Ärende 7, information
Mötesdatum 2020-06-12

Dataskyddsombudets granskningsredogörelse

Bifogat återfinns Dataskyddsombudets granskningsredogörelse för Göteborgs Stadsteater AB.

Granskningsredogörelsen presenteras på styrelsemötet av teaterns dataskyddsombud Martin Brunhage, Intraservice.

Göteborg 2020-06-04
Björn Sandmark

Göteborgs Stadsteater AB
Box 5094 SE-402 22 Göteborg, Sverige
+46 (0)31 708 70 00
www.stadsteatern.goteborg.se

Göteborgs Stadsteater

Göteborgs Stad

Behandling av anställdas personuppgifter

Granskningsrapport för Göteborgs Stadsteater AB

2020-05-25

Innehåll

1 Inledning 3

1.1 Bakgrund 3

1.2 Granskningsområde 3

1.3 Tillvägagångssätt 3

2 Granskningen 4

2.1 Granskade dokument 4

2.2 Område 1 Personuppgiftsbiträdesavtal och personuppgiftsbiträdeskontroll 4

2.2.1 Bedömning 4

2.2.2 Slutsats/Rekommendation 5

2.3 Område 2 Dokumenterade medarbetarsamtal 5

2.3.1 Bedömning/Slutsats 5

2.4 Område 3 Informationsplikt anställda 6

2.4.1 Bedömning/Slutsats 6

2.5 Område 4 Är personuppgiftsbehandlingarna upptagna i personuppgiftsbehandlingsregistret 6

2.5.1 Bedömning/Slutsats 6

2.6 Område 5 Sker kontrollåtgärder gentemot anställda och är de i linje med dataskyddsförordningen 7

2.6.1 Bedömning/Slutsats 7

3 Sammanfattning 7

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 Granskningsområde

En utgångspunkt i dataskyddsförordningen är att personuppgiftsansvarig och dataskyddsombud ska arbeta riskbaserat. Dataskyddsombudet har vid denna granskning valt att titta på hur bolaget hanterar de anställdas personuppgifter och om behandlingen av dessa uppgifter är i linje med dataskyddsförordningens krav. Området är valt utifrån dataskyddsombudets bedömning att behandlingen av de anställdas personuppgifter ligger högst i risk utifrån de registrerades fri- och rättigheter av de personuppgiftsbehandlingar som bolaget utför.

Granskningen är uppdelad i fem delområden som tar sikte på bland annat om formella krav enligt dataskyddsförordningen är uppfyllda.

1.3 Tillvägagångssätt

Granskningen har utförts genom intervjuer och dokumentgranskning. Intervjuer har skett med bolagets dataskyddskontakter. Granskningens delområden täcker inte all den behandling av anställdas personuppgifter som utförs i bolaget utan ska ses som stickprov. Utifrån granskningsunderlaget skapade dataskyddsombudet ett första utkast till denna granskningsrapport 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 granskningsrapporten görs detta endast på basis av vad som framkommit i de granskade dokumenten och vad som framkommit i intervjuer med ovan nämnda.

2 Granskningen

2.1 Granskade dokument

GDPR/DSF – hantering av personuppgifter inom Göteborgs Stadsteater AB

Visma AGDA PS (SaaS och OnPrem) Personuppgiftsbiträdesavtal

2.2 Område 1 Personuppgiftsbiträdesavtal och personuppgiftsbiträdeskontroll

Vid hantering av personuppgifter som sker hos annan (personuppgiftsbiträde) än personuppgiftsansvarig krävs enligt dataskyddsförordningen[1] att bolaget reglerar ansvaret mellan parterna och att bolaget ger instruktioner till biträdet hur uppgifterna får behandlas. Det finns inga krav i dataskyddsförordningen som styr hur detta ska regleras mellan parterna men det har utvecklats en praxis på området att man gör detta via ett separat avtal som benämns personuppgiftsbiträdesavtal (PUB-avtal). Personuppgiftsansvarig har även ansvar att kontrollera att personuppgiftsbiträdet hanterar personuppgifterna på avtalat sätt. Detta krav kan härledas till principen ansvarsskyldighet i dataskyddsförordningen[2] Principen ansvarsskyldighet innebär att personuppgiftsansvarig ska kunna visa att och hur bolaget lever upp till dataskyddsförordningen. Kontrollen av personuppgiftsbiträdet kan ske på många olika sätt. Exempel på kontroller är revison i biträdets lokaler och/eller ta del av biträdes egenkontroller och/eller ta del av biträdets granskningsrapporter utifrån eventuell certifiering[3]. Bolagets personuppgiftsbiträdeskontroller ska alltid dokumenteras. I denna granskning har dataskyddsombudet valt att granska om bolaget uppfyller dessa krav i personuppgiftsbehandlingen "Hantera anställning".

