Göteborgs Stad

Tjänsteutlåtande
Utfärdat 2019-01-22
Diarienummer 0048/18

Handläggare
Katrin Gundersen
Telefon: 031-368 55 12
E-post: katrin.gundersen@gotalejon.goteborg.se

Punkt 19 Avstämningsunderlag från Dataskyddombudet angående status av implementeringen av GDPR

Förslag till beslut i styrelsen för Försäkrings AB Göta Lejon

- anta Avstämningsunderlaget från Dataskyddsombudet angående status av implementeringen av GDPR

Sammanfattning

Dataskyddsombudet för Försäkrings AB Göta Lejon har vid avstämning av implementeringen av GDPR i bolaget tagit fram rekommendationer som bolaget kommer att arbeta med under 2019. Detta arbete kommer att genomföras tillsammans med dataskyddsombudet.

Ekonomiska konsekvenser

Bolaget har inte funnit några särskilda aspekter på frågan utifrån detta perspektiv.

Barnperspektivet

Bolaget har inte funnit några särskilda aspekter på frågan utifrån detta perspektiv.

Mångfaldsperspektivet

Bolaget har inte funnit några särskilda aspekter på frågan utifrån detta perspektiv.

Jämställdhetsperspektivet

Bolaget har inte funnit några särskilda aspekter på frågan utifrån detta perspektiv.

Miljöperspektivet

Bolaget har inte funnit några särskilda aspekter på frågan utifrån detta perspektiv.

Omvärldsperspektivet

Bolaget har inte funnit några särskilda aspekter på frågan utifrån detta perspektiv.

Bilagor

1. Avstämningsunderlag angående implementeringen av GDPR

Ärendet

Beskrivning av ärendet

Enligt Dataskyddsförordningen (GDPR) ska bolaget följa lagstiftningen. Staden har beslutat att en gemensam nämnd med dataskyddsombud ska upprättas för att kunna hjälpa bolagen med implementering och uppföljning samt inneha en rådgivande funktion.

Bolagets bedömning

Det är bolagets bedömning att rekommendationerna i avstämningsunderlaget kommer att kunna genomföras under 2019.

Katrin Gundersen	Annika Forsgren
Ekonomichef	VD

Avstämning av förutsättningar för dataskyddsarbete

Inledning

Stadens dataskyddsombud har till uppgift att övervaka efterlevnaden av dataskyddsförordningen hos samtliga personuppgiftsansvariga förvaltningar och bolag, och kommer som ett led i detta arbete att genomföra periodiska granskningar och uppföljningar av deras arbete. En grundläggande förutsättning för att detta ska vara möjligt är att den personuppgiftsansvarige bedriver ett eget förbättringsarbete inom dataskydd som kan granskas och följas upp.

Därför rekommenderas att det i varje förvaltning eller bolag inrättas någon form av intern funktion med ett utpekat operativt ansvar för dataskyddsfrågor. En sådan *organisation för dataskydd* utformas lämpligen efter de individuella förutsättningar och behov som finns hos varje personuppgiftsansvarig och kan därför variera i form och omfattning. Dataskyddskontakterna bör rimligen ingå i denna organisation.

I syfte att kartlägga hur stadens personuppgiftsansvariga arbetat med detta efterfrågar dataskyddsombuden svar på ett antal avstämningsfrågor. Till skillnad från framtida granskningsprocesser har denna avstämning som ändamål att undersöka om de grundläggande förutsättningarna för dataskyddsarbete finns ute i förvaltningarna och bolagen, samt att verka som en uppföljning av de organisatoriska åtgärder som planerats i de handlingsplaner som togs fram under stödprojektets översyn.

Resultatet från avstämningen kommer utvärderas av dataskyddsombudet och återkopplas till styrelsen/nämnden senast den 30 november 2018.

Avstämningsfrågor

Nedan följer ett antal avstämningsfrågor om förekomsten av och formerna för den personuppgiftsansvariges *organisation för dataskydd*.

I den mån åtgärder är planerade men inte implementerade anges dessa.

Organisation för dataskydd

1. Har ni en organisation med utpekat ansvar för ert dataskyddsarbete?
2. Hur är organisationens ansvar och mandat utformat?
3. Hur är organisationen sammansatt? (en person, en gruppering, m.m.)
4. Vad har motiverat den sammansättningen? (särskilda kompetenser, organisatoriska fördelar m.m.)
5. Vem har den sammankallande/ledande rollen i organisationen?

