Tjänsteutlåtande

Dataskyddsombud
Datum 2019-09-12

Till Tekniska nämnden

Granskningsrapport dataskydd; dataskyddsombudets årsrapport 2018-2019

Sammanfattning

Dataskyddsförordningen, även kallad GDPR, trädde i kraft den 25 maj 2018 och innebar en rad förändringar för kommunens personuppgiftshantering. Då kommunen dagligdags hanterar stora mängder personuppgifter, varav många känsliga och extra skyddsvärda, har dataskyddsförordningen betydande påverkan på kommunens hantering av personuppgifter.

Denna rapport innefattar genomgång av väsentliga delar av de minimikrav som dataskyddsförordningen ställer på den personuppgiftsansvarige samt en återkoppling hur dataskyddsarbetet har integrerats i det dagliga arbetet på förvaltningen. Under våren har dataskyddsombudet genomfört en granskning gällande dataskyddsarbetet i de kommunala nämnderna. Granskningen gjordes huvudsakligen genom en enkätundersökning.

Denna rapport gäller i stora delar generellt i hela kommunen men frågeställningarna har i vissa fall brutits ner att gälla enbart den personuppgiftsansvariga nämnden.

Bakgrund

Krav och ansvarsfördelning enligt dataskyddsförordningen generellt
Varje kommunal nämnd är personuppgiftsansvarig och enligt förordningen ytterst ansvarig för att dataskyddsförordningens regler efterlevs. Varje förvaltning/enhet är i sin tur ansvarig för respektive anpassning och efterlevnad av dataskyddsförordningen. Därmed förkommer flertalet variationer av anpassningstakt, metod och arbetssätt inom enheterna.

Dataskyddsombud, vars roll också regleras i förordningen, har en uppgift bl.a. att övervaka att förordningen efterlevs och ge råd och stöd till den ansvarige (nämnden) om dess skyldigheter. Dataskyddsombudet ska även samarbeta med tillsynsmyndigheten.

Dataskyddsorganisation i Österåkers kommun
En ny stödfunktion, dataskyddsstrateg, inrättades i augusti 2019. Dataskyddsstrategen är även dataskyddsombud för de olika nämnderna i kommunen. Dataskyddsstrategen tog fram en skiss för kommunens dataskyddsorganisation, se bilaga 1. Då skapades en ytterligare ny funktion, dataskyddskoordinator, och varje förvaltning skulle utse minst en koordinator. Därefter har kontinuerliga träffar hållits med dataskyddskoordinatorerna under ledning av dataskyddsstrateten. På träffarna har det hållits utbildningar och koordinatorerna har också har haft möjligheten att föra fram förvaltningarnas frågor. Dataskyddsstrategen har haft en stödjande samt utbildande funktion och förvaltningarna har kunna anropa dataskyddsstrategens tjänster vid behov.

Anpassning till dataskyddsförordningen
Kommunens anpassningsarbete påbörjades i februari 2018 under ledning av advokatbyrån Time. Då fick samtliga förvaltningar i uppdrag att kartlägga nämndernas personuppgiftsbehandlingar samt anteckna dessa i en registerförteckning, även en del andra frågor skulle besvaras av förvaltningarna (se bilaga 2). Registerförteckningarna redovisades till Time i särskilda sittningar enskilt med varje förvaltning. Utifrån materialet tog Time fram informationstexter som samtliga förvaltningar inklusive enheter skulle använda sig av. Utöver informationstexter tog Time även fram ett förslag till intern personuppgiftspolicy, riktlinjer för hantering av e-post, riktlinjer för att hantera ostrukturerat material samt riktlinjer för de olika nämnderna.

Inför att dataskyddsförordningen trädde i kraft utsågs dataskyddsombud för samtliga personuppgiftsansvariga nämnder i maj 2018. Dataskyddsombudet tog fram en åtgärdsplan för dataskyddsarbetet som delgavs samtliga förvaltningar samt ett förslag till ändringar i delegationsordningar för samtliga nämnder. De flesta nämnderna har ändrat sina delegationsordningar för att täcka de förvaltningsbeslut som behöver fattas enligt lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen).

