Styrelsehandling 16
Älvstranden Utveckling AB
Dnr 0097/19
2019-10-25
Patrik Lindberg

ÄLVSTRANDEN UTVECKLING
ETT BOLAG I GÖTEBORGS STAD

Informationsärende – dataskyddsarbetet på Älvstranden Utveckling

Sammanfattning

På styrelsesammanträdet får vi besök av Martin Brunhage som arbetar på Intraservice och är dataskyddsombud för Älvstranden Utveckling.

Martin berättar för styrelsen om sitt och vårt arbete kring datasäkerhet.

Den aktuella rapporten från 2019-09-30 finns med som Bilaga 1.

Bakgrund

I Göteborgs Stad ansvarar varje enskild nämnd och bolagsstyrelse för personuppgifter och ansvarar därigenom att behandla personuppgifterna enligt dataskyddsförordningens bestämmelser.

För att säkerställa detta måste varje personuppgiftsansvarig bedriva ett eget förbättrings-arbete inom dataskydd. Det förutsätter i sin tur någon form av intern funktion med ett utpekat operativt ansvar för den personuppgiftsansvariges dataskyddsarbete.

En sådan funktion finns på Älvstranden Utveckling.

Den aktuella rapporten

Den bifogade rapporten är vald utifrån dataskyddsombudets bedömning att behandlingen av de anställdas personuppgifter ligger högst i risk utifrån de registrerades fri- och rättigheter av de personuppgiftsbehandlingar bolaget utför.

Olika 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.

ÄLVSTRANDEN UTVECKLING
ETT BOLAG I GÖTEBORGS STAD

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.

Föredragande

Martin Brunhage dataskyddsombud för Älvstranden Utveckling och som arbetar på Intraservice.

Bilagor

Bilaga 1. Behandling av anställdas personuppgifter. Granskningsrapport för Älvstranden Utveckling AB.

Göteborgs Stad

Behandling av anställdas personuppgifter

Granskningsrapport för Älvstrandens Utveckling AB

2019-09-30

Innehåll

1 Inledning 3

1.1 Bakgrund 3

1.2 Granskningsområde 3

1.3 Tillvägagångssätt 3

2 Granskningen 4

2.1 Granskade dokument 4

2.2 Område 1 Personuppgiftsbiträdesavtal och personuppgiftsbiträdeskontroll 4

2.2.1 Bedömning 5

2.2.2 Slutsats/Rekommendation 5

2.3 Område 2 Dokumenterade medarbetarsamtal 6

2.3.1 Bedömning 6

2.3.2 Slutsats 7

2.4 Område 3 Informationsplikt anställda 7

2.4.1 Bedömning 7

2.4.2 Slutsats 7

2.5 Område 4 Är personuppgiftsbehandlingarna upptagna i personuppgiftsbehandlingsregistret 7

2.5.1 Bedömning/Slutsats 8

2.6 Område 5 Sker kontrollåtgärder gentemot anställda och är de i linje med dataskyddsförordningen 8

2.6.1 Bedömning 8

2.6.2 Slutsats 8

3 Sammanfattning 9

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 Granskningsområde

En utgångspunkt i dataskyddsförordningen är att personuppgiftsansvarig och dataskyddsombud ska arbeta riskbaserat. Dataskyddsombudet har vid denna granskning valt att titta på hur bolaget hanterar de anställdas personuppgifter och om behandlingen av dessa uppgifter är i linje med dataskyddsförordningens krav. Området är valt utifrån dataskyddsombudets bedömning att behandlingen av de anställdas personuppgifter ligger högst i risk utifrån de registrerades fri- och rättigheter av de personuppgiftsbehandlingar som bolaget utför.

Granskningen är uppdelad i fem delområden som tar sikte på bland annat om formella krav enligt dataskyddsförordningen är uppfyllda och om bolaget har vidtagit rimliga skyddsåtgärder vid behandlingen av de anställdas uppgifter.

1.3 Tillvägagångssätt

Granskningen har utförts genom intervjuer och dokumentgranskning, Intervjuer har skett med bolagets dataskyddskontakter, IT-ansvarig, HR-ansvarig och löneadminstratör. Granskningens delområden täcker inte all den behandling av anställdas personuppgifter som utförs i bolaget. I delområdena har ett eller flera stickprov tagits utifrån bolagets stödjande och styrande dokument. Utifrån granskningsunderlaget skapade dataskyddsombudet ett första utkast till denna granskningsrapport som dataskyddskontakterna 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 granskningsrapporten görs detta endast på basis av vad som framkommit i de granskade dokumenten och vad som framkommit i intervjuer med ovan nämnda.

