Göteborgs Stad

Organisatoriska förutsättningar för dataskyddsarbete

Avstämningsrapport för Göteborg & Co AB

2018-12-10

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) 6
3 Sammanfattande bedömning 7
Bilaga avstämningsunderlag 8

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 personuppgifts-ansvarig 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 personuppgifts-ansvarige 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 dataskyddskontakten (Anders Fahl) vid möte med dataskyddsombudet (Martin Brunhage) 24 oktober 2018. Dataskyddsombudet gick igenom frågorna på mötet med dataskyddskontakterna och antecknade dataskyddskontakternas svar. Dataskyddskontakten (Anders Fahl) 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 29 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 dataskyddskontakten 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 dataskyddskontakten.

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

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 bedömning.

2.1.1 Ansvar och mandat (f 1-2)

2.1.1.1 Resultat

Dataskyddskontakterna har nära dialog med ledningsgruppen. Dataskyddskontakterna uppfattar inte att de har problem med att få fokus på dataskyddsfrågorna. Bolaget har för avsikt att komplettera bolagets interna IT-anvisning med dataskyddskontaktens ansvar och mandat.

2.1.1.2 Kommentar

Att dataskyddskontakterna har nära dialog med ledningsgruppen ser dataskyddsombudet som positivt då detta är ett tecken på att dataskyddsfrågor prioriteras i bolaget.

2.1.2 Sammansättning och ledning (f 3-4)

2.1.2.1 Resultat

Dataskyddsgruppen består av två dataskyddskontakter.

Sammansättning utifrån behov, särskilda kompetenser och erfarenheter samt utifrån organisationens storlek och komplexibilitet.

2.1.2.2 Kommentar

Utifrån den relativt begränsade mängden personuppgiftsbehandlingar som utförs i bolaget, både vad det gäller harmlösa och känsliga personuppgifter, bedömer dataskyddsombudet att bolaget bör ha goda möjligheter att i dataskyddsorganisationen hantera följsamhetsfrågor avseende dataskyddsförordningen på ett effektivt sätt.

2.1.3 Arbetsprocesser (f 5-6)

2.1.3.1 Resultat

Huvuddataskyddskontakten sammankallar/leder dataskyddsorganisationen. Det fortlöpande arbetet främst vid behov samt löpande arbete. Planer finns på att dataskyddskyddsorganisationen ska lyfta frågor/rapporter gällande dataskyddsarbetet till styrelsen med viss intervall. Arbetet sker fortlöpande i den dagliga verksamheten.

2.1.3.2 Kommentar

Dataskyddsombudets uppfattning är att det utifrån dataskyddskontakternas ordinarie arbetsuppgifter finns en naturlig koppling till dataskyddsarbete.

I dataskyddsarbete är kontinuitet viktigt för att dataskyddsfrågor inte ska riskera att hamna i skymundan utifrån övrig verksamhet i bolaget. Dataskyddsombudet rekommenderar att bolaget tar fram en arbetsinstruktion för dataskyddsorganisationen och att dataskyddsorganisationen har planerade möten.

2.1.4 Effektivitetsaspekter (f 7-8)

2.1.4.1 Resultat

Avstämningsmötet per avdelning. Information till nyanställda, Intranät. Förhoppning om en kommungemensam tjänst som tillhandahåller nanoutbildningar inom området.

Prioritering efter behov. Storleken på bolaget samt dess behov gör att det går att lösa dataskyddsarbetet även med "ordinarie" arbetsuppgifter.

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 avstämningsmöten i verksamheten, på bolagets intranät och specifikt till nyanställda 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 dataskyddskontakterna ges faktiska tidsresurser för att agera på ett verkningsfullt. Även om tiden för dataskyddskontaktens dataskyddsarbete inte är särskilt reglerad uppfattar dataskyddsombudet det som att dataskyddskontakten i nuläget kan få tillgång till extra resurser om det uppstår problem för dataskyddskontakterna att bedriva dataskyddsarbetet på ett ändamålsenligt sätt.

2.1.5 Återrapportering och uppföljning (f 9-10)

2.1.5.1 Resultat

Frågor lyfts med ledningsgruppen vid behov.

Avstämningsmöten med dataskyddsombudet är planerade till fyra gånger per år och utifrån behov vid konsekvensbedömning och personuppgiftsincidenter.

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 förmedlar information till de registrerade via sin hemsida (http://goteborgco.se/hur-behandlar-vi-dina-personuppgifter) samt information via mejl vid behov.

Samtyckesmail till respektive registrerad i bolagets kontaktregister. Informationstexter i samband med avtal. Vid olika typer av förfrågningar och intresseanmälningar. Framgår mer detaljerat i bolagets inventering samt åtgärdsplan följsamhet mot Dataskyddsförordningen. När det gäller nyanställningar så kommer information ges tillsammans med anställningsavtalet. Bolaget kommer troligtvis att informera de anställda som inte har fått information tillsammans med sitt anställningsavtal genom och gruppmail och information till samtlig personal på intranätet.