Utöver utbildning till dataskyddskoordinatorer har det hållits olika utbildningsserier. I juni 2018 höll dataskyddsombudet en utbildning för samtliga förvaltningar om registerförteckning för att avsluta det initiala arbetet med registerförteckningen som gjordes med Time. Utbildningsmaterial innefattande bl.a. en film hur man fyller i en registerförteckning finns på Inomskärs och är tillgänglig för samtliga anställda. Under våren 2019 höll dataskyddsstrategen fördjupande utbildningar i ämnen som registerförteckning, informationsplikt och registerutdrag, upphandling/inköp och personuppgiftsbiträdesavtal. Under hösten 2019 har utbildningar hållits om bilder och filmer i kommunal verksamhet samt en utbildning om bild och film som riktades särskilt till skolor och förskolor.

Styrande dokument och information
Under hösten 2019 tog dataskyddsstrategen fram ett förslag till personuppgiftspolicy samt riktlinjer för hantering av personuppgifter. Personuppgiftspolicyn antogs av Kommunfullmäktige den 28 januari 2019. Riktlinjer har inte blivit formellt antagna men anvisningarna finns att läsa på Inomskärs som en skrift. Arbetet för att ta fram riktlinjer för e-post tilldelades en arbetsgrupp bestående av chefer i kommunledningsgruppen i januari 2019.

Dataskyddsstrategen har också utvecklat dataskyddssidan på Inomskärs. Av sidan framgår det som förvaltningarna/nämnderna behöver veta om dataskydd, bl.a. blanketter och information om regisförteckning, registerutdrag, informationsplikt, konsekvensbedömningar, dataskydd vid upphandlingar/inköp, personuppgiftsincidenter, personuppgiftsbiträdesavtal, integritet- och dataskydd inom skolan samt foto/film i kommunal verksamhet.

Självutvärdering/enkät
Under våren har dataskyddsombudet genomfört en granskning hur dataskyddsarbetet fallit på plats. Granskningen gjordes huvudsakligen genom en enkätundersökning till enheterna under maj och juni 2019 samt genom viss insamling av registerförteckningar, rutiner m.m. Syftet med självutvärderingen var att kartlägga och bedöma nivån av anpassning och efterlevnad av de lagstadgade kraven i dataskyddsförordningen och även för att visa enheterna vilka minimikrav som ställs på enheterna i dataskyddsarbetet.

Inom Tekniska nämnden har flera enheter svarat på självutvärderingen/enkäten, se bilaga 3, och svarsfrekvensen är god. Svaren är inte entydiga och vissa fall har svar fallit bort och finns i rådatat. Men svaren ger dock in fingervisning hur det ligger till inom nämnden och vilka arbetsområden man måste arbeta mer på.

Kartläggning, registrering, dokumentation och information av personuppgiftsbehandlingar
En nyhet i dataskyddsförordningen var att den personuppgiftsansvarige måste kunna visa att denna lever upp till förordningens krav. Den ansvarige har alltså bevisbördan för detta och dokumentationen blir därför en väldigt viktig del för upprätthållande av rättssäkerhet och t.ex. vid eventuell tillsyn och avsaknad av dokumentation kan innebära att tillsynsmyndigheten är mer benägen att tilldöma sanktionsavgifter. Kartläggningen av personuppgifter utgör också en grund och en förutsättning för förvaltningarnas arbete i dataskyddsfrågor. Kartläggningen mynnar ut till en registerförteckning som är obligatoriskt för varje personuppgiftsansvarig. Registret ska finnas dokumenterat och tillgängligt.

För att kartlägga personuppgiftsbehandlingar samt fylla i en registerförteckning kräver ingående verksamhetskunnande och inblick i verksamheten vilket är anledningen till att det är verksamheterna själva som ska kartlägga behandlingarna samt fylla i registerförteckningen. I Österåker har man valt att använda sig av SKL:s mall för registerförteckning. Man har även valt att inkludera andra delar av kartläggningen samt dokumentation i registerförteckningen, enligt SKL:s rekommendation.
En del av enheterna har valt att arbeta med kartläggningen och registerförteckningarna helt själva men en del har också bokat in sittningar med dataskyddsstrategen. I de fall det har funnits oklarheter har samtliga enheter haft möjlighet att ställa kompletterande frågor till dataskyddsstrategen/-ombudet. Mallar och information om hur man arbetar med förteckningen finns på Inomskärs. Det är viktigt att observera att alla enheter i kommunal verksamhet behandlar personuppgifter och ska därmed kartlägga sina behandlingar samt föra in dem i nämndens registerförteckning.

