



Beslutsunderlag 11

Styrelsen 2021-09-23

Diarienummer 67/21

Handläggare: Charlotte Lundell, ekonomichef

Telefon: 031-708 70 19

E-post: charlotte.lundell@stadsteatern.goteborg.se

Kontroll av dataskyddsarbete 2021, delårsrapport

Förslag till beslut

I styrelsen för Göteborgs Stadsteater AB:

Styrelsen antecknar informationen.

Sammanfattning

I Göteborgs Stad är varje enskild nämnd eller bolagsstyrelse personuppgiftsansvarig och ansvarar därigenom för att dess personuppgiftsbehandlingar utförs i enlighet med dataskyddsförordningens bestämmelser. Utifrån dataskyddsförordningen ska dataskyddsombudet övervaka bolagets efterlevnad av förordningen. Denna granskning är en del av detta arbete.

Utifrån kontrollplanen ska dataskyddsombudet i varje enskilt bolag och förvaltning utföra två kontroller avseende dataskydd mellan mars och maj månad varje år. Detta år har dataskyddsombudet valt att utföra kontroller avseende bolagets personuppgiftsregister (ersatt utbildningskontrollen) och IT-system och digitala verktyg.

Dataskyddsombudet anser att bolaget på det stora hela har god kontroll och ordning gällande dataskyddet på de kontrollerade IT-systemen och personuppgiftsbehandlingarna. Det förbättringsområde som dataskyddsombudet har identifierat vid denna kontroll gäller uppdateringen av personuppgiftsregistret (Draftit). Även informationsklassning och riskanalyser av IT-system/behandlingar kan tydliggöras utifrån informationen som hanteras.

Bedömning ur ekonomisk dimension

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

Bedömning ur ekologisk dimension

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

Bedömning ur social dimension

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

Bilagor

1. Göteborgs Stadsteater AB delårsrapport kontroller dataskydd 2021

2021-09-16

Björn Sandmark

VD, Göteborgs Stadsteater AB



Göteborgs
Stad

Dataskyddsombudets delårsrapport 2021

**Fördjupade kontroller enligt kontrollplan
dataskydd för Göteborgs Stadsteater AB**

2021-06-08

Innehåll

1	Inledning	3
1.1	Bakgrund	3
1.2	Kontroller dataskydd	3
2	Kontrollen.....	3
2.1	Granskade dokument	3
2.2	Kontrollpunkt Personuppgiftsregister	4
2.2.1	Bedömning	4
2.2.2	Slutsats	4
2.3	Kontrollpunkt IT-system och digitala verktyg	4
2.3.1	Bedömning	5
2.3.2	Slutsats	5
3	Sammanfattning.....	5

1 Inledning

1.1 Bakgrund

Dataskyddsförordningen ställer höga krav på organisationers behandling av enskildas personuppgifter. Utöver att insamlingen av personuppgifterna ska vara tillåten, måste den personuppgiftsansvarige dessutom hantera dessa uppgifter på ett korrekt sätt, med respekt för den enskildes integritet och med beaktande av lämpliga säkerhetsåtgärder.

I Göteborgs Stad är varje enskild nämnd eller bolagsstyrelse personuppgiftsansvarig och ansvarar därigenom för att dess personuppgiftsbehandlingar utförs i enlighet med dataskyddsförordningens bestämmelser.

Utifrån dataskyddsförordningen ska dataskyddsombudet övervaka bolagets efterlevnad av förordningen. Denna granskning är en del av detta arbete.

1.2 Kontroller dataskydd

I början av år 2021 så beslutades att dataskyddsombuden ska arbeta efter en gemensam kontrollplan för att skapa förutsägbarhet för stadens verksamheter. Utifrån kontrollplanen så ska dataskyddsombudet i varje enskilt bolag och förvaltning utföra två kontroller avseende dataskydd mellan mars och maj månad varje år. Detta år har dataskyddsombudet valt att utföra kontroller avseende bolagets personuppgiftsregister (ersatt utbildningskontrollen) och IT-system och digitala verktyg.

Kontrollerna har utförts genom dokumentgranskning och intervjuer med bolagets dataskyddskontakter och marknadsförare.

Utifrån intervjuer och dokumentgranskning skapade dataskyddsombudet ett första utkast till rapport utifrån kontrollpunkterna som dataskyddskontakterna fått lämna synpunkter på. Eventuella synpunkter från dataskyddskontakterna har beaktats i denna rapport.

I de fall där dataskyddsombudet lämnar synpunkter och/eller andra kommentarer i rapporten görs detta endast på basis av vad som framkommit i de granskade dokumenten och vad som framkommit i intervjuer med ovan nämnda.

