteborgs Stads årsredovisning och resultat.
Årsredogörelse	Årsredogörelsen upprättas av stadsrevisionen och innehåller en beskrivning och sammanfattning av de genomförda granskningarna under året.

Januari 2023

Titel: Göteborg & Co AB – granskning av verksamhetsåret 2022

Diarienummer: 0154/22

Lekmannarevisorer: Birgitta Adler och Lars-Gunnar Landin

Yrkesrevisor: Mia van Hoewijk

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.

Granskningen av verksamheten omfattar en grundläggande del, som är en översiktlig granskning av bolagets ledning, styrning och interna kontroll, en fördjupning samt uppföljning av tidigare års granskning.

Vi redovisar våra granskningar genom att först beskriva lekmannarevisorernas bedömningar. Därefter redogör vi för våra iakttagelser.

1.1 Sammanfattande bedömning

Lekmannarevisorernas sammanfattande bedömning är att bolagets styrning och kontroll kan förbättras. Därför lämnar vi rekommendationer till styrelsen och vd. Utöver det bedömer vi 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. Därefter följer en tabell med de rekommendationer vi lämnar.

- **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 informationssäkerhet:** Granskningen syftar till att bedöma om bolagets arbete med informationssäkerhet är tillräckligt i förhållande till Göteborgs Stads säkerhetspolicy och de riktlinjer som finns inom området för informationssäkerhet. Vår bedömning är att arbetet med att säkra den information som bolaget hanterar inte fullt ut följer Göteborgs Stads riktlinje för informationssäkerhet. Vi lämnar därför två rekommendationer till styrelsen och vd (se tabellen sist i sammanfattningen).
- **Uppföljning av granskning: Ägarstyrning mot kommunfullmäktiges mål:** Granskningens syfte var att bedöma om bolaget har en tillräcklig styrning och uppföljning av fullmäktiges övergripande verksamhetsmål för klustret. Vår uppföljande granskning visar att rekommendationen är omhändertagen.
- **Uppföljning av granskning: Hantering av avtal och överenskommelser** Granskningens syfte var att bedöma om det fanns en ändamålsenlig styrning och uppföljning för att säkerställa följsamhet mot de avtal och

överenskommelser som bolaget slutit. Vår uppföljande granskning visar att bolaget har påbörjat ett arbete men att det ännu inte är helt implementerat. De åtgärder som bolaget vidtagit och planerar att vidta gör att vi bedömer att rekommendationen är omhändertagen. Vi kommer att följa arbetet fortsättningsvis.

1.2 Sammanställning av rekommendationer

Område	Rekommendation
Granskning av informationssäkerhet	Lekmannarevisorerna rekommenderar styrelsen att se till att tillämpliga regler, lagar och avtalsrättsliga åtaganden tydligt definieras och dokumenteras för respektive informationssystem och att information som hanteras av externa leverantörer har det skydd som krävs enligt riktlinjen för informationssäkerhet och att det regleras i avtal. Lekmannarevisorerna rekommenderar vd att rapportera informationssäkerhetsnivån till styrelsen i enlighet med riktlinjen för informationssäkerhet.

2 Grundläggande granskning

Den grundläggande granskningen syftar till att översiktligt bedöma bolagets ledning och styrning samt interna kontroll. Styrningen och kontrollen ska vara tillräcklig för att leva upp till mål, beslut och föreskrifter.

Den grundläggande granskningen består av tre övergripande revisionsfrågor:

- Har bolaget genomfört sitt uppdrag på ett ändamålsenligt sätt?
- Har bolaget en ändamålsenlig styrning, uppföljning och rapportering av sin ekonomi?
- Har bolaget sett till att den interna styrningen, uppföljningen och kontrollen är tillräcklig?

Granskningen är avvikelsebaserad och fokuserar i huvudsak på bolagets övergripande systematik, strukturer och arbetssätt.

Granskningen av bolag genomförs under hela granskningsåret. Stadens tidsplan medger inte någon detaljerad granskning av årsrapporten.

2.1 Bedömning

Vår bedömning utifrån en översiktlig granskning är att bolaget har genomfört sitt grunduppdrag på ett ändamålsenligt sätt. Vi bedömer även att bolaget i allt väsentligt har ett ändamålsenligt beslutsfattande.

Vi bedömer att bolaget har en ändamålsenlig styrning, uppföljning och rapportering av sin ekonomi. Slutligen är vår bedömning att bolaget har sett till att den interna styrningen, uppföljningen och kontrollen är tillräcklig.