Exempel på dokumentation

- Registerförteckning
- Checklistor
- Rutinbeskrivningar
- Behörighetstilldelning
- Informationstexter riktade till registrerade (och i vissa fall registrerades anhöriga) kring hur personuppgifter behandlas
- Informationssäkerhetsskrifter
- Dokumenterade konsekvensbedömningar
- Förfrågningsunderlag i upphandlingar
- Dokumentation av personuppgiftsincidenter
- Dokumenthanteringsplan och gallringsrutiner
- Personuppgiftsbiträdesavtal med instruktionsbilaga
- Informationssäkerhetsklassning av system

Informationstexter är en viktig del i dataskyddsarbetet. Advokatbyrån Times tog fram informationstexter som har använts av en del förvaltningar och enheter. Dessa texter innehöll en del felaktigheter som har rättats till i efterhand när dessa har upptäckts men det kan fortfarande förekomma fel. Dataskyddsstrategen har även tagit fram en generell informationstext tillsammans

med Kommunikationsenheten. Denna text ska anpassas till den egna verksamheten och informationstexten ska knytas till hemsidor, formulär, blanketter och e-tjänster, skyltar m.m. där medborgare kommer i kontakt med kommunen på olika sätt. Detta är ett arbete som åvilar förvaltningarna och ska tas med som en naturlig del i verksamheten. På vilket sätt man informerar kan variera från fall till fall beroende på sammanhang och vad man ska informera om. Kommunikationsenheten har utbildats av dataskyddsstrategen att hitta olika vägar i denna kommunikation.

Registerutdrag
Den registrerade kan vända sig till kommunen för att få veta hur nämnden behandlar dennes personuppgifter genom att begära ett registerutdrag. Dataskyddsombudet känner endast till fåtal begäran om registerutdrag som har inkommit. Detta kan bero på flera faktorer; att utlämnandet fungerar som den ska, att kommunen inte informerat tillräckligt tydligt om rätten till registerutdrag eller att en sådan begäran misstagits för att vara en begäran av något annat, t.ex. begäran av allmän handling. Det finns dagsläget ingen kommungemensam process för att lämna ut registerutdrag då man har valt att det är varje personuppgiftsansvarig själv som sköter hantering av en sådan begäran. Dataskyddsombudet har inte några synpunkter på detta så länge hanteringen fungerar på ett rättssäkert sätt.

Personuppgiftsincidenter
En annan nyhet i dataskyddsförordningen är att den ansvarige ska rapportera in vissa personuppgiftsincidenter till tillsynsmyndigheten. En rutin för incidenter togs fram våren 2018 och en blankett för att underlätta dokumentation och eventuell rapportering av incidenter togs fram vintern 2019. Dataskyddsstrategen har utbildat dataskyddskoordinatorerna om vad en incident är och erbjudit sig att komma och prata om ämnet på personalmöten.

Dataskyddsombudet har under 2018 fått kännedom om endast ett fåtal personuppgiftsincidenter i hela kommunen och anmält en incident till Datainspektionen under 2019. Det låga antalet kan antas snarare bero på att kunskaper beträffade vad en personuppgiftsincident är låga och att rutiner för att hantera en sådan inte är inarbetat i organisationen än att kommunens processer är så säkra och fungerande så att inga personuppgiftsincidenter inträffar. Dataskyddsombudets bedömning är att antalet incidenter bör vara högre i en kommun i Österåkers storlek och troligen uppdagas endast en bråkdel av incidenterna. Detta är en reell brist, dels för att det strider mot dataskyddsförordningen att inte dokumentera och rapportera incidenter samt dels för att det är svårare att identifiera bristerna samt arbeta förebyggande för att nya personuppgiftsincidenter inte inträffar. Arbetet med att informera och synliggöra incidenter måste därför fortsättas och bedömningen är att detta görs lämpligast på enhetsnivå t.ex. på arbetsplatsträffar.

Konsekvensbedömningar
En konsekvensbedömning ska göras om en viss personuppgiftsbehandling *sannolikt leder till en hög risk för fysiska personers rättigheter och friheter*. Risken ska i första hand bedömas utifrån dataskydd och integritet, men även utifrån andra grundläggande rättigheter som yttrandefrihet, tankefrihet, fri rörlighet, förbud mot diskriminering, rätt till frihet, samvete och religion. Syftet är att förebygga risker innan de uppkommer. Konsekvensbedömning ska genomföras innan man påbörjar en personuppgiftsbehandling, om risken med en pågående behandling ändras eller för pågående behandlingar om man inte har gjort det tidigare. Dataskyddskoordinatorerna har utbildats om

behovet av konsekvensbedömningar samt det finns utförlig information på Inomskärs när och hur en konsekvensbedömning ska göras.