6. Beskriv i korthet hur arbetet planeras att bedrivas. (Planer, mötesfrekvens, m.m.)
7. Hur säkerställs att organisationens arbete förankras med och når ut till alla delar i verksamheten?
8. Om organisationen bemannas av personal som därtill har ordinarie arbetsuppgifter, hur säkerställs att dessa ges tillräckligt med tid för att dataskyddsarbetet kan bedrivas ändamålsenligt?
9. Hur säkerställer ni att förvaltningsledningen hålls uppdaterad om arbetet?
10. Hur planerar ni att hålla dataskyddsombudet informerat och involverat i organisationens löpande arbete?

Övriga frågor

11. Vilka åtgärder har vidtagits för att informera de registrerade om behandlingen av deras personuppgifter? (”integritetspolicy”, andra informationstexter, m.m.)		
12. Hur tillhandahåller ni informationen till de registrerade? (publicering på hemsida, m.m.)		
Dataskyddsombud		
Har ni anmält vem som är ert dataskyddsombud till Datainspektionen?	Ja	Nej

Göteborgs Stad

Organisatoriska förutsättningar för dataskyddsarbete

Avstämningsrapport för Försäkrings AB Göta Lejon

2018-11-30

Versionshantering

Datum	Version	Beskrivning	Ändrat av
23/11/18	1.0	Utkast	Abtin Kronold
3/011/18	2.0	Slutlig	Abtin Kronold

Innehåll

1 Inledning

1.1 Bakgrund

Dataskyddsförordningen ställer höga krav på den personuppgiftsansvarigas 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.

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

Detta förutsätter i sin tur någon form av intern funktion/organisation med ett utpekat operativt ansvar för den personuppgiftsansvariges implementeringsarbete. En sådan organisation är därför en grundläggande förutsättning för att kunna efterleva dataskyddsförordningen i sin helhet.

Den här avstämningen har därför som syfte att undersöka huruvida en sådan organisation finns och hur den ser ut.

1.2 Utgångspunkter

Enligt artikel 24(1) dataskyddsförordningen ska den personuppgiftsansvarige med bland annat beaktande av behandlingens art, omfattning, sammanhang och ändamål genomföra *lämpliga tekniska och organisatoriska åtgärder* för att säkerställa sin följsamhet gentemot dataskyddsförordningen.

Med organisatoriska åtgärder menas att det ska finnas en dedikerad organisation/funktion med förmåga att planera och implementera dataskyddsförordningen.

Dataskyddsombudets skyldighet att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras vidare i artikel 39 i samma förordning. Ett utflöde av denna skyldighet är därför att genomföra kontroller av den personuppgiftsansvariges organisation.

1.3 Metodbeskrivning

Avstämningen består av tre delar. Den första delen har varit ett frågeunderlag (se bilaga) som har skickats ut per e-post till bl.a. personuppgiftsansvarigas förvaltningsbrevlåda. Underlaget har besvarats av den personuppgiftsansvariga och har sedan skickats tillbaka till dataskyddsombudet.

I den andra delen har dataskyddsombudet gått igenom svaren och vid behov kontaktat den personuppgiftsansvariga för att räta ut eventuella frågetecken. Därefter har en rapport sammanställts.

I den sista delen har dataskyddsombudet gått igenom den preliminära rapporten med den personuppgiftsansvariga antingen i person eller per distans. Detta för tillrätta eventuella missförstånd innan en slutgiltig rapport presenteras.

2 Avstämning

2.1 Organisation för dataskydd

Huvudfokus för avstämningen ligger på att identifiera en organisation/funktion med förutsättningarna för ett löpande implementerings- och dataskyddsarbete.

Nedan redogörs först resultatet utifrån den personuppgiftsansvarigas svar och därefter dataskyddsombudets kommentar.

