Handläggare: Camilla Nyman
Tel: 031-368 40 11
E-post: camilla.nyman@goteborg.com

Göteborg & Co:s införande av dataskyddsförordningen

Styrelsen föreslås besluta

1) Att anteckna informationen.

Sammanfattning

25 maj 2018 ersätter dataskyddsförordningen dagens personuppgiftslag (1998:204). Den nya lagen ställer högre krav på hur myndigheter och företag hanterar personuppgifter i sina verksamheter. Föreliggande ärende beskriver hur Göteborg & Co har arbetat med införandet av dataskyddsförordningen i bolaget samt vilka konsekvenser lagen har för verksamheten.

Ekonomiska konsekvenser

Göteborg & Co:s årliga kostnad för dataskyddsombud uppgår till 140 056 kronor.

Olika Perspektiv

Barnperspektivet

Ett av syftena med dataskyddsförordningen är att skydda enskildas grundläggande rättigheter och friheter, särskilt när det gäller rätt till skydd av personuppgifter. Rätten till privatliv uttrycks i den Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR). Barn anses vara särskilt skyddsvärda i detta avseende.

Jämställdhetsperspektivet

Göteborg & Co har inte funnit några särskilda aspekter utifrån detta perspektiv.

Mångfaldsperspektivet

Göteborg & Co har inte funnit några särskilda aspekter utifrån detta perspektiv.

Miljöperspektivet

Göteborg & Co har inte funnit några särskilda aspekter utifrån detta perspektiv.

Omvärldsperspektivet

Dataskyddsförordningen skapar en enhetlig och likvärdig nivå för skyddet av personuppgifter inom EU så att det fria flödet av uppgifter inom unionen inte hindras. Detta uppnås genom att

förordningen är direkt tillämplig i de olika medlemsstaterna och att samma regler gäller inom hela unionen från och med 25 maj 2018.

Ärendet

Bakgrund

I april 2016 beslutade EU om att införa ett regelverk kring hantering av personuppgifter som blir direkt tillämpligt i samtliga medlemsstater 25 maj 2018. Regelverket, kallat dataskyddsförordningen, ersätter dagens personuppgiftslag (1998:204) och har som huvudsakligt syfte att stärka det personliga integritetsskyddet för människor och på så vis skydda människors grundläggande rättigheter och friheter. Ambitionen är att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter inom EU så att det fria flödet av uppgifter inom unionen inte hindras. Stora delar av lagen har även att göra med de krav som det nya digitala samhället ställer på myndigheter, företag och organisationer i form av en större digital marknad och ett större flöde av personuppgifter.

Dataskyddsförordningens regelverk innebär krav på anpassning från myndigheter och företag för att säkerställa att organisationerna lever upp till de nya bestämmelserna.

Respektive förvaltning och bolag i Göteborgs Stad är ansvariga för att nå följsamhet gentemot dataskyddsförordningen senast 25 maj 2018. För att koordinera och underlätta införandet i staden skapades under 2017 en projektorganisation i Stadsledningskontorets regi.

Föreliggande tjänsteutlåtande beskriver bl.a. arbetsprocessen för införandet av dataskyddsförordningen i Göteborg & Co, de förändringar som föreligger i samband med detta samt ansvarsfördelningen inom bolaget.

Införandet av dataskyddsförordningen i Göteborg & Co

Bolaget har drivit sitt arbete i projektform med en liten arbetsgrupp och haft en styrgrupp bestående av Administrativ chef, AO-chef möten, Chef HR och IT-chef.

Styrgruppen fastställde 2017-06-05 en handlingsplan för införande av dataskyddsförordningen som avrapporterats till Stadsledningskontorets projektorganisation. Handlingsplanen definierar bland annat projektets förväntade resultat, omfattning och avgränsning, tidsram och aktivitetsplan, eventuella kostnader, organisering och kommunikationsinsatser. Avstämningar mot Stadsledningskontoret har skett regelbundet under tiden för införandet.

