Kommunfullmäktiges revisorer

Svar på revisorernas granskning av Sundbybergs stads efterlevnad av Dataskyddsförordningen GDPR

Stadens revisorer har i skrivelse till kommunstyrelsen granskat efterlevnaden av Dataskyddsförordningen (GDPR) och har framställt fem rekommendationer på åtgärder för att stärka stadens kontroll över och efterlevnad av dataskyddet.

Kommunstyrelsen bedömer att rapporten inte ska läsas självständigt utan tillsammans med den rapport som stadens revisorer inkom med i juni 2019 avseende stadens arbete med informationssäkerhet.

Eftersom kommunstyrelsen inte själv äger hela ansvaret för samtliga rekommendationer som lämnats har stadsmiljö- och tekniska nämnden medverkat vid utformningen av svaren. Båda nämnderna träffas av rekommendation 2 varför svar lämnas för respektive nämnd i den delen. I övrigt svarar kommunstyrelsen på övriga rekommendationer. Kommunstyrelsen kommer att bistå stadsmiljö- och tekniska nämnden i arbetet i enlighet med rekommendationerna.

Kommunstyrelsen lämnar följande kommentarer som svar på revisionens rekommendationer och övriga bedömningar:

Rekommendation 1: Styrning och styrdokument.
För att säkerställa att Sundbybergs stads alla bolags och verksamheters rutiner beträffande hantering av personuppgifter sker i enlighet med kraven i dataskyddsförordningen bör Sundbybergs stad förtydliga sin informationssäkerhetspolicy. Genom denna kan en strategi och ett förtydligat syfte för dataskyddsarbetet förankras från politisk nivå hela vägen ner i verksamheterna. Policyn hänvisar till riktlinjer och anvisningar för dataskyddsarbetet, men dessa saknas och bör således skapas. De bör täcka in alla relevanta aspekter av dataskyddsförordningen. Sundbybergs stad rekommenderas även implementera en rutin för att följa upp att verksamheterna efterföljer de regler och policys som är fastställda i styrdokumentet.

Kommentar: Kommunstyrelsen instämmer i revisorernas bedömning gällande informationssäkerhetspolicyn. Ett förslag till ny informationssäkerhetspolicy togs fram i februari 2020 av stadsledningskontoret och inväntar nu godkännande för remissbehandling i stadens nämnder och bolag. Konkretisering av policyn i form av riktlinjer, uppdelade i fyra kapitel (A-D) är under utveckling. Kapitel A är helt färdigställt och inväntar stadsledningskontorets godkännande för politisk behandling. Kapitel B och D är nästan färdigställda. Kapitel C är ännu ej påbörjad då stadsledningskontoret inväntar beslut om en ny systemförvaltningsmodell. Varje kapitel ska remitteras ut till samtliga nämnder och bolag för yttrande.

Kommunstyrelsen fastställer därefter, i enlighet med bestämmelsen i dess reglemente om att leda arbetet med informationssäkerhet, dessa riktlinjer för staden. För att riktlinjerna ska kunna verkställas krävs det lokala rutiner och rutiner för uppföljning på central nivå. Nämnderna måste upprätta lokala rutiner utifrån verksamhetskännedom medan kommunstyrelsen tar fram rutiner för central uppföljning. För att kunna följa att egenkontroller genomförs i enlighet med de bestämmelser som framgår av dataskyddsförordningen bedöms det nödvändigt att införa ett verksamhetssystem i vilket nämnderna kan genomföra sina egenkontroller. Ett sådant system sammanställer stadens arbete med dataskyddet och möjliggör för tillsynsmyndigheten att på begäran snabbt, detaljerat och i samlad form ta del av hur staden arbetar med dataskydd och vilken säkerhetsnivå som det arbetet håller.

Rekommendation 2: Organisation och ansvarsfördelning.
Sundbybergs stad bör dokumentera en formell, informationssäkerhetsspecifik organisationsstruktur med tillhörande roller och tydlig ansvarsfördelning för att undvika överarbetsbelastning och personberoende. EY föreslår även att organisationsstrukturen ses över och eventuellt ändras till att bättre passa IT:s centrala roll i stadens verksamheter och de ökade kraven på informationssäkerhet. Dessutom bör staden avsätta resurser specifikt för att utveckla sitt dataskyddsarbete, så att man kan utföra gap-analyser av utvecklingsområden, skapa tillhörande rutiner och processer, och sedan granska efterlevnaden av de processer som implementerats. Sundbybergs stad rekommenderas följaktligen också att fastställa en åtgärdsplan inkluderande tidsplan och ansvarig person för att åtgärda eventuella gap där dataskyddsförordningen inte efterlevs.