2.2.1.2 Kommentar

Dataskyddsombudet bedömer att det finns goda förutsättningar för den "externt" registrerade att få information om bolagets behandling av personuppgifter.

Det framgår av avstämningsunderlaget att bolaget arbetar med att ta fram ytterligare information till de anställda om hur deras personuppgifter behandlas. Att de anställda informeras om hur deras personuppgifter behandlas i bolaget är viktigt för att bolaget ska uppfylla sin informationsplikt utifrån dataskydds-förordningens krav.

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 bolaget arbetar aktivt och genomtänkt med dataskyddsfrågor.

Det framgår av avstämningsunderlaget att bolaget arbetar med att ta fram ytterligare information till de anställda om hur deras personuppgifter behandlas. Att de anställda informeras om hur deras personuppgifter behandlas i bolaget är viktigt för att bolaget ska uppfylla sin informationsplikt utifrån dataskyddsförordningens krav.

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

Göteborg 2018-12-10

Martin Brunhage

Dataskyddsombud

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?
Ja
2. Hur är organisationens ansvar och mandat utformat?
Dataskyddskontakterna har nära dialog med ledningsgruppen. Dataskydds-kontakterna uppfattar inte att de har problem med att få fokus på dataskydds-frågorna. Bolaget har för avsikt att komplettera bolagets interna IT-anvisning med dataskyddskontaktens ansvar och mandat. (Svaret är uppdaterat av dataskydds-ombudet efter mejlkontakt med dataskyddskontakten 20181205)
3. Hur är organisationen sammansatt? (en person, en gruppering, m.m.)
Två stycken dataskyddskontakter varav en av dessa eventuellt kommer att bytas ut. (Svaret är uppdaterat av dataskyddsombudet efter mejlkontakt med dataskyddskontakten 20181205)
4. Vad har motiverat den sammansättningen? (särskilda kompetenser, organisatoriska fördelar m.m.)
Utifrån behov, särskilda kompetenser och erfarenheter samt utifrån organisationens storlek och komplexibilitet.
5. Vem har den sammankallande/ledande rollen i organisationen?
Dataskyddskontakten

6. Beskriv i korthet hur arbetet planeras att bedrivas. (Planer, mötesfrekvens, m.m.)
Främst vid behov samt löpande arbete. Planer finns på att dataskyddskydds-organisationen ska lyfta frågor/rapporter gällande dataskyddsarbetet till styrelsen med viss intervall.
7. Hur säkerställs att organisationens arbete förankras med och når ut till alla delar i verksamheten?
Avstämningsmötet per avdelning. Information till nyanställda, Intranät. Förhoppning om en kommungemensam tjänst som tillhandahåller nanoutbildningar inom områ-det.
8. Om organisationen bemannas av personal som därtill har ordinarie arbets-uppgifter, hur säkerställs att dessa ges tillräckligt med tid för att dataskydds-arbetet kan bedrivas ändamålsenligt?
Prioritering efter behov. Storleken på bolaget samt dess behov gör att det går att lösa dataskyddsarbetet även med "ordinarie" arbetsuppgifter.
9. Hur säkerställer ni att förvaltningsledningen hålls uppdaterad om arbetet?
Frågor lyfts med ledningsgruppen vid behov.
10. Hur planerar ni att hålla dataskyddsombudet informerat och involverat i organisationens löpande arbete?

Varje kvartal och vid behov. Vid personuppgiftsincident och konsekvens-bedömningar.

Övriga frågor

11. Vilka åtgärder har vidtagits för att informera de registrerade om behandlingen av deras personuppgifter? ("integritetspolicy", andra informationstexter, m.m.)
Samtyckesmail till respektive registrerad i bolagets kontaktregister. Informations-texter i samband med avtal. Vid olika typer av förfrågningar och intresse-anmälningar. Framgår mer detaljerat i bolagets inventering samt åtgärdsplan följsamhet mot Dataskyddsförordningen. När det gäller nyanställningar så är de nya kontrakten uppdaterade med information. Men vi funderar på hur vi på ett bra sätt informerar alla som varit anställda en tid många i över 10 år. Vi kommer troligtvis göra det genom och gruppmail till samtlig personal och information på intranätet. (Svaret är uppdaterat av dataskyddsombudet efter mejl-kontakt med dataskyddskontakten 20181205)
12. Hur tillhandahåller ni informationen till de registrerade? (publicering på hem-sida, m.m.)
Information på hemsidan http://goteborgco.se/hur-behandlar-vi-dina-personuppgifter/ Samt information mailleds vid behov. Se svaret på fråga 11.
Dataskyddsombud

Har ni anmält vem som är ert dataskyddsombud till Data-inspektionen?	Ja **Anmält och verifierat av DSO**	Nej