Störningsjouren

Störningsjouren i Göteborg AB

Styrelsehandling nr 8
Datum: 2021-02-05
Diarienummer: SJ2021-0014

Handläggare: Sofia Gärdsfors

Telefon: 031-773 83 84
E-post: sofia.gardsfors@storningsjouren.goteborg.se

Stadsrevisionens granskningsredogörelse verksamhetsåret 2020

Informationsärende

Styrelsen Störningsjouren i Göteborg AB föreslås

Att Anteckna information om Stadsrevisionens granskning av verksamhetsåret 2020 för Störningsjouren i Göteborg AB

Ärendet

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.

Årets granskning av bolaget omfattar grundläggande granskning och granskning av implementering av dataskyddsförordningen. Den grundläggande granskningen visar inte på några väsentliga avvikelser.

Lekmannarevisorerna bedömer att bolaget har ett i stora delar strukturerat arbetssätt för att säkerställa en god efterlevnad av dataskyddsförordningen, men att det i vissa delar finns brister.

Inga rekommendationer lämnas.

Granskningsrapporten skickas till bolaget efter det att styrelsen beslutat att fastställa årsredovisningen. Uttalandet i granskningsrapporten grundar sig på granskningsredogörelsen.

Bedömning ur ekonomisk dimension

Bolaget inte har funnit några särskilda aspekter på frågan utifrån denna dimension.

Bedömning ur ekologisk dimension

Bolaget inte har funnit några särskilda aspekter på frågan utifrån denna dimension.

Bedömning ur social dimension

Bolaget inte har funnit några särskilda aspekter på frågan utifrån denna dimension.

Samverkan

Ärendet är inte föremål för samverkan.

Bilagor

1. Följebrev Lekmannarevisorer - Granskning av verksamhetsåret 2020
2. Granskningsredogörelse Störningsjouren i Göteborg AB -Granskning av verksamhetsåret 2020, 2021-01-19

Göteborgs Stad

Granskning av verksamhetsåret 2020

Vi, lekmannarevisorer i Störningsjouren i Göteborg AB, har avslutat granskningen av bolaget avseende verksamhetsåret 2020. 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 2021

Gun Cederborg
Lekmannarevisor utsedd
av kommunfullmäktige

Stefan Dahlén
Lekmannarevisor utsedd
av kommunfullmäktige

Göteborgs Stad

Störningsjouren i Göteborg AB

– granskning av verksamhetsåret 2020

2021-01-19

Januari 2021

Störningsjouren i Göteborg AB – granskning av verksamhetsåret 2020

Diarienummer: 0145/20

Lekmannarevisorer: Gun Cederborg, Stefan Dahlén

Yrkesrevisor: Jesper Wigh

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.

Årets granskning av bolaget omfattar:

- grundläggande granskning
- granskning av implementering av dataskyddsförordningen

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 samt granskning av införandet av Dataskyddsförordningen.

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 och direktiv för Göteborgs Stads bolag
- 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.

2.1 Implementering av Dataskyddsförordningen

2.1.1 Utgångspunkter i granskningen

Lekmannarevisorerna har granskat bolagets implementering av Dataskyddsförordningen.

EU:s nya dataskyddsförordning (DSF), även kallad GDPR – General Data Protection Regulation, innehåller regler om hur personuppgifter får behandlas. Förordningen började gälla den 25 maj 2018 och ersatte då personuppgiftslagen (PuL). DSF gäller för alla organisationer och branscher som sparar eller på något sätt hanterar personlig och känslig information om sina anställda, leverantörer eller sina kunder.

Förordningen innebär bland annat hårdare krav på hantering av personuppgifter. Vidare ställer förordningen krav på rutiner och processer för säker hantering av register. Detta medför även krav på ansvarig ledningsnivå att säkerställa efterlevnad av förordningen inom organisationen. Vid granskning av verksamheters efterlevnad av lagstiftningen av tillsynsmyndigheten, Datainspektionen, ska den granskade verksamheten kunna bevisa att de följer lagstiftningens krav på bland annat dokumentation.

