Göteborgs Stad

Organisatoriska förutsättningar för dataskyddsarbete

Avstämningsrapport för Familjebostäder i Göteborg AB

2018-11-29

Versionshantering

Datum	Version	Beskrivning	Ändrat av
2018-11-26	0,1	Första utkast	Nina Havner
2018-11-26	0,1	Utkast skickas till DSK för kommentar	Nina Havner
2018-11-29		Slutversion	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 15 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

Familjebostäder i Göteborg AB har beslutat om en övergripande struktur för dess dataskyddsorganisation. Som redovisats kommer denna bestå av flera dedicerade funktioner som i olika grad ansvarar för det strategiska och operativa arbetet.

Dataskyddskontakten är utsedd av VD och har ett övergripande ansvar för att leda, följa upp och rapportera dataskyddsarbetet utifrån dataskyddsförordningen.

Utöver dataskyddskontaktens utpekade ansvar för det strategiska och operativa dataskyddsarbetet ingår styrelsen som sådan, VD och ledningsgruppen, säkerhetschefen och informationssäkerhetssamordnaren i organisationsstrukturen. Dataskyddskontakten är bolagets ekonomichef och ingår i bolagets ledningsgrupp.

Bolagets säkerhetschef har ett ansvar för alla säkerhetsfrågor vilket också berör informationssäkerhet och dataskydd. Bolaget har utpekade systemägare och systemansvariga med ansvar för dataskydd för respektive systems dataskydd.

På koncernnivå finns dataskyddskoordinator som samordnar rutiner och frågeställningar och leder en arbetsgrupp med representanter tillika dataskyddskontakter från de olika bolagen som träffas varannan vecka. I den arbetsgruppen och för bolagets vidkommande deltar dock informationssäkerhetssamordnaren.

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 bolagets VD och styrs ytterst av styrelsen. Bolaget har genomfört ett arbete i projektform som involverat en rad resurser, bl. a inom IT, verksamhetscontroller, jurist, information och chefer. Informationssäkerhetssamordnaren har under styrgruppen lett detta arbete. Dessa personer har byggt upp en kompetens kring frågorna och deltar i det fortsatta arbetet. Grupperingen är inte fast utan resurser medverkar i mån av behov beroende på frågornas karaktär.

Motivet till den organisatoriska sammansättningen är att skapa den breda kompetensen i grupperingen som krävs för att hantera frågeställningarna. Samtliga personer är placerade på huvudkontoret Södra Vägen och de flesta tillhör Ekonomiavdelningen. Kompetenserna är knutna till bolagets kärnverksamhet och stödfunktioner med samarbetskoppling till varandra och stora delar av verksamheten i sitt övriga arbete.

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, som också är ekonomichef och ansvarig chef för de flesta av de berörda, har ansvaret för det bolagsövergripande arbetet. Informationssäkerhetssamordnaren har en viktig roll att följa upp och koordinera arbetet. Personerna samverkar utifrån behov och frågornas karaktär.

Bolaget jobbar i stor utsträckning fortfarande med hantering och uppföljning av frågor och behov som identifierats under införandeprojektet. Bolaget gör nu en ny uppföljning för att identifiera de kvarstående frågor men också nya frågor om behandlingar som tillkommit i samverkan mellan dataskyddskoordinatorn

och informationssäkerhetssamordnaren för bolaget. Den operativa samordningen i dataskyddsrådet sker ca två gånger per månad och dataskyddskoordinatorn är sammankallande.

Parallellt med detta planeras för hur löpande kontroller av dataskyddsarbetet ska formas. Avsikten är att så långt som möjligt integrera detta i bolagets övriga arbete med intern styrning och kontroll.

2.1.3.2 Kommentar

Bolaget har sedan tidigare satt en färdplan med fastlagd regelbundenhet för möten, interna kontroller 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.

Bolagets dataskyddsarbete förankras i organisationen genom information på intranätet som innehåller både allmänna och i styrande dokument. Cheferna som kanal för att nå verksamheten etablerades under införandeprojektet och är fortsatt en informationsväg till och från verksamheten. Under projektets gång genomfördes också olika informationsinsatser för all personal.

Dataskyddsinformationsavsnitt har tagits in i bolagets introduktionsutbildning. HR avdelningen ansvarar för materialet som kallas *Under vårt tak* och avsikten med utbildningen är också att den kan och kommer att genomföras repetitivt av personalen.

En annan effektivitetsaspekt är att organisationen ges faktiska tidsresurser för att agera på ett verkningsfullt sätt. Arbete med dataskydd uppges vara bolagets chefers ansvar och frågan kommer att följas upp av dataskyddkontakten tillika ekonomichefen. Flera av nyckelresurserna är också underställda och ingår i dataskyddskontaktens personalstyrka. 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 kompetensbredd och omfattning som organisationen getts 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

Dataskyddskontakten och den interna arbetsgruppen utgör navet som bolagets dataskyddsorganisation kopplar an till. Dataskyddskontakten ingår i ledningsgruppen och säkerställer genom sin medverkan i ledningsgruppsmöten att företagsledningen hålls uppdaterad.

Bolagets styrelse har fastställt att dataskyddsombudet ska medverka vid två styrelsemöten per år. Dataskyddsombudet planeras delta vid styrelsemöte den 10 december 2018.

Bolaget planerar att regelbundet bjuda in dataskyddsombudet till möte med bolaget. 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 möten 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 *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. Information vid vissa specifika behandlingar, både

behandlingar som berör hyresgäster och medarbetare, har upprättats och delgivits de registrerade.

Utöver information som tillhandhålls på bolagets hemsida och intranät delges information via hyresgästtidning och nyhet på webb. Ny informationsbilaga vid tecknande av hyresavtal och ny avtalsbilaga till anställningskontrakt används. Befintliga anställda har fått mejl med skriftlig information. Vid vissa behandlingar, tex utlämnande av elektroniska låsbrickor används separata skriftlig information. I något fall ges information direkt i system.

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

Familjebostäder 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 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