

Informationsärende – Avstämningsrapport dataskyddsarbetet på Älvstranden Utveckling

Sammanfattning

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 förbättringsarbete 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.

Dataskyddsenheten på Intraservice har i samarbete med Stadsrevisionen stämt av dataskyddsarbetet med oss på Älvstranden Utveckling. Avstämningen ska rapporteras till styrelsen.

Bakgrund

Avstämningen har utförts med hjälp av ett förfrågningsunderlag. Underlaget presenterades för dataskyddskontakterna (Patrik Lindberg och Emma Einarsson), chefen för verksamhetsstöd (Ninni Tossavainen) och IT-ansvarig (Glenn Johansson) vid möte med dataskyddsombudet (Martin Brunhage) 10 september 2018.

Sammanfattande bedömning

Ett bra dataskyddsarbete kännetecknas av ständig förbättring vilket är en viktig delkomponent för att uppnå följsamhet mot dataskyddsförordningen.

Dataskyddsombudets uppfattning är att bolagets arbete med dataskyddsfrågor är både ambitiöst och väl genomtänkt.

Dataskyddsombudet uppfattar bemanningen på Älvstranden Utvecklings dataskyddsorganisation som ambitiös och välbalanserad utifrån bolagets verksamhet. Dataskyddsombudet bedömer att vi bör ha goda förutsättningar att i dataskyddsorganisationen hantera följsamhetsfrågor kring dataskyddsförordningen på ett effektivt sätt.

Att frågor gällande efterlevnaden av dataskyddsförordningen kommer att ingå i bolagets kvalitetsledning och process för internkontroll uppfattar dataskyddsombudet som positivt. Att låta dataskyddsfrågor ingå i bolagets kvalitetsledningssystem och process för internkontroller är ett bra sätt för bolaget att visa på följsamhet utifrån dataskyddsförordningens krav.

Att frågor gällande efterlevnaden av dataskyddsförordningen kommer att ingå i bolagets kvalitetsledning kan möjliggöra att bolaget kan hantera avvikelser i personuppgiftsbehandlingar snabbare och mer systematiskt vilket i sin tur kan minska/mildra effekterna av eventuell uppkommen avvikelse.

Avslutningsvis har dataskyddsombudet uppfattningen att dataskyddskontaktarna ger dataskyddsombudet goda förutsättningar och ett bra stöd i att utföra sitt arbete i bolaget.

Bilagor

Bilaga 1. Organisatoriska förutsättningar för dataskyddsarbete – Avstämningsrapport för Älvstranden Utveckling



Organisatoriska förutsättningar för dataskyddsarbete

**Avstämningsrapport för Älvstranden Utveckling
AB**

2018-12-20

Innehåll

1	Inledning	3
1.1	Bakgrund	3
1.2	Utgångspunkter.....	3
1.3	Metodbeskrivning (Tillvägagångssätt för avstämningen)	3
2	Avstämning	4
2.1	Organisation för dataskydd	4
2.1.1	Ansvar och mandat (f 1-2).....	4
2.1.2	Sammansättning och ledning (f 3-4).....	4
2.1.3	Arbetsprocesser (f 5-6)	5
2.1.4	Effektivitetsaspekter (f 7-8).....	5
2.1.5	Återrapportering och uppföljning (f 9-10)	6
2.2	Övriga frågor	6
2.2.1	Informationsåtgärder (f 11-12).....	7
3	Sammanfattande bedömning	8
4	Bilaga avstämningsunderlag	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. 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 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 bland annat beaktande av 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 (Tillvägagångssätt för avstämningen)

Avstämningen har utförts med hjälp av ett förfrågningsunderlag, fortsättningsvis benämnd avstämningsunderlag, innehållande ett antal på förhand specificerade frågor. Avstämningsunderlaget presenterades för dataskyddskontakterna (Patrik Lindberg och Emma Einarsson), chefen för verksamhetsstöd (Ninni Tossavainen) och IT-ansvarig (Glenn Johansson) vid möte med dataskyddsombudet (Martin Brunhage) 10 september 2018.

Dataskyddsombudet gick igenom frågorna på mötet med dataskyddskontakten

och antecknade dataskyddskontaktens svar. Dataskyddskontakten fick därefter avstämningsunderlaget med dataskyddsombudets antecknade svar för granskning och kontroll. Dataskyddskontakten har varit fri att formulera sina svar och göra kompletteringar efter eget gottfinnande. Bolagets svar inkom den 4 oktober 2018 och återfinns under punkt 4 (Bilaga avstämningsunderlag). Utifrån avstämningsunderlaget skapade dataskyddsombudet ett första utkast till denna avstämningsrapport som dataskyddskontakten fått lämna synpunkter på. Eventuella synpunkter från dataskyddskontaktarna har beaktats i denna rapport.