Göteborgs stad initierade inför införandet av DSF ett införandeprojekt som stöd för verksamheternas arbete med anpassning till den nya lagstiftningen. Projektet resulterade bland annat i ett dokument ”Checklista avseende följsamhet mot EU:s dataskyddsförordning (DSF)” innehållandes ett antal åtgärder och aktiviteter bolag och verksamheter skulle vidta för att ha en god följsamhet mot den nya lagstiftningen. I granskningen har vår utgångspunkt varit att checklistans konkretisering av dataskyddsförordningens artiklar, samt ett antal artiklar från förordningen, täcker de mest väsentliga delarna vid implementering av dataskyddsförordningen.

Syftet med granskningen är att bedöma om bolaget har vidtagit tillräckliga åtgärder i syfte att säkerställa följsamhet mot dataskyddsförordningen. Granskningen har genomförts genom analys av relevanta dokument och intervjuer med företrädare för verksamheten.

Iakttagelser i granskningen har bedömts mot krav och bestämmelser i nedan angivna lagar, råd och rutiner, direktiv och anvisningar:

- Dataskyddsförordningen (Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016)
    - art. 24(1)
    - art. 28.3
    - art. 34
    - art. 37

- Göteborgs Stads interna styrande dokument (checklistor och mallar) för införandet av DSF
    - Checklista avseende följsamhet mot EU:s dataskyddsförordning (DSF)
    - Stöd för personuppgiftshantering
    - Mall handlingsplan förvaltning/bolag – 2017-02-08)

2.1.2 Iakttagelser

2.1.2.1 Intern organisation

I dataskyddsförordningens artikel 24(1) framgår att den personuppgiftsansvarige[1], med beaktande av bland annat behandlingens art, omfattning, sammanhang och ändamål ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa sin följsamhet gentemot dataskyddsförordningen samt att dessa åtgärder ska ses över och uppdateras vid behov.

Inför införandet instiftade Framtiden AB, koncernmoder i Framtidenkoncernen, en arbetsgrupp, kallad DSF-rådet, för att hantera frågor på ett koncerngemensamt sätt. I rådet ingick representanter från respektive bolag i form av dataskyddskontakter (DSK) samt en dataskyddskoordinator. Tjänsten som dataskyddskoordinator har sedan en tid varit vakant. Vid intervjuer med Störningsjourens DSK framkommer en önskan om att tjänsten återbesätts.

Störningsjouren i Göteborg AB (Störningsjouren) har fattat beslut om en övergripande struktur för bolagets dataskyddsarbete. Strukturen består av fyra nivåer som i varierande grad deltar i det strategiska och praktiska arbetet. Organisationen utgörs av DSK, vd och styrelse samt den ovan nämnda koncerngemensamma funktionen dataskyddskoordinator men som sedan en tid är vakant.

Enligt Dataskyddsförordningen, artikel 37, ska en personuppgiftsansvarig utse ett dataskyddsombud (DSO) om den personuppgiftsansvarige är en kommunal myndighet eller om den personuppgiftsansvarige antingen har som sin kärnverksamhet att regelbundet övervakade registrerade i stor omfattning eller består av behandling av vissa kategorier av personuppgifter. Kommunstyrelsen har beslutat att DSO tillhandahålls alla nämnder och bolag via Intraservice. Det ankommer enligt beslutet på respektive verksamhet att meddela Datainspektionen. Störningsjouren har enligt de intervjuade meddelat Datainspektionen vem som utsetts till DSO.

[1] Personuppgiftsansvarig är den organisation (till exempel aktiebolag, stiftelse, förening eller myndighet) som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till.

2.1.2.2 Införandet enligt projektet

I dokumentet ”Checklista avseende följsamhet mot EU:s dataskyddsförordning (DSF)”[2] listas ett antal åtgärder som verksamheterna uppmanades genomföra i syfte att säkerställa en följsamhet mot DSF. Bolaget antog inför arbetet en projektplan som upprättats i enlighet med implementeringsprojektets mall. Projektplanen innehåller uppgifter om vem som är projektägare, projektledare samt styrgrupp. Projektplanen innehåller även en tidsram för kritiska moment och en aktivitetsplan för åtgärder som skulle vidtas innan lagen trädde i kraft den 25 maj 2018.