2.2 Iakttagelser

2.2.1 Har bolaget genomfört sitt uppdrag på ett ändamålsenligt sätt?

Bolaget ska genomföra sitt grunduppdrag enligt bolagsordningen och ägardirektivet samt enligt de mål och riktlinjer som fullmäktige har beslutat om. Fullmäktige har genom budgeten gett bolagsklustren specifika mål som ska uppnås. Fullmäktige har även gett vissa bolag specifika uppdrag som ska genomföras. Vi har översiktligt granskat hur bolaget har genomfört sitt grunduppdrag och arbetat med fullmäktiges specifika mål och uppdrag, i den utsträckning sådana mål och uppdrag finns för bolaget. Vi har även granskat styrelsens protokoll och beslutsunderlag.

Granskningen visar att bolaget i huvudsak har genomfört sitt uppdrag på ett ändamålsenligt sätt. Inga väsentliga avvikelser har noterats.

2.2.2 Har bolaget en ändamålsenlig styrning, uppföljning och rapportering av sin ekonomi?

Bolaget ska se till att det finns en kontinuerlig ekonomisk uppföljning och rapportering. Vi har översiktligt granskat bolagets styrning av ekonomin samt dess ekonomiska uppföljning och rapportering.

Vår granskning visar att bolaget har genomfört en kontinuerlig uppföljning och rapportering av sin ekonomi.

2.2.3 Har bolaget sett till att den interna styrningen, uppföljningen och kontrollen är tillräcklig?

Bolaget ska se till att det finns ett systematiskt arbete med intern styrning och kontroll och riskhantering inom väsentliga områden. Bolaget ska även följa upp och utvärdera detta arbete. Vi har översiktligt granskat bolagets interna styrning, uppföljning och kontroll.

Vår granskning visar att bolaget har upprättat en samlad riskbild och en internkontrollplan. Riskhantering har skett inom väsentliga områden. Granskningen visar att bolaget har ett arbetssätt för att följa upp den interna kontrollen och utvärdera sitt system för styrning, uppföljning och kontroll. I granskningen av informationssäkerhet ser vi att bolaget kan öka sin styrning och uppföljning av informationssäkerhetsarbetet.

3 Granskning av informationssäkerhet

Granskningen syftar till att bedöma om bolagets informationssäkerhetsarbete är tillräckligt i förhållande till Göteborgs Stads säkerhetspolicy och i förhållande till riktlinjer inom området för informationssäkerhet.

Granskningen har genomförts genom intervjuer, analyser av dokument och genom att ta stickprov. På Göteborg & Co har vi tagit stickprov på ett av bolagets egna system. Mycket av bolagets skyddsvärda information, som framför allt är personuppgifter, hanteras i kommungemensamma system. För att få klarhet i hur säkerheten för bolagets personuppgifter hanteras har vd sedan tidigare ställt frågor till förvaltningen för Intraservice. Intraservice har ännu inte besvarat frågorna. Vi har valt att inte ta något stickprov på system där Intraservice är systemförvaltare. Av de it-system som bolaget är systemförvaltare för är det få system som hanterar exempelvis personuppgifter eller annan skyddsvärd information. Det stickprov vi har tagit är från systemet FileMaker Compis. Compis är ett egenutvecklat CRM-system (Customer relationship management) som i första hand lagrar information om befintliga och potentiella kunder. Systemet innehåller personuppgifter och de uppgifter som läggs in godkänns enligt bolaget av de medverkande via ett formulär.

Granskningen syftar till att få svar på följande frågor:

- Arbetar bolaget i enlighet med det regelverk som finns för informationssäkerhet?
- Har bolaget en tillräcklig styrning och uppföljning av informationssäkerhetsarbetet?
- Har bolaget ett arbete som motsvarar dataskyddsförordningens krav på enskildas rätt till skydd av personuppgifter?

Utgångspunkter i granskningen har varit:

- Dataskyddsförordningen, artikel 5, 13–16 och 28
- säkerhetspolicy för Göteborgs Stad
- riktlinje för informationssäkerhet
- regler gällande informationssäkerhetsansvar för chefer i Göteborgs Stad
- regler för IT-användare i Göteborgs Stad.

3.1 Bedömning

Det är vår bedömning att arbetet med att säkra den information som bolaget hanterar inte fullt ut följer Göteborgs stads riktlinje för informationssäkerhet.

Utöver att se till att tillämpliga regler, lagar och avtalsrättsliga åtaganden tydligt definieras och dokumenteras för respektive informationssystem bör bolaget försäkra sig om att innehållet i riktlinjen för informationssäkerhet regleras i avtal, om information hanteras av externa leverantörer. Bolaget bör också se till att de övervakar och har möjlighet att följa upp om riktlinjen för informationssäkerhet följs av externa leverantörer.