I de fall där dataskyddsombudet lämnar synpunkter och/eller andra kommentarer i avstämningsrapporten görs detta endast på basis av vad som framkommit i det skriftliga avstämningsunderlaget och vid kontakt med dataskyddskontaktarna.

Vid varje delområde i avstämningsrapporten finns en referens till vilka frågor(f) i avstämningsunderlaget (se Bilaga avstämningsunderlag) som ingår i delområdet.

2 Avstämmning

2.1 Organisation för dataskydd

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

2.1.1 Ansvar och mandat (f 1-2)

2.1.1.1 Resultat

Personuppgiftsbehandlingar ansvarar arkivorganisation för. Ansvariga för att ”underhålla” personuppgiftsbehandlingarna är arkivredogörarna. Ansvarig för arkivorganisationen är dokumentcontrollern som även är dataskyddskontakt. Det strategiska arbetet är delegerat från styrelsen.

2.1.1.2 Kommentar

Dataskyddsombudets uppfattning är att dataskyddsorganisationen i bolaget har ett tydligt delegerat mandat och ansvar.

2.1.2 Sammansättning och ledning (f 3-4)

2.1.2.1 Resultat

Dataskyddsorganisationen är grupperad utifrån process och var man verkar i organisationen.

Bemanningen motiveras med hänsyn till organisatoriska fördelar och särskilda kompetenser. Fokus är att få en samlad hantering av behandlingar både utifrån dataskyddsförordningen och arkivhantering.

2.1.2.2 Kommentarer

Dataskyddsombudet uppfattar bemanningen i bolagets dataskyddsorganisationen som ambitiös och välbalanserad utifrån bolagets verksamhet. Dataskyddsombudets bedömning är att bolaget bör ha goda förutsättningar att i dataskyddsorganisationen hantera följsamhetsfrågor avseende dataskyddsförordningen på ett effektivt sätt.

2.1.3 Arbetsprocesser (f 5-6)

2.1.3.1 Resultat

Avstämningsmöten enligt arkivorganisationens arbetssätt. Andra delar planeras att tas med utifrån it-/informationssäkerhet (dataskyddsredogörande). Registeruppdatering planerad att ske minst en gång per år.

Dataskyddsarbetet är inplanerat, ej genomfört ännu, att kopplas till bolagets kvalitetsledning och process för internkontroll.

2.1.3.2 Kommentarer

Att frågor gällande efterlevnaden av dataskyddsförordningen kommer att ingå i bolagets kvalitetsledning och process för internkontroll uppfattar dataskyddsombudet som positivt. Internkontroll är ett bra sätt att systematiskt följa upp regelefterlevnad vilket är en del av att uppvisa följsamhet utifrån dataskyddsförordningens krav. Att frågor gällande efterlevnaden av dataskyddsförordningen kommer att ingå i bolagets kvalitetsledning kan möjliggöra att bolaget hantera avvikelser i personuppgiftsbehandlingar snabbare och mer systematiskt vilket i sin tur kan minska/mildra effekterna av en eventuell uppkommen avvikelse.

2.1.4 Effektivitetsaspekter (f 7-8)

2.1.4.1 Resultat

Uppdragsformen har starkt mandat i alla berörda processer som hanterar personuppgifter. Löpande personalinformation till anställda. Ansvariga för dataskyddsarbetet har även använt ledningsgruppen och fått resurser från vd. Informationsmaterial har tagits fram och presenterats på olika arbetsplatsträffar och på begäran. Arkivorganisationen (arkivredogörare) och systemägare har fått special-information.

Utbildning för samtliga anställda på gång/planeras.

Arkivredogörare har arbetsuppgifterna inskrivna i befattningsbeskrivningen, och den är förankrat i chefsgruppen, vilket är den ledningsfunktion som är resursägare i bolaget. Vid ökat behov av tid så bokas samtal in med chef för resursmängd. Dataskyddskontakter upplever att de hinner med dataskyddsarbetet i nuläget och ser inga problem med att få resursförstärkning vid behov.

2.1.4.2 Kommentar

Avgörande för ett effektivt dataskyddsarbete är bland annat att dataskyddsperspektiven når ut till samtliga delar av bolagets verksamhet. Genom att informera på arbetsplatsträffar och ge specifik information utifrån arbetsuppgifter finns det goda möjligheter att nå bolagets samtliga anställda vilket möjliggör att de anställda får kunskap i hur de ska hantera dataskyddsfrågor på ett lämpligt sätt.