Av projektplanen framgår att bolaget tidsatt samtliga moment som nämns i ”Checklista avseende följsamhet…”. Inför ikraftträdandet av DSF i maj 2018 upprättades en lägesbild av var bolaget stod i sitt införande. Lägesbilden visar att för fem av de nio angivna momenten ansåg bolaget att arbetet var klart, för tre moment angavs att arbetet pågår och i ett fall – styrelse har fattat beslut om hur ofta DSO kommer att närvara vid styrelsemöten – hade arbetet inte påbörjats.

Enligt ”Checklista avseende följsamhet…” ska verksamheterna genomföra informationskartläggning och informations- och säkerhetsklassningar i enlighet med instruktionerna. Vi har tagit del av genomförd kartläggning och informations- och säkerhetsklassningar av information som rör bolagets kärnprocess ”Utföra utredning och hantering av oriktiga hyresförhållanden”. Materialet är inlagt i Draftit[3] där samtliga behandlingar av personuppgifter ska registreras. Enligt bolagets DSK finns vid granskningens genomförande 92 registreringar av personuppgifter inlagda i Draftit. Arbetet med att hålla registret i systemstödet uppdaterat är ett pågående arbete.

Bolaget upprättade den 24 oktober 2017 en ”Riskanalys avseende informationssäkerhet” som redogör för det arbete som utförts rörande kartläggning av informationssäkerheten och personuppgiftshanteringen i bolaget. Riskanalysen innehåller identifierade risker med bedömda sannolikheter och konsekvenser samt framtagna åtgärdsförslag för respektive riskområde. I riskanalysen anges att informationsägaren, årligen och vid större förändringar i verksamheten eller informationshanteringen, behöver utvärdera riskanalysen för att på så sätt säkerställa att riskerna är hanterade samt om det finns ytterligare behov av riskanalys. Vår granskning visar att ”Riskanalys avseende informationssäkerhet” inte har uppdaterats efter upprättandet.

Enligt dataskyddsförordningen art. 34 ska en personuppgiftsincident[4] anmälas till tillsynsmyndigheten utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att den personuppgiftsansvarig fått kunskap om incidenten.

[2] 2017-06-06
[3] Utgör stadens system för hantering av personuppgiftshanteringar
[4] Enligt Datainspektionen utgörs en personuppgiftsincident av en säkerhetsincident som kan innebära risker för människors friheter och rättigheter.

Om det är osannolikt att incidenten innebär risker för de registrerades fri- och rättigheter behöver incidenten inte anmälas till Datainspektionen. Även om personuppgiftsincidenten inte är anmälningspliktig är den personuppgiftsansvariga skyldig att registrera och dokumentera vad som har hänt. De beslut som har tagits i samband med hanteringen av incidenten ska även motiveras. Om personuppgiftsincidenten sannolikt lett till hög risk för de registrerades rättigheter ska den registrerade utan onödigt dröjsmål informeras om incidenten.

För att säkerställa att verksamheten har en god följsamhet mot regelverket vid eventuella personuppgiftsincidenter bör, enligt Datainspektionen, en rutin finnas på plats. Rutinen bör innehålla uppgifter om till vilken tillsynsmyndighet som incidenten ska rapporteras, vilken information som ska lämnas, hur de registrerade ska informeras om incidenten samt hur personuppgiftsincidenter ska dokumenteras. Granskningen visar att Störningsjouren har en rutin för rapportering av personuppgiftsincidenter. På bolagets intranät finns också instruktioner samt en mall för rapportering av incidenten. Bolagets dataskyddskontakt beslutar efter samråd med DSO om en anmälan ska göras till Datainspektionen.

När en personuppgiftsansvarig låter någon annan behandla personuppgifter på dennes uppdrag ska ett *personuppgiftsbiträdesavtal* (PuB-avtal) upprättas. Artikel 28.3 i dataskyddsförordningen anger vilken information som ska framgå om behandlingen och de minimikrav som ställs på vad avtalet ska innehålla. Störningsjouren har PuB-avtal, med dels de kunder där Störningsjouren utgör biträde, dels med de leverantörer till Störningsjouren som utgör biträden till Störningsjouren. PuB-avtal finns på plats med samtliga systerbolag inom koncernen samt med de större privata aktörerna. Störningsjouren anger att de skickat ut förslag på PuB-avtal till sina mindre kunder och att de flesta är återsända.