Från projektet avgränsades:

- Aktiviteter som syftar till att säkra kommungemensamma tjänster ur ett utvecklings-, drifts- och säkerhetsperspektiv. Detta förutsätts hanteras centralt inom staden.
- Det ingår i projektet att kravställa följsamhet mot DSF hos externa leverantörer av systemutveckling och driftstjänster men inte att i egen regi genomföra dessa åtgärder.

I ett tidigt skede beslöt klustret att samverka i införandeprocessen. Bolagen har haft en gemensam grundstruktur för sitt arbete och gjort gemensamma grundläggande tolkningar av

den praktiska tillämpningen av dataskyddsförordningen. Ett externt stöd i arbetet mot följsamhet mot dataskyddsförordningen. Under tiden för införandeprojektet har ett antal klustergemensamma arbetsmöten genomförts tillsammans med en konsult inom området informationssäkerhet i syfte att dela erfarenheter och få stöd i processen. Varje bolag har genomfört ett eget förberedelsearbete utifrån vart bolags förutsättningar.

Inom ramen för införandeprojektet genomförde Göteborg & Co en informationskartläggning av personuppgifter i verksamheten med tillhörande informationsklassning. Utifrån resultatet från informationskartläggningen och klassningen kan slutsats dras att bolaget i sina verksamheter hanterar relativt få personuppgifter och i mycket sällan förekommande fall känsliga sådana, så kallade klass 2-uppgifter.

Utifrån kartläggningen skapades en riskanalys och åtgärdsplan bestående av sammanlagt 32 punkter upprättats. Av de 32 åtgärderna har de mest angelägna varit att slutföra inventeringen av ostrukturerad data i bolagets verksamheter, utveckla rutiner för gallring i verksamhetssystemet Compis samt införa och skapa en process för att vidmakthålla löpande hantering av personuppgiftsincidenter och datasäkerhetsrisker. Majoriteten av de åtgärdspunkter som identifierats har varit av mindre vikt och har krävt ringa insatser att ombesörja.

Av samtliga 32 insatser i åtgärdsplanen är 29 stycken antingen pågående eller genomförda. De kvarvarande delar som ännu inte ombesörjts beräknas vara åtgärdade innan dataskyddsförordningens inträde 25 maj 2018.

Hantering av ostrukturerade data

Hantering av personuppgifter kan ske genom strukturerad eller ostrukturerad behandling. Strukturerad behandling sker när hanteringen av personuppgifterna omfattas av så kallade hanteringsregler, ofta med hjälp av systemstöd. Ostrukturerad behandling är när personuppgifter inte ingår i, eller är avsedda att ingå i, en samling av personuppgifter som har strukturerats för att påtagligt underlätta sökning efter, eller sammanställning av, personuppgifter. Tidigare har ostrukturerad behandling av personuppgifter omfattats av ett enklare regelverk än det som gäller för strukturerad behandling. I och med datasskyddsförordningens nya lagkrav kommer samma regler gälla för ostrukturerade som för strukturerade behandlingar.

I syfte att nå följsamhet har Göteborg & Co utfört en genomlysning av ostrukturerade behandlingar av personuppgifter i hela bolaget. Samtlig personal har fått inventera sin eventuella ostrukturerade data vilken sedan har setts över och hanterats enligt det nya regelverket. Bolaget bedömer att detta ska vara tillräckligt för att tillgodose de nya krav som dataskyddsförordningen ställer.

Dataskyddsombud

För varje personuppgiftsansvarig (juridisk person) ska det enligt lag finnas ett dataskyddsombud. Ombudet är en fysisk person vars roll bl.a. innebär att kontrollera att

dataskyddsförordningen följs inom organisationen, till exempel genom att samla in information om hur organisationen behandlar personuppgifter, kontrollera att organisationen följer bestämmelser och interna styrdokument samt utföra kontroller och informationsinsatser.

Kommunstyrelsen beslutade 2017-08-23 att ge nämnden för Intraservice i uppdrag att nyutveckla en kommungemensam intern tjänst med för att fylla stadens behov av dataskyddsombud. Intraservice har sedan dess inrättat en intern organisation som tillhandahåller dataskyddsombud för stadens bolag och förvaltningar. Information kring Göteborg & Co:s dataskyddsombud väntas inkomma från intraserice inom snar framtid.