En annan effektivitetsaspekt skulle vara att medlemmarna i dataskyddsorganisationen ges faktiska tidsresurser för att agera på ett verkningsfullt sätt vilket inte är tydligt om så är fallet i dagsläget. Även om tiden för dataskyddskontaktens dataskyddsarbete inte skulle vara särskilt reglerad uppfattar dataskyddsombudet det som att dataskyddskontakterna i nuläget kan få tillgång till extra resurser om det uppstår problem för dataskyddsorganisationen att bedriva dataskyddsarbetet på ett ändamålsenligt sätt.

2.1.5 Aterrapportering och uppföljning (f 9-10)

2.1.5.1 Resultat

Rapportering och hantering av dataskyddsarbetet leds av dataskyddskontakt till chefsgruppen som i sin tur rapporterar och eskalerar vid behov till ledningsgrupp & styrelse.

Avstämningsmöten med dataskyddsombudet är planerade till fyra gånger per år och vid dataskydds-nätverksträffar. Vid behov och vid personuppgiftsincidenter involvera dataskydds-ombud.

2.1.5.2 Kommentar

Dataskyddsombudets uppfattning är att bolaget genom dataskyddskontakterna 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 (f 11-12)

2.2.1.1 Resultat

Bolaget har tagit fram riktat informationsmaterial utifrån kategorier av registrerade med hjälp av advokatbyrå. Bolaget har lagt ut på hemsidan grundläggande information till de registrerade med bland annat kontaktuppgifter till dataskydds-ombudet enligt tilldelningsbeslut.

Bolaget förmedlar information till de registrerade via sin hemsida (<http://alvstranden.com/om-oss/personuppgiftbehandling/>).

De målgrupper av registrerade som når Älvstranden via vår hemsida kommer vi publicera per målgrupp anpassad information på hemsidan.

Avtalsparter som tex hyresgäster, leverantörer mm informeras både i avtalstexter och på hemsidan.

Bolagets personal informeras enligt rutiner för intern kommunikation.

Leverantörer som lämnar anbud till Älvstranden informeras tidigt i upphandlings-processen.

Besökare till Älvstrandens platsskapande aktiviteter informeras vid bokning av besök samt via hemsidan.

2.2.1.2 Kommentar

Dataskyddsombudet bedömer att det finns goda förutsättningar för den registrerade att få information om bolagets behandling av personuppgifter. Informationen till de registrerade är uppdelad utifrån målgrupp på ett föredömligt sätt.

Dataskyddsombudet har i denna avstämning inte granskat om informationen uppnår en tillräcklig grad av transparens eller tillgänglighet utifrån dataskyddsförordningen krav.

2.2.1.3 Resultat

Anmälan av dataskyddsombud har gjorts till Datainspektionen.

2.2.1.4 Kommentar

Dataskyddsombudet har fått bekräftelse att registrering har utförts från Datainspektionen.

3 Sammanfattande bedömning

Ett bra dataskyddsarbete kännetecknas av ständig förbättring vilket är en viktig delkomponent för att uppnå följsamhet mot dataskyddsförordningen.

Dataskyddsombudets uppfattning utifrån de möten som ägt rum med dataskyddskontakten samt granskat avstämningsunderlag är att bolagets arbete med dataskyddsfrågor är både ambitiöst och väl genomtänkt.

Dataskyddsombudet uppfattar bemanningen i bolagets dataskyddsorganisationen som ambitiös och välbalanserad utifrån bolagets verksamhet. Dataskyddsombudet bedömning är att bolaget bör ha goda förutsättningar att i dataskyddsorganisationen hantera följsamhetsfrågor avseende dataskyddsförordningen på ett effektivt sätt.

Att frågor gällande efterlevnaden av dataskyddsförordningen kommer att ingå i bolagets kvalitetsledning och process för internkontroll uppfattar dataskyddsombudet som positivt. Att låta dataskyddsfrågor ingå i bolagets kvalitetsledningssystem och process för internkontroller är ett bra sätt för bolaget att visa på följsamhet utifrån dataskyddsförordningens krav.

Att frågor gällande efterlevnaden av dataskyddsförordningen kommer att ingå i bolagets kvalitetsledning kan möjliggöra att bolaget kan hantera avvikelser i personuppgiftsbehandlingar snabbare och mer systematiskt vilket i sin tur kan minska/mildra effekterna av eventuell uppkommen avvikelse.