Vi riktar därför följande rekommendationer till styrelsen och vd:

Lekmannarevisorerna rekommenderar styrelsen att se till att tillämpliga regler, lagar och avtalsrättsliga åtaganden tydligt definieras och dokumenteras för respektive informationssystem och att information som hanteras av externa leverantörer har det skydd som krävs enligt riktlinjen för informationssäkerhet och att det regleras i avtal.

Lekmannarevisorerna rekommenderar vd att rapportera informationssäkerhetsnivån till styrelsen i enlighet med riktlinjen för informationssäkerhet.

3.2 Iakttagelser

Med informationssäkerhet menas enligt Göteborgs Stads riktlinje för informationssäkerhet att se till att information hanteras på ett säkert sätt så att Göteborgs Stad, annan organisation eller enskild person inte utsätts för skada.

Information ska skyddas så att:

- endast behöriga personer kan ta del av den (konfidentialitet)

- den är korrekt och inte manipulerad eller förstörd (riktighet)
- den alltid finns tillgänglig när den behövs (tillgänglighet).

3.2.1 Följsamhet mot regelverket för informationssäkerhet

3.2.1.1 Förteckningen över informationssystemen behöver kompletteras

Samtliga system som bolaget använder för att hantera information ska finnas förtecknade. I förteckningen ska ändamålet med systemet beskrivas och ansvarsfördelning så som informationsägare, systemägare et cetera ska framgå. Tillämpliga regler, lagar och avtalsrättsliga åtaganden ska klart och tydligt definieras och dokumenteras för respektive informationssystem. Informationen i systemen ska klassificeras med hänsyn till vikten av konfidentialitet, riktighet och tillgänglighet. Den klassificeringen ska göras enligt en tregradig skala beroende på vilken skada som en individ, Göteborgs Stad eller annan kan utsättas för om informationen hanteras på ett felaktigt sätt.

Bolaget har en förteckning över sina it-system som är uppdaterad år 2022. Informationen är klassificerad med hänsyn till vikten av konfidentialitet, riktighet och tillgänglighet och utifrån de tre skyddsnivåerna. Av systemförteckningen framgår exempelvis ansvarsfördelning och ändamål med it-systemen Det framgår inte av förteckningen vilken typ av information som it-systemen innehåller. Hänvisning till regler, lagar och avtalsrättsliga åtaganden är inte klart och tydligt definierade och dokumenterade.

3.2.1.2 Säkerställ hanteringen av information som lagras hos extern leverantör

I riktlinjen för informationssäkerhet finns krav på hur informationen ska hanteras utifrån exempelvis:

- fysisk säkerhet,
- styrning av kommunikation, drift och åtkomst,
- anskaffning utveckling och underhåll,
- incidenthantering,
- och kontinuitetsplanering.

Det är informationsägaren som ansvarar för att det finns ett nödvändigt skydd och att säkerheten uppfyller ställda och rättsliga krav.

Merparten av ovanstående punkter hanteras i bolagets anvisning för informationssäkerhet och i interna rutiner. Det it-system som utgör vårt stickprov driftas av en extern leverantör och informationen lagras i en datorhall hos den externa leverantören. Vi har översiktligt granskat driftavtalet för Compis men inte verifierat hur bolaget övervakar om de krav som ställs i riktlinjen för informationssäkerhet följs av den avtalade leverantören.

3.2.2 Styrning och uppföljning av informationssäkerhetsarbetet

3.2.2.1 Organisation och ansvar för informationssäkerhet är dokumenterade

Säkerhetspolicy för Göteborgs Stad fastställer att informationssäkerhet är ett av fyra åtgärdsområden som ska inkluderas i säkerhetsarbetet. De övriga tre är personsäkerhet, fysisk säkerhet och krisberedskap. Samma policy fastställer att organisation, delegation, beslut, planer och åtgärder beträffande säkerhetsarbetet ska dokumenteras.

I Göteborgs och Co:s anvisning för informationssäkerhet beskrivs vilket ansvar bola-gets vd, chefer och medarbetare har för informationshantering. Det finns också beskrivningar av vilket ansvar som systemägare och systemadministratörer har i de it-system som bolaget använder. Utöver det beskrivs rutiner för incidenthantering och hur it-behörigheter ska initieras, kontrolleras och avslutas.

3.2.2.2 Säkerhetsnivån för informationssäkerhet har inte rapporterats till styrelsen

Enligt Säkerhetspolicy för Göteborgs Stad ska bolagsledningen minst årligen följa upp att säkerhetsnivån är acceptabel. Uppföljningen ska återrapporteras till styrelsen. Informationssäkerhet är, som vi nämnts i stycket ovan, ett av fyra åtgärdsområden som ska inkluderas i säkerhetsarbetet.