Enligt art. 35.2 ska dataskyddsombudet rådfrågas vid genomförande av konsekvensbedömning. Med tanke på den verksamhet som bedrivs inom Tekniska nämnden är det är sannolikt att det även finns behov av att göra konsekvensbedömningar. Dataskyddsombudet har inte rådfrågats om att göra konsekvensbedömning inom nämndens verksamhet. Detta är en brist och rekommendationen är den inledande riskanalysen tas med som rutin vid nya personuppgiftsbehandlingar och att man även gör en riskbedömning, samt vid behov konsekvensanalys, i de redan pågående behandlingarna.

Personuppgiftsbiträdesavtal
Den personuppgiftsansvarige ska se till att det finns ett personuppgiftsbiträdesavtal i de fall ett personuppgiftsbiträde finns. Det krävs alltså en kartläggning av befintliga avtal och eventuella biträdessituationer samt att biträdessituationer även behöver identifieras vid upphandling och inköp. Informationsmaterial samt länkar till biträdesavtal med instruktionsbilagor finns på Inomskärs. I Österåker har man valt att använda SKL:s biträdesavtal men även företagens egna avtal kan godkännas efter genomgång. Dataskyddsstrategen har hjälpt verksamheterna med biträdesavtal och framförallt med instruktionsbilagorna till biträdesavtalet vid förfrågningar från verksamheterna.

Dataskyddsstrategen har tagit fram ett förslag till *en intern rättsakt* som ska reglera personuppgiftsansvarig/-biträdessituationerna inom kommunen. Ett beslut behöver tas av kommunledningen i frågan. Rekommendationen är att beslut om rättsakt fattas snarast så att ansvarsgränserna som rör framförallt de kommunövergripande funktionerna såsom HR, IT, Servicecenter tydliggörs.

Känsliga eller extra skyddsvärda personuppgifter
Huvudregeln är att all behandling av känsliga personuppgifter är förbjudet. Det finns dock undantag från förbudet i stora delar av kommunal verksamhet där behandlingen av känsliga personuppgifter är nödvändiga, t.ex. myndighetsutövning reglerad i lag, HR, omsorgsverksamhet och skola. Observera att behandlingen i sådana fall alltid ska kunna härledas till en lag, föreskrift eller skyldighet som ankommer kommunen. Hantering av känsliga och extraskyddsvärda personuppgifter kräver förhöjt säkerhet och säkerhetsmedvetande, dvs. satsningar både på organisatorisk och på teknisk säkerhet.

Informationssäkerhet
I dataskyddsförordningen finns ett tydligare krav på att det måste finnas ett kontinuerligt informationssäkerhetsarbete för att garantera skydd för de personuppgifter man behandlar (artikel 32 och skäl 83). Skyddet för personuppgifter ska därmed tas med i det systematiska informationssäkerhetsarbetet för att kunna efterleva de krav som finns i dataskyddsförordningen. För att arbeta med informationssäkerhet krävs det att frågorna initieras av ledningen och ett tydligt mandat för att driva arbetet. Att kommunen inte generellt arbetar med informationssäkerhet är en brist.

Ledningens engagemang
För att dataskyddsfrågorna ska få genomslagskraft krävs det förståelse och engagemang hos ledningen för frågorna. Dessutom rapporterar dataskyddsombudet direkt till personuppgiftsansvariges högsta förvaltningsnivå (art. 38.3) och det är därför viktigt att dataskyddsombudet regelbundet kallas till ledningsgruppsmöten för att ta upp relevanta

frågeställningar. Dataskyddsombudet har varit bjudet till förvaltningschefsmöten vid två tillfällen i våren 2018 samt till kommunledningsgruppen en gång på våren 2019 och en gång hos förvaltningsledningen inom samhällsbyggnadsförvaltningen hösten 2019. För att kontinuerligt arbeta med frågorna behöver dataskyddsombudet med regelbundenhet bjudas in i ledningsgrupperna och detta är en brist i dagsläget.

Utbildning av personal samt deltagande i dataskyddsarbetet
Samhällsbyggnadsförvaltningen har utsett en representant som dataskyddskoordinator. Med tanke på förvaltningens storlek skulle det behövas minst en till representant med en möjlighet att avsätta tid till dataskyddsarbetet.

Personalen på förvaltningen/nämnden har aktivt deltagit i de utbildningar som har anordnats inom dataskydd. Dataskyddsstrategen/-ombudet har även varit inbjuden till olika sittningar med enheterna samt rådfrågats flitigt vid olika situationer. Sammanfattningsvis kan man säga att dataskyddsombudet har integrerats tillfredsställande sätt i det dagliga arbetet inom nämndens verksamhet.

