Göteborgs Stad

Organisatoriska förutsättningar för dataskyddsarbete

Avstämningsrapport för Störningsjouren i Göteborg AB

2018-11-00

Versionshantering

Datum	Version	Beskrivning	Ändrat av
2018-11-14	0,1	Första utkast	Nina Havner
2018-11-21	0,1	Utkast skickas till bolaget för kommentar	Nina Havner

Innehåll

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. För att uppnå detta måste varje personuppgiftsansvarig bedriva ett eget förbättringsarbete inom dataskydd. Detta förutsätter i sin tur någon form av intern funktion med ett utpekat operativt ansvar för den personuppgiftsansvariges dataskyddsarbete. En sådan organisation för dataskydd är därför en grundläggande förutsättning för att kunna följa dataskyddsförordningen i sin helhet.

Den här avstämningen har därför som syfte att undersöka huruvida Göteborgs Stads personuppgiftsansvariga har vidtagit eller planerar att vidta åtgärder som möjliggör ett sådant löpande dataskyddsarbete.

1.2 Utgångspunkter

I dataskyddsförordningens artikel 24(1) framgår att den personuppgiftsansvarige 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. Från detta utläser man kravet på en organisatorisk förmåga att planera och implementera sådana åtgärder.

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

1.3 Metodbeskrivning

Avstämningen har skett genom att ett förfrågningsunderlag skickades till bolagets dataskyddskontakt per epost den 11 september 2018. Underlaget bestod av ett antal på förhand specificerade frågor. Bolaget har varit fri att formulera sina svar efter eget gottfinnande, utan påseende av dataskyddsombudet. Bolagets svar inkom den 19 oktober 2018.

I den del dataskyddsombudet lämnar synpunkter och/eller andra kommentarer på svaren görs detta endast på basis av vad som framkommer i det skriftliga svarsunderlaget, och med beaktande av att någon kontroll av de egentliga sakförhållandena inte varit föremål för denna process. Dataskyddsombudets kommentarer sker därför i detta skede endast utifrån allmänna grundsatser om vad som framstår som rimligt i den givna situationen.

2 Avstämning

2.1 Organisation för dataskydd

Huvudfokus för avstämningen ligger på de organisatoriska förutsättningarna för ett löpande dataskyddsarbete. Nedan redogörs för resultatet från avstämningen och dataskyddsombudets kommentarer.

2.1.1 Ansvar och mandat (fråga 1–2)

2.1.1.1 Resultat

Störningsjouren i Göteborg AB har beslutat om en övergripande struktur för dess dataskyddsorganisation. Som redovisats kommer denna även i fortsättningen att bestå av fyra dedicerade funktioner som i olika grad ansvarar för det strategiska och operativa arbetet, dataskyddskontakt, VD, styrelsen samt dataskyddskoordinator på koncernnivå. Förutom styrelsen som sådan ingår även dataskyddsombudet utöver personalkollektivet i strukturen och har därmed identifierats som relevanta aktörer i det övergripande dataskyddsarbetet.

Fördelningen i ansvar och mandat för dessa olika skikt varierar. I all väsentlighet har denna fördelning gjorts utifrån en modell om beslutande, styrande, stödjande, och verkställande funktioner, och sammanfaller naturligt med den hierarkiska hemvisten i organisationen.

2.1.1.2 Kommentar

Den beslutade organisationen framstår som genomtänkt. Att särskild vikt lagts vid att förankra dataskyddsfrågan i både bolagets ledning och på koncernnivå ses som positivt.

2.1.2 Sammansättning och ledning (fråga 3–4)

2.1.2.1 Resultat

Organisationen styrs ytterst av styrelsen, ledd av bolagets VD. Dataskyddskontakt besätts i sin tur av personal med kompetens inom administration och rapporterar direkt till VD som rapporterar till styrelsen. Dataskyddskontakten ansvarade för kartläggningen av

personuppgiftsbehandlingar och förberedande arbetet runt införandet av dataskyddsförordningen. Rollen som administratör var ur organisatoriskt perspektiv bäst lämpad som dataskyddskontakt. I dataskyddskontaktens uppdrag ingår även att representera bolaget i regelbundna möten i en koncerngemensam arbetsgrupp s.k. DSF-råd.

DSF-rådet består av dataskyddskontakter från dotterbolagen med olika och kompletterande kompetenser som knyter an till de olika verksamhetsprocesser som aktiveras i samband med ett koncernövergripande och stödjande dataskyddsarbete. Dataskyddskoordinator har ett övergripande uppdrag i koncernen och fungerar som stöd och är sammankallande för DSF-rådet.

2.1.2.2 Kommentar

Kompetensfördelningen tycks heltäckande och genomtänkt som tillsammans med ett koncernövergripande samarbete och dess kompetenser framstår som välbalanserade.

2.1.3 Arbetsprocesser (fråga 5–6)

2.1.3.1 Resultat

Organisationens uppdrag är att ta fram rutiner och processer för att bland annat hantera den registrerades rättigheter, hantera personuppgiftsincidenter, administrera och underhålla personuppgiftsbiträdesavtal, samt arbeta med utbildning och information inom den egna verksamheten.

VD har den sammankallande och ledande rollen i organisationen. Dataskyddskontakten arbetar med interna utbildningsinsatser bl.a. genomförs introduktionsutbildningar till nyanställda medarbetare och en gång per år genomförs en utbildningsinsats till all personal.

Den operativa samordningen av koncerngemensamma rutiner i DSF-rådet sker ca två gånger per månad och kommuniceras av dataskyddskontakten till VD genom löpande avstämning. VD i sin tur informerar löpande både sin ledningsgrupp och styrelsen. Exempel på planerade koncerngemensamma insatser är rutiner och rapport för personuppgiftsincidenter och registerutdrag.