2 Granskningen

2.1 Granskade dokument

Blankett prestationssamtal

Blankett utvecklingssamtal

Information personal

Personuppgiftsbiträdesavtal mellan Älvstranden Utveckling AB och Förvaltnings AB Göteborgslokaler (20180515 dianummer 0479/18)

Generell överenskommelse och Avtal (2015-12-29 diarienummer 1138/15.1) även benämnt som tjänsteavtal.

Checklista nyanställning_plrev190822

Anvisning för IT-användning (Diarienummer 1146/15, Upprättad 2017-01-23 Version 2.0)

Anvisning mobiltelefon_surfplatta_bärbar dator (skapad 2015-04-27)

Personalhandboken (diarienr 0589/15)

Avtal innehav mobiltelefon surfplatta bärbar dator.

2.2 Område 1 Personuppgiftsbiträdesavtal och personuppgiftsbiträdeskontroll

Vid hantering av personuppgifter som sker hos annan (personuppgiftsbiträde) än personuppgiftsansvarig krävs enligt dataskyddsförordningen[1] att bolaget reglerar ansvaret mellan parterna och att bolaget ger instruktioner till biträdet hur uppgifterna får behandlas. Det finns inga krav i dataskyddsförordningen som styr hur detta ska regleras mellan parterna men det har utvecklats en praxis på området att man gör detta via ett separat avtal som benämns personuppgiftsbiträdesavtal (PUB-avtal). Personuppgiftsansvarig har även ansvar att kontrollera att personuppgiftsbiträdet hanterar personuppgifterna på avtalat sätt. Detta krav kan härledas till principen ansvarsskyldighet i dataskyddsförordningen[2] Principen ansvarsskyldighet innebär att personuppgiftsansvarig ska kunna visa att och hur bolaget lever upp till dataskyddsförordningen. Kontrollen av personuppgiftsbiträdet kan ske på många olika sätt. Exempel på kontroller är revison i biträdets lokaler och/eller ta del av biträdes egenkontroller och/eller ta del av biträdets granskningsrapporter utifrån eventuell certifiering[3]. Bolagets personuppgiftsbiträdeskontroller ska alltid dokumenteras. I denna granskning har dataskyddsombudet valt att granska

[1] Artikel 28.3 dataskyddsförordningen
[2] Artikel 5 dataskyddsförordningen
[3] Exempelvis ledningssystem för informationssäkerhet ISO 27001

om bolaget uppfyller dessa krav i personuppgiftsbehandlingen "Hantera anställning".

2.2.1 Bedömning

Enligt uppgift i personuppgiftsbehandlingsregistret hanteras merparten av personuppgifterna i ett IT-system som levereras från företaget Hogia Aktiebolag och där driften hanteras av Förvaltnings AB Göteborgslokaler (Framtidens IT). Bolaget och Framtidens IT har upprättat ett personuppgiftsbiträdesavtal (diarienummer 0479/18) och ett tjänsteavtal (Generell Överenskommelse och Avtal, diarienummer 1138/15.1).

Personuppgiftsbiträdesavtalet mellan bolaget och personuppgiftsbiträdet är skrivet på en övergripande nivå och tar sikte på all behandling som personuppgiftsbiträdet utför för bolaget. Bolaget har större delen av sin IT-relaterade drift hos Framtidens IT. I personuppgiftsbiträdesavtalets punkt 2.3 finns en hänvisning till tjänsteavtalet. I tjänsteavtalet beskrivs behandlingarna/informationsbärarna och instruktionerna till personuppgiftsbiträdet med en högre detaljgrad.

I tjänsteavtalet förekommer ingen hänvisning till IT-systemet från Hogia eller referens till behandlingen "Hantera Anställning". IT-ansvarig på bolaget har i samtal med dataskyddsombudet bekräftat att inga ytterligare sidoavtal finns avseende IT-systemet från Hogia utan de generella krav som beskrivs i tjänsteavtalet ska anses gälla mellan parterna.

Enligt uppgift från IT-ansvarig ska bolaget byta till ny leverantör av IT-relaterade tjänster.

Bolaget har inte utfört någon kontroll/revision av Framtidens IT:s hantering av IT-systemet från Hogia utifrån avtalade krav. Enligt IT-ansvarig så är bolaget på gång med att införa systematiska kontroller av bolagets personuppgiftsbiträden.

