Intraservice

Göteborgs Stad

Organisatoriska förutsättningar för dataskyddsarbete

Avstämningsrapport för Bostads AB Poseidon

2018-11-28

Versionshantering

Datum	Version	Beskrivning	Ändrat av
2018-11-23	0,1	Första utkast	Nina Havner
2018-11-26	0,1	Utkast skickas till DSK för kommentar	Nina Havner
2018-11-28		Slutlig version	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 16 oktober 2018.

I den del dataskyddsombudet lämnar synpunkter och-/eller andra kommentarer på svaren görs detta endast på basis av vad som framkommit 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

Bostads AB Poseidon har beslutat om en övergripande struktur för dess dataskyddsorganisation. Som redovisats kommer denna bestå av en dedicerad person, dataskyddskontakten, utsedd av bolagets VD och meddelad kontaktperson till dataskyddsombudet samt koncernens dataskyddskoordinator.

Dataskyddskontakt är bolagets interncontroller och tillhör avdelningen Administrativ utveckling på bolagets huvudkontor. Dataskyddskontaktens ansvar är att hålla ihop bolagets dataskyddsfrågor gentemot organisationen och gentemot koncernens dataskyddskontakt samt kontaktperson gentemot dataskyddsombudet. Dataskyddskontaktens uppgift är att vara rådgivande för organisationen i dataskyddsfrågor och kontrollera efterlevnaden gällande lagar och regelverk.

Utöver dataskyddskontaktens utpekade ansvar för det strategiska och operativa dataskyddsarbetet ingår styrelsen som sådan, VD och ledningsgruppen, dataskyddsombudet samt det stora 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 och robust. Att särskild vikt lagts vid att tydligt urskilja de beslutande, stödjande och utförande

uppgifterna samt förankra dataskyddsfrågan både i bolagets ledning och på koncernnivå ses som positivt.

2.1.2 Sammansättning och ledning (fråga 3–4)

2.1.2.1 Resultat

Organisationen leds av VD och styrs ytterst av styrelsen. Den nytillträdda dataskyddskontakten är bolagets interncontroller med juridisk kompetens och tillhör avdelningen Administrativ utveckling på bolagets huvudkontor.

I den planerade organisationen kommer en grupp av nyckelpersoner att utses med olika kompetenser knutna till bolagets kärnverksamhet och stödfunktioner under ledning av dataskyddskontakten. I dataskyddskontaktens uppdrag ingår även att representera bolaget i regelbundna möten i en koncerngemensam arbetsgrupp, dataskyddsrådet.

Dataskyddsrådet 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. Koncernens dataskyddskontakt har ett övergripande uppdrag att fungera som stöd och är sammankallande för dataskyddsrådet.

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.

Dataskyddskontakten har den sammankallande och ledande rollen i organisationen. I den interna arbetsgruppen som planeras kommer nyckelpersoner från områdena HR, IT, kommunikation, inköp, uthyrning och förvaltning att ingå. Mötesfrekvens är ännu inte fastställd.

Den operativa samordningen i dataskyddsrådet sker ca två gånger per månad och koncernens dataskyddskontakt är sammankallande. Dataskyddsrådet ska behandla gemensamma frågor och vara ett forum för erfarenhetsutbyte.

2.1.3.2 Kommentar

Bolaget har sedan tidigare satt en färdplan med fastlagd regelbundenhet för möten, interna kontroller och utbildningsinsatser vilket 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. Arbetsprocesser inklusive kontinuerliga utbildningsinsatser åsyftas underlätta informationsspridningen.

Under våren 2018 stod dåvarande dataskyddskontakt tillika projektledare för införandet av dataskyddsarbete i enlighet med dataskyddsförordningen. Samtliga medarbetare fick utbildningen genom medverkan på arbetsplatsträffar. Ett flertal nyckelpersoner deltog i införandet. Göteborgs Stad via Stadsledningskontorets stödprojekt, genomförde e -learning utbildning under våren 2018 riktad till samtliga medarbetare. Tanken är att nyckelpersonerna i den interna arbetsgruppen ska fungera som länk ut i organisationen för att informera, diskutera och fånga upp aktuella frågeställningar. Dataskyddskontakten kommer även i fortsättningen att hålla löpande utbildning/information om dataskyddsfrågor. Bolaget planerar att ta fram ett introduktionspaket för nyanställda medarbetare vilket även diskuteras i koncernens dataskyddsråd.

En annan effektivitetsaspekt är att organisationen ges faktiska tidsresurser för att agera på ett verkningsfullt sätt. Arbete med dataskydd uppfattas vara prioriterat område för dataskyddskontakten. Förutom dataskyddsarbetet ingår främst att hålla ihop hyresjuridiska frågor samt arbete med riskanalys och bolagsövergripande internkontroll. Rapportering görs till administrativ chef som ingår i företagsledningen och är ”back-up” för dataskyddsarbetet. 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 både tidigare och nuvarande dataskyddskontaktens utpekade roll och kompetens framstår bolaget ha bra strategi och goda förutsättningar för att bedriva ett ändamålsenligt dataskyddsarbete. Även om den faktiska effektiviteten först kan bedömas i efterhand ter sig den nuvarande organisationen prioritera dataskyddsarbetet vilket är positivt.

2.1.5 Återrapportering och uppföljning (fråga 9–10)

2.1.5.1 Resultat

Dataskyddskontakt och den interna arbetsgruppen utgör navet som bolagets dataskyddsorganisation kopplar an till. Under införandefasen gjordes avrapportering om status i projektet till företagsledningen genom medverkan på ledningsgruppsmöte.

Dataskyddskontakten har löpande avstämning och rapporterar till administrativ chef som ingår i företagsledningen och ansvarar för att frågorna lyfts på ledningsnivå. Bolagets styrelse har fastställt att dataskyddsombudet ska medverka vid två styrelsemöten per år. Dataskyddsombudet deltog vid styrelsemötet den 27 september 2018.

Bolaget planerar att regelbundet bjuda in dataskyddsombudet till möte med bolaget. Utöver styrelsemöten två gånger per år kommer dataskyddsombudet även att medverka vid ledningsgruppsmöten någon gång per år. Dataskyddsombudet deltog på ledningsgruppsmötet den 15 november 2018. Bolaget planerar att regelbundet samarbeta med dataskyddsombudet vid särskilda händelser t.ex. personuppgiftsincidenter liksom andra möten av större vikt.

Dataskyddsombudet kommer även regelbundet att bjudas in till gemensamma möte i koncernens dataskyddsråd.

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

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 har en genomtänkt plan och 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. Informationsmaterial till personal finns på bolagets intranät. Nyanställd

personal får information i samband med anställning. Andra blanketter t.ex. samtycke, i de fall detta krävs, har uppdaterats men även registerutdrag som serviceåtgärd för kunderna/de registrerade och har även publicerats på bolagets hemsida.

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.

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

Bostads AB Poseidon har i sitt svar till avstämningsunderlaget presenterat en genomarbetat och ambitiös plan för sin dataskyddsorganisation. Genom att ta höjd för behovet av flera olika nivåer, från strategiskt till operativ, har bolaget visat 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.

Nina Havner

Dataskyddsombud