Kommentar: Kommunstyrelsen instämmer i revisorernas bedömning. På verksamhetsnivå inleddes det under hösten 2019 en samverkan med utsedda informationssäkerhetsombud under ledning av trygghets- och säkerhetsavdelningen i syfte att skapa medvetande och involvering i stadens informationssäkerhetsarbete. Dessa kommer också att bistå dataskyddsombudet i personuppgiftsärenden tillsammans med stadens systemförvaltare. Målet med åtgärden är att försöka lätta på den arbetsbelastning och det personberoende som revisorerna identifierat. Stadsledningskontoret har tagit fram en arbetsmodell för informationsklassificering som består av fyra steg: Omvärldsanalys, verksamhetsanalys, riskanalys och gapanalys. Dessa analyser bedöms gemensamt möta revisorernas rekommendation att utföra gapanalyser av olika utvecklingsområden. Gapanalyserna kommer också att redovisa tidplaner och ansvar för att åtgärda eventuella gap inom informationssäkerheten. Arbetet förväntas bedrivas under en oöverskådlig tid framåt. En tidsbegränsning av uppdraget bedöms inte lämplig då det rör sig om omfattande informationsmaterial som ska analyseras och kommunstyrelsens bedömning är att det är prioriterat att arbetet görs grundligt.

Kommunstyrelsen konstaterar också att uppdragen som informationssäkerhetssamordnare och dataskyddsombud inte är lämpliga att kombinera. Dataskyddsombudet har till uppgift att genomföra egenkontroll av

verksamheterna för frågor som informationssäkerhetssamordnaren i sitt uppdrag bidrar till att upprätta rutiner och processer inom. Det innebär att dataskyddsombudet inte kan genomföra erforderliga egenkontroller då revisionen i sådana fall också omfattar dataskyddsombudets eget arbete i egenskap av informationssäkerhetssamordnare. Uppdragen är i dagsläget inte tidsfördelade utan ska utföras inom ramen för en heltidstjänst. I praktiken är det dock två tjänster. Som framgår av föreliggande granskning och av den granskning som genomfördes av informationssäkerhetsarbetet under 2019 skulle det behövas två informationssäkerhetsombud på ändamålsenlig omfattning för att möta alla de rekommendationer som stadens revisorer lämnat. I övrigt skulle dataskyddsombudet behöva vara en självständig resurs för att stötta staden i *hela* dataskyddet, särskilt de delarsom idag inte alls berörs, till exempel det risk- och sårbarhetsanalysarbete som krävs för att tillsynsmyndigheten ens ska påbörja handläggning av begäran om förhandsbesked. På sikt, när Sundbyberg stad kan garantera att det finns erforderliga processer och rutiner på plats för att säkra dataskyddet, bör omfattningen av denna tjänst ses över, då personuppgiftsansvaret åligger respektive nämnd, inte dataskyddsombudet. Samtliga nämnder, inklusive kommunstyrelsen, behöver således axla ett större ansvar för personuppgiftsskyddet och det praktiska arbetet som följer av det ansvaret än de i dagsläget gör.

Rekommendation 3: Granskning och rapportering.
Begränsad uppföljning av verksamheternas informationssäkerhetsarbeten medför risk för att nämndernas och förvaltningarnas dagliga informationshantering avviker från sättet som både stadens ansvariga och stadsledningskontoret anvisar och tror att arbetet bedrivs på. Staden rekommenderas därför att implementera en granskningsplan för att utvärdera och säkerhetsställa att man uppfyller relevanta krav på hantering av personlig information samt en formell rutin för att dokumentera och rapportera resultat till ledningsnivå. Kontroller av stadens dataskyddsarbete kan exempelvis integreras i stadens och dess nämnders internkontrollarbete. Staden rekommenderas även att fastställa ett rapporteringskrav gällande frekvens och innehåll som rapporteringen till kommunstyrelse ska utgå från för att säkerställa att uppföljning av dataskyddsförordningen utförs och kommuniceras till ledningen.

