Göteborgs Stad

Dataskyddsombudets delårsrapport 2021

Fördjupade kontroller enligt kontrollplan dataskydd för Got Event AB

2021-05-27

Innehåll

1 Inledning 3
1.1 Bakgrund 3
1.2 Kontroller dataskydd 3
1.3 Tillvägagångssätt 3
2 Kontrollen 4
2.1 Granskade dokument 4
2.2 Kontrollpunkt IT-projekt och upphandling 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 6

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 IT-projekt och upphandling och IT-system och digitala verktyg.

1.3 Tillvägagångssätt

Kontrollerna har utförts genom dokumentgranskning och intervjuer med bolagets dataskyddskontakt, säljchef och avtalscontroller.

Utifrån intervjuer och dokumentgranskning skapade dataskyddsombudet ett första utkast till rapport utifrån kontrollpunkterna som dataskyddskontakten 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

Got Event AB anvisning för inköp/upphandling, revision 2020-02-13.

Direktupphandling Handledning, 2021-03-02.

Nytt CRM-system- Handlingsplan - 2019-10-23.xls

Konsekvensbedömning nytt crm system.docx

2.2 Kontrollpunkt IT-projekt och upphandling

Kontrollpunkten avser verksamhetens organisation och rutiner för hantering av dataskyddsfrågor inom IT-projekt och upphandling. I detta ingår till exempel hur verksamheten integrerar dataskyddsfrågor i arbetet med upphandling av nya, samt utvecklingen av, befintliga system och tjänster. Dataskyddsombudet har vid denna kontroll valt att titta på rutiner avseende dataskydd vid IT-projekt och upphandling.

2.2.1 Bedömning

Bolaget har en dokumenterad anvisning/handledning vid upphandling. Inget av dokumenten täcker in dataskydd. Dataskyddskontakten är den som i nuläget säkrar att dataskyddsperspektivet hanteras i bolaget IT-projekt och upphandlingar.

2.2.2 Slutsats

Bolaget behöver dokumentera hur dataskyddsperspektivet tas om hand vid upphandling och i IT-projekt. Bolaget har själva identifierat denna brist och ett arbete är påbörjat för att åtgärda eventuella brister. Dataskyddsombudet har blivit inbjuden för att stödja i detta arbete vilket dataskyddsombudet ser som väldigt positivt.

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 i bolagets IT-system.

2.3.1 Bedömning

Bolaget hanterar kunduppgifter i framförallt IT-systemet Lime. Lime Technologies Sweden AB sköter driften av Lime. Personuppgiftsbiträdesavtal finns tecknat mellan parterna.

I Lime så hanteras bland annat kunduppgifter, prospekt och offerter. Bolagets kunder är i huvudsak juridiska personer. Fritextfält förekommer i IT-systemen och det är upp till bolagets kundansvariga att säkra att inga känsliga personuppgifter finns inlagda. Rutin för hantering av personuppgifter i bland annat fritextfält är under framtagande.

Information till kunderna gällande hur bolaget hanterar personuppgifter ges på bolagets hemsida[1].

Bolaget har en aggregerad informationsklassning/riskanalys av IT-systemet[2]. Bolaget har även dokumenterat införda säkerhetskontroller i en handlingsplan[3]. Inga känsliga personuppgifter får hanteras i IT-systemen.

Dataskyddsombudet har gjort en kontroll i bolagets personuppgiftsbehandlingsregister (Draftit) och vad dataskyddsombudet kunde se så är ovan angivna behandlingarna i IT-systemen upptagna i registret[4].

2.3.2 Slutsats

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

De eventuella risker som finns med fritextfält (att anställda av misstag skriver in känsliga personuppgifter så som sjukdom med mera) i IT-system har bolaget hanterat genom information till de kundansvariga. Det finns inget i nuläget som tyder på att känsliga personuppgifter av misstag har dokumenterats i IT-systemet eller att de åtgärder som bolaget har vidtagit inte skulle vara effektiva. Då det i nuläget inte finns någon skriftlig dokumentation för hur fritextfält ska hanteras i Lime bör bolaget slutföra arbetet med rutinen. Detta för att bolaget ska kunna uppfylla ansvarsskyldigheten i dataskyddsförordningen fullt ut.

De förbättringar som bolaget kan vidta är att även dokumentera informationsklassningen av behandling/IT-system så att det framgår hur bolaget har kommit fram till respektive nivå utifrån konfidentialitet, riktighet och tillgänglighet. Bolaget kan även förbättra informationen till kunden i samband med avtalstecknande genom att skriftligen upplysa kunden om hur bolaget hanterar personuppgifter.

[1] https://gotevent.se/om-got-event/integritetspolicy/
[2] Dokument: Konsekvensbedömning nytt crm system.docx
[3] Dokument: Nytt CRM-system- Handlingsplan - 2019-10-23.xls
[4] Behandlingarna kundregister/CRM och register över avtalskunder,

3 Sammanfattning

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

Det finns tre förbättringsområden som dataskyddsombudet har identifierat vid denna kontroll. Det ena området gäller att dokumentera hur dataskyddsperspektivet tas om hand vid upphandling och i IT-projekt. Bolaget har själva identifierat denna brist och ett arbete är påbörjat för att åtgärda dessa brister. Dataskyddsombudet har blivit inbjuden för att stödja i detta arbete vilket dataskyddsombudet ser som väldigt positivt.

Det andra förbättringsområdet är informationsklassningen av IT-system/behandlingar så att det framgår hur bolaget har kommit fram till respektive nivå utifrån konfidentialitet, riktighet och tillgänglighet.

Det tredje förbättringsområdet är att ge skriftlig informationen till kunden i samband med avtalstecknande om hur bolaget hanterar personuppgifter.

Dataskyddsombudet vill avsluta med att konstatera att dataskyddsombudet har bra förutsättningar att verka i bolaget och att dataskyddsombudet får ett mycket bra stöd av bolagets dataskyddskontakt och övriga medarbetare som dataskyddsombudet har varit i kontakt med.