2.2.2 Slutsats/Rekommendation

Dataskyddsombudets rekommendation är att bolaget vid byte av leverantör tydligare beskriver i avtalshandlingarna vilka personuppgiftsbehandlingar/informationsbärare som hanteras av det nya personuppgiftsbiträdet. Bolaget bör även i avtalshandlingarna tydliggöra sina instruktioner till personuppgiftsbiträdet utifrån informationsbärare/personuppgiftsbehandling för att vara följsamma utifrån dataskyddsförordnings krav.

Utifrån effektivitetsskäl kan det vara en lämplig åtgärd att bolaget lyfter frågan till Göteborgs Stadshus AB, via Higab, om de kan ta fram avtalsmallar gällande tjänsteavtal. Avtal av denna typ är komplexa och i bolaget (och de flesta andra bolag i Göteborgs Stad)) är det en sällanuppgift att skriva den här typen av avtal. Avtalsmallar skulle kunna minska kostnaderna för bolaget men även för andra bolag i Göteborgs Stad då det oftast krävs ganska omfattande extern

juridisk rådgivning. Avtalsmallar för Göteborgs Stads bolag skulle även medföra en harmonisering/standardisering av avtalen vilket i sin tur kan leda till en högre kvalité och minskade risker för tolkningsutrymme i avtalen. Om Tjänsteleverantören är ett bolag eller en förvaltning i Göteborgs Stad borde avtalen dessutom kunna förenklas då riskerna är mindre än med externa leverantörer (exempelvis konkurs, uppköp och hur skadestånd ska regleras).

Bolaget är på gång med att införa kontroller av bolagets personuppgiftsbiträden. Dataskyddsombudet rekommenderar att kontrollernas frekvens och omfattning bestäms utifrån de risker behandlingarna medför för de registrerades fri- och rättigheter.

2.3 Område 2 Dokumenterade medarbetarsamtal

Utifrån riskerna för de anställdas fri- och rättigheter har dataskyddsombudet valt att granska hantering av de dokumenterade medarbetarsamtal som utförs i bolaget. Medarbetarsamtalen kan ha olika benämning och syften som varierar mellan olika verksamheter. Utifrån samtalsmallens frågor kan det finnas risk för att känsliga personuppgifter hanteras. Då det ofta förekommer öppna frågeställningar i medarbetarsamtalen finns det en risk för att information om hälsostatus eller andra känsliga/skyddsvärda personuppgifter av misstag kan komma att dokumenteras i samtalsmallarna. Exempel på sådana öppna frågeställningar är ”Hur mår du?” och ”Hur är relationen till dina kollegor?”. Om bolaget har behov att dokumentera känsliga personuppgifter i medarbetarsamtalen krävs att bolaget har en rättslig grund för att få hantera dessa uppgifter och att lämpliga tekniska och organisatoriska skyddsåtgärder har vidtagits.

2.3.1 Bedömning

I Älvstranden finns följande medarbetarsamtal som utförs och dokumenteras: kvartsamtal, utvecklingssamtal och prestationssamtal. De dokumenterade medarbetarsamtalen lagras lokalt hos den anställdes chef.

Utifrån intervju med HR-personal så finns det inget behov för bolaget att dokumentera känsliga personuppgifter som exempelvis hälsa i ovannämnda medarbetarsamtal.

Dataskyddsombudet har granskat samtliga samtalsmallar och funnit öppna frågor som skulle kunna innebära risk för att det av misstag nedtecknas känsliga/skyddsvärda personuppgifter. I samtalsmallarna finns en instruktion som stöd för användandet av mallen där det framgår att känsliga personuppgifter inte ska dokumenteras i blanketten.

2.3.2 Slutsats

Dataskyddsombudet bedömer att det i nuläget inte finns någon större risk att känsliga personuppgifter av misstag kommer att dokumenteras utifrån bolagets medarbetarsamtal då tydliga instruktioner finns i samtliga mallar.

2.4 Område 3 Informationsplikt anställda

Dataskyddsförordningen ställer krav på att personuppgiftsansvarig ska informera om de behandlingar som berör den registrerade. Informationen ska bland annat vara lättåtkomlig, lättbegriplig[4] och upplysa den registrerade vart den kan vända sig vid frågor gällande behandlingen eller om den registrerade vill klaga på behandlingen.

2.4.1 Bedömning

Bolaget lämnar information på sitt intranät om hur de anställdas personuppgifter behandlas. Vid nyanställning i bolaget så ingår det i introduktionen att den anställde ska läsa igenom hur bolaget behandlar den anställdes personuppgifter i bolagets personalhandbok på intranätet. Dataskyddsombudet har granskat informationen i dokumentet "Information personal". Dokumentet tar upp de huvudkategorier av personuppgifter som hanteras och vart den anställde kan vända sig vid frågor om behandlingen. Bolaget har även en checklista som används vid nyanställning där en av punkterna är att informera om hur bolaget behandlar de anställdas personuppgifter.