2.1.1 Ansvar och mandat (fråga 1-2)

2.1.1.1 Resultat

Katrin Gundersen är utsedd dataskyddskontakt med utpekat ansvar för dataskyddsarbetet. Bolaget har tagit fram en rollbeskrivning för dataskyddskontakt men mandat och ansvar ej beskrivet

2.1.1.2 Kommentar

Det är positivt att en dataskyddskontakt är utsedd med ett utpekat ansvar för arbetet. Däremot vore det önskvärt att beskriva rollen mer konkret samt klargöra mandatet.

2.1.2 Sammansättning och ledning (fråga 3-4)

2.1.2.1 Resultat

Försäkrings AB Göta Lejon är ett litet bolag som består av 12 personer, därav endast en person som är dataskyddskontakt. Dataskyddskontakt är tidigare PUL ombud och har tjänsten som bolagsjurist på bolaget.

2.1.2.2 Kommentar

Att endast utse en dataskyddskontakt är rimlig i relation till storlek på verksamheten. Det är positivt att dataskyddskontakten har meriterande kunskaper för att utföra uppdraget.

2.1.3 Arbetsprocesser (fråga 5-6)

2.1.3.1 Resultat

Dataskyddskontakten har den sammankallande rollen i dataskyddsarbetet. Det finns inga planer för hur arbetet ska bedrivas. Liten organisation gör att det är svårt att ta tag i planering.

2.1.3.2 Kommentar

Det är positivt att dataskyddskontakten har den sammankallande rollen i arbetet dock finns det risk för arbetet inte sker eftersom det inte finns plan dokumenterad eller upprättad.

2.1.4 Effektivitetsaspekter (fråga 7-8)

2.1.4.1 Resultat

Dataskyddsombudet har insyn i projekt och får information om olika verksamhetsmöten om problem uppstår.

Det är oklart hur mycket tid rollen som dataskyddskontakt kommer att ta i anspråk.

2.1.4.2 Kommentar

DSO har inte haft något större insyn i projekt. Viss kommunikation har funnits med DSO:t. Det är positivt att rollen utreds för att avgöra hur mycket tid som behövs för att fullgöra uppdraget.

2.1.5 Återrapportering och uppföljning (fråga 9-10)

2.1.5.1 Resultat

Rapporterar riktlinje och policy till styrelsen samt inom den interna organisationen. Bolaget står under tillsyn av Finansinspektionen och har därför även en egen regelefterlevnadsfunktion som genomför revisioner över regelefterlevnaden.

Rutin har ej tagit fram för att hålla dataskyddsombudet informerat och involverat i organisationens löpande arbetet och krav på frekvens och typ av information har ej inkommit från DSO.

2.1.5.2 Kommentar

Det finns rutiner sedan tidigare gällande återrapportering till styrelsen för ärenden gällande regelefterlevande som står under tillsyn av Finansinspektionen. Det finns dock inga rutiner för att involvera eller informera DSO:t, vilket önskas.

2.2 Övriga frågor

Jämte det organisatoriska perspektivet görs även en avstämning av några särskilda frågor som bedömts angelägna att kontrollera i detta inledande skede.

2.2.1 Informationsåtgärder

2.2.1.1 Resultat

Eftersom vi hanterar personuppgifter för skadelidande baserar vi detta på avtal och vi har även information på goteborg.se hur personuppgifter hanteras.

2.2.1.2 Kommentar

Det är positivt att den lagliga grunden för personuppgiftsbehandling har identifierats. Vidare har en informationstext tagits fram och finns publicerad på hemsida. Dock kan texten bearbetas ytterligare för att bl.a. möta alla krav enligt dataskyddsförordningen.

2.2.2 Anmälan av dataskyddsombud

2.2.2.1 Resultat

Ja

2.2.2.2 Kommentar

Försäkrings AB Göte Lejon har anmält dataskyddsombud hos tillsynsmyndigheten.

3 Sammanfattande kommentar

Det är positivt att en dataskyddskontakt har utsett men en rollbeskrivning vore önskvärt. Antal dataskyddskontakt i relation till verksamheten är rimlig. Vidare har dataskyddskontakten meriterande kunskaper för rollen, vilket är positivt.

Det är även önskvärt att en plan för dataskyddsarbete utarbetas och dokumenteras. Vidare är det önskvärt att DSO:s informeras om och involveras i den planen.

Det är positivt att Försäkring AB Göta Lejon har utformat egen informationstext. Den bör dock bearbetas ytterligare i samråd med DSO-enheten.