Rapporteringen av informationssäkerhetsarbetet ska innehålla en analys av vilka risker som finns och vilka åtgärder som har genomförts för att säkerställa att styrningen och uppföljningen av informationssäkerhetsarbetet är tillräcklig.

Vi har inte kunnat ta del av någon återrapportering till säkerhetssamordnare eller it-ansvarig av de åtgärder som olika ansvar, exempelvis chefer, systemägare och systemadministratörer, gör eller initierar.

Bolagsledningen har inte rapporterat säkerhetsnivån för informationssäkerhetsarbetet till styrelsen.

3.2.3 Arbete för att hantera dataskyddsförordningens krav pågår

Alla verksamheter som hanterar personuppgifter måste följa dataskyddsförordningen (GDPR). Det innebär bland annat att följa grundläggande principer, se till att behandlingen av personuppgifter har en rättslig grund och att informera de registrerade om hur deras personuppgifter hanteras.

Bolaget arbetar med att säkerställa en korrekt hantering av personuppgifter genom en pågående GDPR-genomgång med en utsedd projektledare. Det kommungemensamma it-stödet Draftit ska enligt bolaget användas för att registrera behandlingen av personuppgifter och registerförteckningen uppdateras för närvarande. Bolaget har tagit fram en anvisning för dataskydd, som ännu inte är formellt beslutad. Av anvisningen framgår hur registerförteckningen ska

uppdateras och hur bolaget på övergripande nivå ska hantera en begäran från en registrerad om att få sina uppgifter rättade eller raderade. Anvisningen är tänkt att kompletteras med en rutin för hantering av begäran om rättelse, registerutdrag och radering.

4 Uppföljning av tidigare granskning

Ibland resulterar våra granskningar i att revisorerna lämnar rekommendationer och/eller kritik. När detta händer följer vi oftast upp detta nästkommande år. Nedan redogör vi för den uppföljning som vi har genomfört i år.

4.1 Ägarstyrning mot kommunfullmäktiges mål

Lekmannarevisorerna granskade år 2021 bolagets styrning av dotterbolagen med utgångspunkt i de målsättningar som kommunfullmäktige pekat ut för bolagen inom turism, kultur och evenemangsklustret i budgetbeslutet. Granskningen resulterade i att lekmannarevisorerna riktade följande rekommendation till styrelsen:

Lekmannarevisorerna rekommenderar styrelsen att stärka ägarstyrningen av dotterbolagen med utgångspunkt i kommunfullmäktiges budget.

Bolaget bör verka för en samsyn inom TKE-klustret i hur de övergripande verksamhetsmålen tillsammans med de specifika målen ska ligga till grund för styrelsernas verksamhetsplaner och för att respektive styrelse beslutar om lämpliga indikatorer för att nå de specifika målen.

Vi har i år följt upp rekommendationen genom att följa bolagets arbete med att tydligare implementera kommunfullmäktiges mål och genom att granska dotterbolagens uppföljningsrapporter.

4.1.1 Bedömning

Det är vår bedömning att rekommendationen är omhändertagen.

4.1.2 Iakttagelser

En granskning av dotterbolagens uppföljningsrapporter visar att de rapporterar indikatorer för kommunfullmäktiges mål och att samsynen på kommunfullmäktiges mål för klustret har ökat. Bolaget beskriver i sitt yttrande att de under våren 2022, internt och i dialog med Stadshus AB, påbörjade ett arbete med att förbättra och utveckla ägarstyrningen inom klustret. Bolaget har genomfört möten med såväl de verkställande direktörerna som ekonomicheferna inom klustret. Inför dessa möten har bolaget tagit fram förslag på indikatorer till de specifika målen som finns för klustret för respektive dotterbolag. Indikatorerna är till sin karaktär både enskilda för vart och ett av bolagen och gemensamma för hela klustret.

4.2 Hantering av avtal och överenskommelser

Lekmannarevisorerna granskade år 2021 bolagets hantering av avtal och överenskommelser. Granskningen resulterade i att lekmannarevisorerna riktade följande rekommendation till vd:

Lekmannarevisorerna rekommenderar vd att stärka styrning, kontroll och uppföljning inom avtalshanteringen

Vi har i år följt upp rekommendationen genom intervju och dokumentstudier.

4.2.1 Bedömning

Det är vår bedömning att rekommendationen är omhändertagen.

4.2.2 Iakttagelser

Vår uppföljande granskning visar att bolaget har påbörjat ett arbete men att det ännu inte är helt implementerat. De åtgärder som bolaget vidtagit och planerar att vidta gör att vi bedömer att rekommendationen är omhändertagen. Vi kommer att följa arbetet fortsättningsvis.

5 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

6 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