2 Kontrollen

2.1 Granskade dokument

Informationskartläggning reviderad2.xlsx

2.2 Kontrollpunkt Personuppgiftsregister

Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även verksamhetens arbete med, och rutin för, att säkerställa ett uppdaterat och heltäckande personuppgiftsregister innefattas.

2.2.1 Bedömning

I nuläget har bolaget ingen rutin/arbetsbeskrivning för hur personuppgiftsregistret (Draftit) ska hållas uppdaterat. Alla behandlingar är inte överförda till Draftit utan finns i ett separat excelark³.

2.2.2 Slutsats

Dataskyddsombudet har gjort stickprovskontroller utifrån de obligatoriska uppgifter som ska finnas i personuppgiftsregistret enligt artikel 30 i dataskyddsförordningen. I samtliga stickprov så har de obligatoriska uppgifterna funnits med.

Utifrån slutsatsen i kontrollpunkt IT-system och digitala verktyg rekommenderar dataskyddsombudet bolaget att skapa en rutin/arbetsbeskrivning som säkrar att personuppgiftsregistret i Draftit är uppdaterat och hålls uppdaterat.

2.3 Kontrollpunkt IT-system och digitala verktyg

Kontrollpunkten avser verksamhetens rutiner för att säkerställa att verksamhetens personuppgiftshantering inom ramen för IT-system och digitala verktyg är förenlig med dataskyddsförordningen. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår även.

Dataskyddsombudet har valt att vid denna kontroll titta på hur bolaget hanterar kunduppgifter vid marknadsföring i bolagets IT-system APSIS.

¹

<https://www.anpdm.com/public/Editor4PreviewPublic.anp/Show/4145594B734347514270454259?ns=484B5E4B7740455F43764546514A7744465B47>

² <https://stadsteatern.goteborg.se/villkor/#personuppgiftspolicy>

³ Informationskartläggning reviderad2.xlsx

2.3.1 Bedömning

Bolaget hanterar kunduppgifter för marknadsföring framförallt IT-systemet APSIS. APSIS International AB sköter driften av IT-systemet.

Personuppgiftsbiträdesavtal finns tecknat mellan parterna.

I APSIS så hanteras bland annat kunduppgifter, nyhetsbrev, inbjudan till förhandsvisning och merförsäljning som exempelvis middag i samband med föreställning. Bolagets kunder är till största delen privatpersoner och registret innehåller i dagsläget cirka 25 000 kontaktuppgifter.

Information till kunderna om behandlingen i samtyckesbrev, nyhetsbrevet och på bolagets hemsida.

Bolaget har informationsklassat APSIS på aggregerad nivå och även en åtgärdsplan gällande risker finns dokumenterat⁴. Inga känsliga personuppgifter får hanteras i APSIS.

Dataskyddsombudet har gjort en kontroll i bolagets personuppgiftsbehandlingsregister (Draftit) och ovan angivna behandlingarna i APSIS är inte upptagna. Däremot är dessa behandlingar upptagna i dokumentet ”Informationskartläggning reviderad2.xlsx”.

2.3.2 Slutsats

Dataskyddsombudet anser att bolaget på det stora hela har mycket god kontroll och ordning gällande dataskyddet avseende det kontrollerade IT-systemet och tillhörande personuppgiftsbehandlingar.

De förbättringar som bolaget kan vidta är att dokumentera personuppgiftsbehandlingarna som sker i APSIS i personuppgiftsregistret och att i informationsklassningen visa hur bolaget har kommit fram till de aggregerade nivåerna avseende konfidentialitet, riktighet och tillgänglighet. Även riskanalyser kan med fördel dokumenteras utifrån varje behandling/IT-system.

3 Sammanfattning

Dataskyddsombudet anser att bolaget på det stora hela har god kontroll och ordning gällande dataskyddet på de kontrollerade IT-systemet och personuppgiftsbehandlingarna.

Det förbättringsområde som dataskyddsombudet har identifierat vid denna kontroll gäller uppdateringen av personuppgiftsregistret (Draftit). Även informationsklassning och riskanalyser av IT-system/behandlingar kan tydliggöras utifrån informationen som hanteras.

⁴ Informationskartläggning reviderad2.xlsx

Dataskyddsbudet vill avsluta med att konstatera att dataskyddsbudet har bra förutsättningar att verka i bolaget och att dataskyddsbudet får ett mycket bra stöd av både dataskyddskontakter och övriga medarbetare som dataskyddsbudet har varit i kontakt med.