I de fall där Störningsjouren är personuppgiftsansvarig och därmed måste upprätta avtal med sina underleverantörer finns, enligt bolaget, PuB-avtal på plats där det bedöms nödvändigt. Bolaget har både egna avtal med leverantörer och i något fall hanteras personuppgifter i ett ”stadengemensamt” system. I dessa fall ska inte ett PuB-avtal upprättas.

2.1.2.3 Framåtsyftande åtgärder

Den sista åtgärden som listas i ”Checklista avseende följsamhet…” handlar om att kvalitetssäkra ett kontinuerligt uppfyllande av DSF. Enligt implementeringsprojektets anvisningar ska verksamheterna ”implementera ett metodiskt arbetssätt som medför kontroll av att verksamheternas pu-behandling på ett fortvarigt och kontinuerligt sätt säkerställer ett uppfyllande av DSF”. För att uppnå detta ska verksamheterna enligt skrivelsen implementera metodik för informationshantering och säkerställa att arbetssättet används vid alla större förändringar i verksamheten eller vid införande av nya verktyg et cetera.

Verksamheterna ska även säkerställa att DSO involveras så tidigt som möjligt vid förändringar.

Granskningen visar att bolaget vid införandet av lagstiftningen upprättat en åtgärdsplan för att komma tillrätta med de risker som identifierats den tidigare nämnda riskanalysen avseende informationssäkerhet. Vi har inte tagit del av någon kontinuerlig uppdatering av åtgärdsplanen där risker anses omhändertagna vartefter bolaget genomför åtgärder.

Vid intervju redogör DSK för en rad åtgärder som bolaget planerar att vidta för att säkerställa en fortsatt efterlevnad av lagstiftningen. Utifrån DSO:s rapportering[5] till styrelsen har en åtgärdslista tagits fram som bland annat innehåller att ta fram rutiner för behörighetsstyrning, rutiner för processförändringar och så vidare.

Bolaget har även med risken för bristande efterlevnad av GDPR i sin samlade riskbild för år 2020. Angivna åtgärder för att komma tillrätta med den identifierade risken är *Utbildning* och *Underleverantörers efterlevnad*. Bolaget anger att man har introduktioner för nyanställda och årlig utbildning för samtlig personal. Störningsjourens dataskyddskontakt uppger vid intervju att medarbetarnas hantering av personuppgifter är bolagets största riskfaktor att hantera.

2.1.3 Bedömning

Lekmannarevisorerna bedömer att bolaget har ett i stora delar strukturerat arbetssätt för att säkerställa en god efterlevnad av dataskyddsförordningen, men att det i vissa delar finns brister.

Lekmannarevisorernas bedömning är att bolaget följt stadens checklista, och därmed viktiga delar av de krav som ställs utifrån förordningen, inför implementeringen av dataskyddsförordningen. Bolaget har genomfört informationsklassning och informationskartläggning samt upprättat en handlings- och åtgärdsplan för det kommande arbetet efter lagens ikraftträdande i enlighet med projektets anvisningar. Bolaget har också tagit fram en ny åtgärdsplan efter DSOs rapportering till styrelsen.

Vår bedömning är att bolaget har upprättat en organisation med tydliga roller och ändamålsenlig struktur. Lekmannarevisorerna anser däremot att arbetet med att dokumentera både genomförda åtgärder och identifierade åtgärder för att öka efterlevnaden av dataskyddsförordningen kan stärkas. För att ha en långsiktigt god efterlevnad av lagstiftningen är det viktigt att det planerade arbetet förtecknas i en långsiktig handlingsplan som hålls uppdaterad. Verksamheten bör också se till att det finns rutiner som säkerställer att riskhantering, informationskartläggning och informations- och säkerhetsklassning genomförs och dokumenteras vid förändringar i verksamheten.

[5] Styrelsehandling 9, Information från Dataskyddsombud 2020-05-07

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