Avslutningsvis har dataskyddsombudet uppfattningen att dataskyddskontakterna ger dataskyddsombudet goda förutsättningar och ett bra stöd i att utföra sitt arbete i bolaget.

Göteborg 2018-12-20


Martin Brunhage

Dataskyddsombud

4 Bilaga avstämningsunderlag

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.

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?
<i>Ja</i>
2. Hur är organisationens ansvar och mandat utformat?
<i>Personuppgiftsbehandlingar ansvarar arkivorganisation för. Ansvariga för att "underhålla" personuppgiftsbehandlingarna är arkivredogörarna. Ansvarig för arkivorganisationen är dokumentcontrollern som även är dataskyddskontakt. Det strategiska arbetet är delegerat från styrelsen.</i>
3. Hur är organisationen sammansatt? (en person, en gruppering, m.m.)
<i>Gruppering utifrån process och var man verkar i organisationen.</i>
4. Vad har motiverat den sammansättningen? (särskilda kompetenser, organisatoriska fördelar m.m.)
<i>Organisatoriska fördelar och särskilda kompetenser. Fokus är att få en samlad hantering av behandlingar både utifrån Dataskyddsförordningen och arkivhantering.</i>
5. Vem har den sammankallande/ledande rollen i organisationen?
<i>Dataskyddskontakt är sammankallande</i>
6. Beskriv i korthet hur arbetet planeras att bedrivas. (Planer, mötesfrekvens, m.m.)

Avstämningsmöten enligt arkivorganisationen arbetssätt. Andra delar planeras att tas med utifrån it-/informationssäkerhet (dataskyddsredogörande). Register-uppdatering planerad att ske minst en gång per år.

Dataskyddsarbetet är inplanerat, ej genomfört ännu, att kopplas till bolagets kvalitetsledning och process för internkontroll.

7. Hur säkerställs att organisationens arbete förankras med och når ut till alla delar i verksamheten?

Uppdragsformen har starkt mandat i alla berörda processer som hanterar personuppgifter. Löpande personalinformation till anställda. Ansvariga för dataskyddsarbetet har även använt ledningsgruppen och fått resurser från vd. Informationsmaterial har tagits fram och presenterats på olika apt:er och på begäran. Arkivorganisationen (arkivredogörare) och systemägare har fått specialinformation.

Utbildning för samtliga anställda på gång/planeras.

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?

Arkivredogörare har arbetsuppgifterna inskrivna i befattningsbeskrivningen, och den är förankrat i chefsgruppen, vilket är den ledningsfunktion som är resursägare i bolaget. Vid ökat behov av tid så bokas samtal in med chef för resursmängd. Dataskyddskontakter upplever att de hinner med dataskyddsarbetet i nuläget och ser inga problem med att få resursförstärkning vid behov.

9. Hur säkerställer ni att förvaltningsledningen hålls uppdaterad om arbetet?

Rapportering och hantering av dataskyddsarbetet leds av dataskyddskontakt till chefsgruppen som i sin tur rapporterar och eskalerar vid behov till ledningsgrupp & styrelse.

10. Hur planerar ni att hålla dataskyddsombudet informerat och involverat i organisationens löpande arbete?

*Planerade möten med dataskyddsombud kvartalsvis. Vid dataskydds-
nätverksträffar. Vid behov och vid personuppgiftsincidenter involvera dataskydds-
ombud.*

Övriga frågor

11. Vilka åtgärder har vidtagits för att informera de registrerade om behandlingen av deras personuppgifter? ("integritetspolicy", andra informationstexter, m.m.)

Bolaget har tagit fram riktat informationsmaterial utifrån kategorier av registrerade med hjälp av advokatbyrå. Bolaget har lagt ut på hemsidan grundläggande information till de registrerade med bland annat kontaktuppgifter till dataskyddsombudet enligt tilldelningsbeslut.

12. Hur tillhandahåller ni informationen till de registrerade? (publicering på hemsida, m.m.)

De målgrupper av registrerade som når Älvstranden via vår hemsida kommer vi publicera per målgrupp anpassad information på hemsidan.

Avtalsparter som tex hyresgäster, leverantörer mm informeras både i avtalstexter och på hemsidan.

Bolagets personal informeras enligt rutiner för intern kommunikation.

Leverantörer som lämnar anbud till Älvstranden informeras tidigt i upphandlingsprocessen.

Besökare till Älvstrandens platsskapande aktiviteter informeras vid bokning av besök samt via hemsidan.

Se fråga 11

Dataskyddsbud

Har ni anmält vem som är ert dataskyddsbud till Datainspektionen?

Ja
Anmälan registrerad hos Datainspektionen. DSO har verifierat.

Nej