I avvaktan på ett staden gemensamt personuppgiftsregister, Draftit Privacy Records planeras andra operativa insatser utifrån en verksamhetsspecifik nivå (av bolagsspecifik karaktär). T.ex. kontinuerliga kontroller av system och personuppgiftsbiträden men även egna interna kontroller avseende personuppgiftsbehandling bl.a. genom stickprovskontroller gällande hantering av känsliga personuppgifter.

2.1.3.2 Kommentar

Att organisationen redan i detta tidiga skede satt en färdplan med fastlagd regelbundenhet för möten, interna kontroller och utbildningsinsatser borgar för att frågorna behåller sin relevans över tid. Medvetenhet om dataskyddsfrågorna

finns både hos beslutsfattare och medarbetare vilket ses som en förutsättning för att frågorna hålls vid liv, något som bolaget lagt en god grund för.

2.1.4 Effektivitetsaspekter (fråga 7-8)

2.1.4.1 Resultat

Avgörande för effektiviteten i dataskyddsarbetet är bland annat till vilken grad dataskyddsperspektiven når ut till samtliga delar av bolagets verksamhet. Genom beskriven informationskedja enligt ovan 3.1.3 Arbetsprocesser inklusive kontinuerliga utbildningsinsatser avses informationsspridningen till dessa delar underlättas.

En annan effektivitetsaspekt är att organisationen ges faktiska tidsresurser för att agera på ett verkningsfullt sätt. Arbete med dataskydd uppges vara prioriterat område för Dataskyddskontakten. Medan några särskilda åtgärder för reglering av tidsåtgången inte är planerade framkommer alltjämt att organisationens interna funktioner planerat sitt arbete med sådan regelbundenhet att tid i vart fall formellt avsatts för arbetet.

2.1.4.2 Kommentar

Med tanke på dataskyddskontaktens utpekade roll och kompetens framstår bolaget ha goda förutsättningar för att bedriva ett dugligt dataskyddsarbete. Då den faktiska effektiviteten först kan bedömas i efterhand ter sig den nuvarande organisationen inte uppvisa några uppenbara brister i detta avseende.

2.1.5 Återrapportering och uppföljning (fråga 9-10)

2.1.5.1 Resultat

Dataskyddskontakt och VD utgör navet som bolagets dataskyddsorganisation kopplar an till. Utöver kontinuerliga möten med personalen och dataskyddskontaktens löpande avstämning med VD informeras såväl ledningsgruppen som styrelsen. Därutöver får styrelsen information och iakttagelserapporter från dataskyddsombudet två gånger per år. En kontinuerlig mötesavstämning mellan dataskyddskontakten och dataskyddsombudet är inplanerad minst en gång per kvartal och mer vid behov.

Koncernens dataskyddskoordinator har avstämningar till dataskyddsombudet om det övergripande arbetet i koncernen.

Därigenom byggs en kedja för återkoppling som sträcker sig från det operativa planet till det ytterst ansvariga.

Bolaget planerar att regelbundet samarbeta med dataskyddsombudet vid särskilda händelser som t.ex. personuppgiftsincidenter liksom andra möten av större vikt.

2.1.5.2 Kommentar

Bolaget har etablerat en formell struktur för rapportering och uppföljning som verkar nå och täcka hela organisationen. Dataskyddsombudets uppfattning är att bolaget genom dataskyddskontakten ger dataskyddsombudet goda möjligheter att utföra sitt arbete med att följa upp bolagets dataskyddsarbete.

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

Bolaget har tagit fram informationsmaterial/”integritetspolicy” *Skydd och behandling av personuppgifter* som har publicerats på bolagets hemsida. Informationsmaterialet har även kommunicerats med all personal. Andra blanketter t.ex. registerutdrag har också uppdaterats och publicerats som serviceåtgärd för kunderna/de registrerade.

Anpassningar av information som lämnas i anställningsavtal har även skriftligt meddelats personalen.

2.2.1.2 Kommentar

Dataskyddsombudet bedömer att det finns goda förutsättningar för den registrerade att få information om bolagets behandling av personuppgifter. Dataskyddsombudet har i denna avstämning inte granskat om informationsinnehållet uppnår tillräcklig grad av transparens eller tillgänglighet utifrån dataskyddsförordningen krav.

Bolaget tycks ha en tydlig bild om vad som behöver göras i det fortsatta arbetet.

2.2.2 Anmälan av dataskyddsombud

2.2.2.1 Resultat

Anmälan om dataskyddsombud har gjorts till Datainspektionen.

2.2.2.2 Kommentar

Dataskyddsombudet har fått bekräftelse att registrering har utförts från Datainspektionen.

3 Sammanfattande kommentar

Störningsjouren i Göteborg AB har i sitt svar till avstämningsunderlaget presenterat en genomarbetat och ambitiös plan för sin dataskyddsorganisation. Genom att ta höjd för behovet av ökad eller kontinuerlig medvetenhet involveras hela verksamheten från strategiskt till operativ nivå vilket bekräftar förståelse för den genomgripande och verksamhetsövergripande natur som dataskyddsfrågorna får. Graden av tilltänkthet vid utformandet av denna organisation siar om att frågan prioriterats och tillerkänts sin vikt i sammanhanget.

Dataskyddsombudet är i stort positivt till den struktur som presenterats och dataskyddskontakten ger dataskyddsombudet goda förutsättningar och ett bra stöd i att utföra sitt arbete i bolaget.