Dataskyddsombudets iakttagelser och slutsatser

Det är allmänt känt att mognaden i dataskyddsfrågorna tar tid. De kommuner, företag och organisationer som började arbeta med frågorna 1-2 år innan förordningen trädde i kraft har i dagsläget uppnått godtagbar nivå i sitt dataskyddsarbete. Att landa i frågeställningarna i det dagliga arbetet tar tid så även i Österåkers kommun.

Österåkers kommun har en strukturerad organisation för dataskyddsarbetet med tydliga roller och ansvarsområden men de flesta dataskyddskoordinatorerna inte haft någon reell tid eller någon reell möjlighet att ägna dataskyddsfrågorna inom sin ordinarie tjänst. Det har därför varit svårt att bedriva ett effektivt och strukturerat arbete för att uppnå efterlevnad av förordningen. Dataskyddsstrategens/-ombudets arbete är stora delar beroende av att förvaltningarna/enheterna kontaktar funktionen. Merparten av funktionens arbete har bestått av att ge råd och stöd samt hantera mer akuta situationer. Dataskyddsstrategen/-ombudet behöver kontaktas i god tid och det krävs med strukturerat arbete på förvaltningarna i dataskyddsfrågor för att undvika sena lösningar och därmed även höja kvalitén i dataskyddsarbetet. Det krävs också att koordinatorerna har en reell möjlighet att arbeta med frågorna samt att frågorna tydligt ges utrymme i deras tjänstebeskrivningar. Kommunen har, i skrivande stund, bestämt att avveckla rollen dataskyddsstrateg och det oklart hur funktionen dataskyddsombud kommer att hanteras. Det är därför en aktuell fråga hur dataskyddsarbetet kommer att fortsätta för att uppnå en godtagbar nivå av dataskydd.

Rekommendationer

Tekniska nämnden bildades efter valet 2018 men enheterna som ingår i nämnden har sedan dataskyddsförordningen trädde i kraft arbetat med att anpassa sig till kraven i förordningen. Arbetet har bland annat omfattat kartläggning av personuppgiftsbehandlingar, framtagande av personuppgiftsbiträdesavtal, utbildningar till medarbetarna, registrering av personuppgiftsbehandlingar. Detta arbete är inte färdigt utan måste fortsätta för att sedan ingå som en naturlig i den dagliga förvaltningen.

Tjänsteutlåtande

De minimikrav som framgår av denna skrift samt nedanstående lista måste finnas på plats för att tillfredsställande dataskyddsarbete ska kunna bedrivas av nämnden/ kommunen.

- *Att kommunen även i fortsättningen har tydlig organisation för dataskyddsarbete med utpekade funktioner med tydliga uppdrag samt mandat kopplade till rollen.*
- *Att säkerställa att dataskyddsarbetet fortgår även när den centrala funktionen dataskyddsstrateg försvinner.*
- *Övergripande rutiner, processer och arbetssätt för dataskyddsarbetet där rutiner inom följande områden saknas och bör prioriteras:*
    - *Hantering av e-post*
- *En intern rättsakt för att reglera personuppgiftsbiträdessituation mellan nämnderna saknas och bör prioriteras (ett färdigt förslag finns framtaget av dataskyddsstrategen)*
- *Fortsatt arbete med registerförteckning inom respektive nämnd/verksamhet*
- *Fortsatt kartläggning av biträdessituation samt nyteckning av biträdesavtal inom respektive nämnd/verksamhet*
- *Informera och synliggöra personuppgiftsincidenter samt dokumentera dem inom nämnden/enheten*
- *Informera och synliggöra behovet av konsekvensbedömningar samt dokumentera dem inom nämnden/enheten*
- *Större engagemang hos ledningsgrupperna för frågor rörande dataskydd samt informationssäkerhet*
- *Tydliga behörighetsgränser samt loggkontroller i de verksamhetssystem som innehåller personuppgifter, särskilt känsliga personuppgifter*

Ytterligare något som kommunen borde arbeta med som är förutsättning för gott dataskyddsarbete:

- *Systematiskt informationssäkerhetsarbete*
- *Informationssäkerhetspolicy*

Bilagor

1. Dataskyddsorganisation i Österåkers kommun, 2018-08-16
2. Times frågeformulär samt registerförteckning
3. Svar självutvärderingsenkät Tekniska nämnden våren 2019

Anne Savolainen
Dataskyddsombud