2.4.2 Slutsats

Dataskyddsombudets uppfattning är att bolaget ger en bra allmän information till de anställda om hur deras personuppgifter behandlas. Det är i dokumentet tydligt beskrivet vart den anställde kan vända sig både för frågor och klagomål. Den anställda informeras även när den startar sin anställning om var informationen finns, vilket är en bra åtgärd.

2.5 Område 4 Är personuppgiftsbehandlingarna upptagna i personuppgiftsbehandlingsregistret

Den personuppgiftsansvarige är skyldig att föra register (personbehandlingsregister) över de behandlingar bolaget utför[5].

[4] Skäl 39 dataskyddsförordningen
[5] Artikel 10 dataskyddsförordningen

2.5.1 Bedömning/Slutsats

Dataskyddsombudet har kontrollerat om behandlingarna "Hantera utvecklings- och lönesamtal " och " Hantera Anställning " är upptagna i personuppgiftsbehandlingsregistret. Bägge behandlingarna finns nedtecknade i registret.

2.6 Område 5 Sker kontrollåtgärder gentemot anställda och är de i linje med dataskyddsförordningen

Om arbetsgivaren vill göra systematiska kontroller av de anställda krävs rättslig grund, att kontrollen är proportionerligt utifrån syftet, samt att de anställda är informerad innan kontrollen sker. Den anställde har dock rätt till skydd för sin kommunikation och sitt privatliv. Detta gäller även om den anställde använder sig av bolagets egendom i form av arbetsdator/mobiltelefon för privat kommunikation eller som lagring av privata filer[6]. Det är bara vid allvarlig misstanke om illojalt eller brottsligt beteende som det kan vara tillåtet för arbetsgivaren att ta del av själva innehållet i de anställdas privata filer eller e-postmeddelanden.

2.6.1 Bedömning

Dataskyddsombudet har granskat dokumenten: "Anvisning för IT-användning, "Anvisning mobiltelefon_surfplatta_bärbar dator"," Avtal innehav mobiltelefon surfplatta bärbar dator". I de granskade dokumenten framgår inget om att utrustningen inte får användas privat eller att några kontrollåtgärder sker. Utifrån de intervjuer som genomförts har det inte framkommit något som pekar på att kontrollåtgärder utförs gentemot de anställda. Det enda tillfället som arbetsgivaren går in i den anställdes e-post är vid utlämnande av allmän handling Det sker endast om den anställde inte är tillgänglig för att ta fram efterfrågade handlingar. Enligt bolagets representanter så ges den informationen till samtliga anställda.

2.6.2 Slutsats

Dataskyddsombudet har utifrån dokumentgranskningen och intervjuer inte hittat något som antyder att bolaget utför kontrollåtgärder förutom vid eventuell misstanke om allvarlig illojalitet eller brottslig verksamhet. I nuläget finns inget som gör att dataskyddsombudet har skäl till att utföra djupare kontroll/granskning i frågan.

[6]Artikel 8 Europakonventionen för mänskliga rättigheter -"...var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens" Se även rättsfall (61496/08) BĂRBULESCU v. ROMANIA (https://hudoc.echr.coe.int/eng#{"itemid":["001-177082"]}

3 Sammanfattning

Baserat på genomförd granskning så har dataskyddsombudet identifierat ett förbättringsområde och det gäller de avtal som finns mellan bolaget och personuppgiftsbiträdet (Framtidens IT) avseende driften av personalsystemen från Hogia. Det saknas koppling i avtalen både till de behandlingar som sker och informationsbärare. I och med att bolaget ska byta till ny driftsleverantör så är det lämpligt att dessa otydligheter klargörs i de avtal som tecknas med det nya personuppgiftsbiträdet och att avtalshandlingarna möjliggör att det är lätt att uppdatera eventuella framtida förändringar av personuppgiftsbehandlingarna som kan kommer att ske.

Utifrån effektivitetsskäl kan det vara en lämplig åtgärd att bolaget lyfter frågan till Göteborgs Stadshus AB, via Higab, om de kan ta fram avtalsmallar gällande tjänsteavtal. Avtal av denna typ är ofta komplexa och i bolaget (och de flesta andra bolag i Göteborgs Stad) är det en sällanuppgift att skriva den här typen av avtal. Avtalsmallar skulle kunna minska kostnaderna för bolaget men även för andra bolag i Göteborgs Stad då det oftast krävs ganska omfattande extern juridisk rådgivning.

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