2.2.1 Bedömning

Merparten av de anställdas personuppgifter hanteras i ett verksamhetssystem som kallas Agda och levereras som en tjänst från företaget Visma Enterprise AB. Mellan bolaget och personuppgiftsbiträdet Visma finns ett upprättat personuppgiftsbiträdesavtal (Visma AGDA PS (SaaS och OnPrem) Personuppgiftsbiträdesavtal).

Personuppgiftsbiträdesavtalet mellan bolaget och personuppgiftsbiträdet reglerar ansvar och skyldigheter mellan bolaget och Visma på en övergripande nivå. I avtalet finns få direkta instruktioner för hur informationen ska behandlas hos personsuppgiftsbiträdet. I personuppgiftsbiträdesavtalet finns hänvisning till tjänsteavtal.

[1] Artikel 28.3 dataskyddsförordningen
[2] Artikel 5 dataskyddsförordningen
[3] Exempelvis ledningssystem för informationssäkerhet ISO 27001

Bolaget har inte utfört någon kontroll/revision utifrån avtalade krav av den personuppgiftsbehandling som Visma utför för bolagets räkning.

2.2.2 Slutsats/Rekommendation

För att uppfylla ansvarsskyldigheten enligt dataskyddsordningen måste bolaget kunna visa att och hur man lever upp till dataskyddsförordningen krav. Att utföra leverantörsuppföljning/kontroll är en del av att uppfylla ansvarsskyldigheten. Dataskyddsombudet rekommenderar att bolaget utför kontroller av personuppgiftsbiträden med en frekvens och omfattning som bestäms utifrån de risker behandlingarna medför för de registrerades fri- och rättigheter. Dataskyddsombudet rekommenderar även bolaget att kontrollera så att tjänsteavtalet mellan bolaget och Visma tydliggör de krav (behandlingsinstruktioner) som bolaget ställer på personsuppgiftsbiträdet utifrån informationsklassning och riskanalyser.

2.3 Område 2 Dokumenterade medarbetarsamtal

Utifrån riskerna för de anställdas fri- och rättigheter har dataskyddsombudet valt att granska hantering av de dokumenterade medarbetarsamtal som utförs i bolaget. Medarbetarsamtalen kan ha olika benämning och syften som varierar mellan olika verksamheter. Utifrån samtalsmallens frågor kan det finnas risk för att känsliga personuppgifter hanteras. Då det ofta förekommer öppna frågeställningar i medarbetarsamtalen finns det en risk för att information om hälsostatus eller andra känsliga/skyddsvärda personuppgifter av misstag kan komma att dokumenteras i samtalsmallarna. Exempel på sådana öppna frågeställningar är ”Hur mår du?” och ”Hur är relationen till dina kollegor?”. Om bolaget har behov att dokumentera känsliga personuppgifter i medarbetarsamtalen krävs att bolaget har en rättslig grund för att få hantera dessa uppgifter och att lämpliga tekniska och organisatoriska skyddsåtgärder har vidtagits.

2.3.1 Bedömning/Slutsats

Medarbetarsamtalen dokumenteras på papper och förvaras hos ansvarig chef. I de intervjuer som har ägt rum så finns det inget som antyder att de fysiska dokumenten organiseras på ett sådant sätt att behandlingen träffas av dataskyddsförordningens krav. För att träffas av dataskyddsförordningens krav behöver fysiska dokument indexeras på ett sådant sätt att indexeringen möjliggör två eller fler sökingångar till personuppgifter i dokumenten. Om bolaget i framtiden har som avsikt att digitalisera medarbetarsamtalen behöver bolaget tillse att behandlingen följer dataskyddsförordningens krav.

2.4 Område 3 Informationsplikt anställda

Dataskyddsförordningen ställer krav på att personuppgiftsansvarig ska informera om de behandlingar som berör den registrerade. Informationen ska bland annat vara lättåtkomlig, lättbegriplig[4] och upplysa den registrerade vart den kan vända sig vid frågor gällande behandlingen eller om den registrerade vill klaga på behandlingen.