Ansvar

Nedan beskrivs ansvarsfördelning kopplad till personuppgiftshantering och dataskyddsförordning på Göteborg & Co.

Styrelsen för Göteborg & Co

Styrelsen är personuppgiftsansvarig för Göteborg & Co. Personuppgiftsansvar innebär det yttersta ansvaret för bestämmelser gällande ändamålen med, och medlen för, behandling av personuppgifter. Ansvaret kan inte delegeras.

IT-chef

IT-chefen är bolagets kontakt gentemot dataskyddsombudet.

Dataskyddsombud

Dataskyddsombudets ansvar innefattar att

- samla in information om hur organisationen behandlar personuppgifter
- kontrollera att organisationen följer bestämmelser och interna styrdokument
- informera och ge råd inom organisationen.
- ge råd om konsekvensbedömningar
- vara kontaktperson för Datainspektionen
- vara kontaktperson för de registrerade och personalen inom organisationen
- samarbeta med Datainspektionen, till exempel vid inspektioner.

En preciserad tjänstebeskrivning för dataskyddsombudets roll väntas inkomma från Intraservice inom kort.

Göteborg & Co kommer se över sina rutiner kring följsamhet mot dataskyddsförordningen tillsammans med dataskyddsombudet efter att denne påbörjat sin tjänst. Rutiner och arbetssätt kan i och med detta komma att justeras.

Personuppgiftsbiträdesavtal

Personuppgiftsbiträde är den person eller det företag som behandlar personuppgifter för den personuppgiftsansvariges räkning. Det kan handla om ett företag som tillhandahåller en tjänst vilken innebär hantering av personuppgifter som ägs av en annan organisation. Vid en sådan överenskommelse är det nödvändigt att ett personuppgiftsbiträdesavtal upprättas, i vilket det anges att biträdet endast får lov att hantera personuppgifter i enlighet med instruktioner från beställaren. Det är alltid den personuppgiftsansvariges skyldighet att se till att ett sådant avtal finns. En genomlysning av Göteborg & Co:s verksamhet visar att erforderliga personuppgiftsbiträdesavtal finns tecknade med parter utanför staden i de fall det krävs. När det gäller personuppgiftsbiträdesavtal för intraservice hantering av kommungemensamma tjänster så arbetar intraservice med att fram ett sådant för Göteborg & Co:s del.

Lokal IT-anvisning för Göteborg & Co

För att skapa en vägledning för, och beskrivning av, hur bolaget ser på IT-relaterade frågor och vilka rutiner som etablerats har Göteborg & Co arbetat fram en lokal IT-anvisning.

I den lokala anvisningen beskrivs bland annat bolagets processer för att IT-och informationssäkerhet samt tillämpningen av dataskyddsförordningen.

Uppföljning

För att säkerställa en fortsatt följsamhet mot dataskyddsförordningen även i framtiden kommer Göteborg & Co att genomföra årligen återkommande riskanalyser och kontroller av incidenthantering, personuppgiftsincidenthantering och användarbehörighet. Även stöddokumentet ”Råd – metodikbeskrivning för säker informationshantering” kommer att användas som stöd för uppföljningsarbetet. Intraservice har tilldelat bolaget ett dataskyddsombud och har aviserat att ytterligare information kring tjänsteanvisning och ansvar meddelas snarast möjligt. Det är sannolikt att dataskyddsombudet kommer kunna bidra med ytterligare anvisningar och kontrollaktiviteter som befintlig anvisning och rutiner får kompletteras med.

Insatserna kan komma att justeras för samordning med eventuella kontrollaktiviteter som genomförs av dataskyddsombudet.

Utöver detta har Göteborg & Co tagit fram ett utbildningsmaterial för nyanställda. Syftet är att ge ny- och projektanställda de kunskaper som krävs för att hantera personuppgifter i enlighet med lagens krav och bolagsspecifika anvisningar.

Expedieras