Kommentar: Kommunstyrelsen instämmer i revisorernas bedömning. Varje nämnd har var för sig utsett dataskyddsombudet och enligt förordningen ska dataskyddsombudet regelbundet beredas tillgång till ledningen. En sådan tillgång i förordningens mening tar inte enbart sikte på tjänstemannaledningen utan också på nämnden eftersom den bär det yttersta personuppgiftsansvaret. I enlighet med dataskyddsförordningen är det också den personuppgiftsansvariges skyldighet att aktivt efterfråga information och avrapportering i nämnden, samt hålla sig uppdaterad om förvaltningens hantering av personuppgiftsrelaterad information. Stadsledningskontoret ska under 2020 ta fram rutiner för hur avrapportering till varje nämnd med regelbundenhet ska ske. I den rutinen bedömer stadsledningskontoret att det, för att följa skyldigheterna i dataskyddsförordningen,

är nödvändigt att göra ett avsteg från principen om att inte hålla föredragningar i nämnderna för att möjliggöra för dataskyddsombudet att överlämna muntlig rapportering i nämnderna samt ge dess ledamöter möjligheter att ställa frågor till dataskyddsombudet vid ett samlat sammanträde.

Kommunstyrelsen önskar också göra ett förtydligande rörande rekommendationen att kommunstyrelsen också ska fastställa ett rapporteringskrav gällande frekvens och innehåll som rapporteringen till kommunstyrelse ska utgå från för att säkerställa att uppföljning av dataskyddsförordningen utförs och kommuniceras till ledningen. Vad revisionen avser torde vara att kommunstyrelsen ska ta fram en rutin för hur rapporteringen ska gå till. Den ska sedan användas av samtliga nämnder i deras verksamheter, inte enbart av kommunstyrelseförvaltningens egenrapportering. Syftet med rutinen är att säkra att kommunstyrelsen kan ta sitt ledningsansvar för dataskyddet i staden, men fråntar inte nämnderna skyldigheten att genomföra egenkontroller genom sitt utnämnda dataskyddsombud.

Rekommendation 4: Utbildning och medvetenhet.
Staden löper för närvarande hög risk att dess medarbetare behandlar och sprider personuppgifter felaktigt. Dessutom skulle instruktioner såsom stadens incidenthanteringsdokument kunna vara verkningslösa om inte personalen är medveten om vad som kan utgöra en incident eller att instruktionerna existerar. Dessa instruktioner och rutiner bör kommuniceras regelbundet. Staden bör se till att nyanställda genomför en utbildning inom alla relevanta aspekter av personuppgiftshanteringen och att alla medarbetare genomför utbildningar regelbundet, exempelvis en gång per år. Utbildningarna bör uppdateras alltjämt som lagkraven blir tydligare och nya exempel finns tillgängliga.

Kommentar: Kommunstyrelsen instämmer i revisorernas bedömning. Under 2020 kommer stadsledningskontoret att ta fram webbaserade kortutbildningar som stadens samtliga medarbetare ska erbjudas. I detta arbete ingår också att undersöka vilka möjligheter Sundbybergs stad har neka tillträdde till stadens IT-system för nyanställda till fullföljandet av obligatoriska webbutbildningar inom området informationssäkerhet. Stadsledningskontoret ser också över möjligheten att i olika former koppla e-utbildningar till kvitteringen av inpasseringskort. Detta för att säkerställa förståelsen för informationssäkerhet och dataskydd innan nya medarbetare bereds tillträde till stadens lokaler.

Kommunstyrelsen önskar också förtydliga att samtliga nämnder, inklusive kommunstyrelsen, behöver kalla dataskyddsombudet till sig i syfte att utbildas i ämnet om dataskydd så att de kan ta det ansvar som följer av dataskyddsförordningen. Dataskyddsförordningen ålägger inte dataskyddsombudet att be om tillträde till ledningen. Istället är det den personuppgiftsansvariges skyldighet att hålla sig informerad om arbetet och därmed också den som ska begära att dataskyddsombudet infinner sig och utbildar om ansvaret för dessa frågor.

Rekommendation 5: Leverantörsrelationer.
Staden rekommenderas att slutföra sin inventering av de IT-system och tjänster som behandlar personuppgifter och som tillhandahålls till leverantörer, samt att ingå personuppgiftsbiträdesavtal med samtliga leverantörer där det är relevant.

Kommentar: Kommunstyrelsen instämmer i revisorernas bedömning. Stadsledningskontoret har sedan våren 2019 samverkat med samhällsbyggnads- och serviceförvaltningen kring ett arbete med att identifiera samtliga verksamhetskritiska IT-system. Det i kombination med att hela staden nu genomför en uppdatering av registerförteckningen syftar till att skapa en fullständig förteckning över alla driftsatta och aktiva verksamhetssystem i staden, inkluderat fullständig kontroll över den personuppgiftsbehandling som där förekommer. Under 2020 ska en fördjupad kontroll över stadens personuppgiftsbiträdesavtal genomföras med tonvikt på att upprätta sådana avtal där det i dagsläget eventuellt saknas.

På kommunstyrelsens vägnar

Peter Schilling (S)
kommunstyrelsens ordförande