2.4.1 Bedömning/Slutsats

Dataskyddsombudet har granskat informationen i dokumentet "GDPR/DSF – hantering av personuppgifter inom Göteborgs Stadsteater AB" som är en bilaga till anställningskontraktet. Dokumentet lämnas som bilaga till anställningsavtalet och finns tillgängligt på bolagets intranät. Dokumentet tar upp de huvudkategorier av personuppgifter som hanteras och vart den anställde kan vända sig vid frågor om behandlingen. Dataskyddsombudets uppfattning är att bolaget ger en bra allmän information gällande den registrerades rättigheter i enlighet med dataskyddsförordningen. I bolagets information framgår inte vilka specifika behandlingar den anställde kan förekomma i. Eftersom syftet med informationen till den registrerade är att bland annat möjliggöra för den registrerade att invända mot en behandling så rekommenderar dataskyddsombudet bolaget att tydliggöra de enskilda behandlingarna där den anställde kan förekomma och komplettera med uppgifter som föreskrivs i dataskyddsförordningen[5] som exempelvis rättslig grund för behandlingen och lagringstid för personuppgifterna. Uppgifterna kan antingen ges direkt i dokumentet eller ske genom hänvisning i dokumentet till var den anställde kan hitta ytterligare information om de specifika behandlingarna.

2.5 Område 4 Är personuppgiftsbehandlingarna upptagna i personuppgiftsbehandlingsregistret

Den personuppgiftsansvarige är skyldig att föra register (personbehandlingsregister) över de behandlingar bolaget utför[6].

2.5.1 Bedömning/Slutsats

Dataskyddsombudet har kontrollerat om behandlingen "Hantera Anställning" är upptagen i personuppgiftsbehandlingsregistret. Behandlingen finns upptagen i bolagets personuppgiftsbehandlingsregister under namnet personakt. Det saknas uppgift om att behandlingen sker med hjälp av ett personuppgiftsbiträde i

[4] Skäl 39 dataskyddsförordningen
[5] Artikel 13 dataskyddsförordningen
[6] Artikel 10 dataskyddsförordningen

registret. Dataskyddsombudet rekommenderar bolaget att dokumentera eventuella personuppgiftsbiträden i registret under rubriken informationsbärare.

2.6 Område 5 Sker kontrollåtgärder gentemot anställda och är de i linje med dataskyddsförordningen

Om arbetsgivaren vill göra systematiska kontroller av de anställda krävs rättslig grund, att kontrollen är proportionerligt utifrån syftet, samt att de anställda är informerad innan kontrollen sker. Den anställde har dock rätt till skydd för sin kommunikation och sitt privatliv. Detta gäller även om den anställde använder sig av bolagets egendom i form av arbetsdator/mobiltelefon för privat kommunikation eller som lagring av privata filer[7]. Det är bara vid allvarlig misstanke om illojalt eller brottsligt beteende som det kan vara tillåtet för arbetsgivaren att ta del av själva innehållet i de anställdas privata filer eller e-postmeddelanden.

2.6.1 Bedömning/Slutsats

Dataskyddsombudet har utifrån genomförd intervju inte hittat något som antyder att bolaget utför kontrollåtgärder gentemot de anställda förutom vid eventuell misstanke om allvarlig illojalitet eller brottslig verksamhet.

3 Sammanfattning

För att uppfylla ansvarsskyldigheten enligt dataskyddsordningen måste bolaget kunna visa att och hur man lever upp till dataskyddsförordningen krav. Att utföra leverantörsuppföljning/kontroll är en del av att uppfylla ansvarsskyldigheten. Dataskyddsombudet rekommenderar att bolaget utför kontroller av personuppgiftsbiträden och att detta sker med en frekvens och omfattning som bestäms utifrån de risker behandlingarna medför för de registrerades fri- och rättigheter. Dataskyddsombudet rekommenderar även bolaget att lägga in information om personuppgiftsbiträden i personuppgiftsbehandlingsregistret.

Dataskyddsombudets bedömning är att bolaget behöver utöka informationen till den anställde med exempelvis vilka behandlingar som utförs, lagringstid och rättslig grund utifrån den informationsplikt som föreskrivs i dataskyddsförordningen.

Dataskyddsombudet vill avsluta med att konstatera att dataskyddsombudet har bra förutsättningar att verka i bolaget och att dataskyddsombudet får ett mycket

[7]Artikel 8 Europakonventionen för mänskliga rättigheter -"...var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens" Se även rättsfall (61496/08) BĂRBULESCU v. ROMANIA (https://hudoc.echr.coe.int/eng#{"itemid":["001-177082"]}

bra stöd av både dataskyddskontakter och övriga medarbetare som dataskyddsombudet har varit i kontakt med.