

Tjänsteutlåtande

Utfärdat 2023-11-14

Diarienummer 0266/23

Handläggare: Linda Bengtsson

Telefon: 031-368 66 59

E-post: linda.bengtsson@stadsrevisionen.goteborg.se

Beslut om godkännande av framtagen konsekvensbedömning inför lansering av Digitala navet hos stadsrevisionen

Förslag till beslut

Revisorskollegiet föreslås besluta:

att godkänna framtagen konsekvensbedömning enligt dataskyddsförordningen, som avser de personuppgiftsbehandlingar som kommer att ske i IT-systemet Digitala navet.

Sammanfattning

Göteborgs Stad inför en ny lösning för att tillhandahålla en kommungemensam tjänst för intranät till Stadens verksamheter. Då ett införande/lansering av tjänsten hos en verksamhet innebär ett införande av ett nytt IT-system för verksamheten aktualiseras dataskyddsförordningens krav på att utreda behovet av att göra en konsekvensbedömning och om behov konstateras, att även genomföra en sådan. Stadsrevisionen har i detta genom revisionskontoret konstaterat att behov finns och har även genomfört en konsekvensbedömning. Underhandsinformation i ärendet har lämnats till revisorskollegiet vid sammanträde den 17 oktober 2023. Inom ramen för detta tjänsteutlåtande beskrivs översiktligt revisorskollegiets personuppgiftsansvar, varför en konsekvensanalys ska göras, hur beredningen av förslaget till konsekvensanalys gått till samt vissa väsentligare iakttagelser och bedömningar som gjorts under arbetsprocessen. Förslaget till konsekvensanalys bifogas i form av bilaga 1 till tjänsteutlåtandet.

Bedömning ur ekonomisk dimension

Införandet av Digitala navet som ersättning för det tidigare separat uppsatta intranätet innebär att detta system ersätts inom ramen för Stadens befintliga systemstruktur och plattformen Office 365. Ur ett stadsövergripande perspektiv framstår detta som en ekonomiskt fördelaktig lösning då kostnaderna för det äldre (och föråldrade) systemet på sikt kommer att fasas ut och avvecklas. Ur revisionskontorets perspektiv bedöms kostnaderna för att fortsätta använda den kommungemensamma tjänsten för intranät efter systembytet utifrån kända parametrar inte öka i någon betydande mån.

Bedömning ur ekologisk dimension

Revisionskontoret har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Bedömning ur social dimension

Revisionskontoret har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Samverkan

Ärendet har samverkats i den fackliga samverkansgruppen 2023-11-08.

Bilagor

1. Konsekvensbedömning enligt dataskyddsförordningen,
Personuppgiftsbehandlingarna: Att informera och
kommunicera i Digitala navet

Ärendet

Revisorskollegiet ska fatta beslut om att godkänna framtagna konsekvensbedömningar enligt dataskyddsförordningen, som avser de personuppgiftsbehandlingar som kommer att ske i IT-systemet Digitala navet som planeras att driftsättas hos stadsrevisionen.

Beskrivning av ärendet

I Göteborgs Stad finns sedan många år tillbaka ett IT-system som i form av kommun-gemensam tjänst som tillhandahålls stadens verksamheter av nämnden för intraservice (intraservice). Systemet är baserat på en idag föråldrad IT-plattform och ett utbyte till en modernare teknisk lösning har därför beretts av projektgrupp i Staden. Den lösning Staden valt att gå vidare med i detta är baserad på och utvecklad för applikationen SharePoint som ingår i Microsoft Office 365-plattformen. Lösningen har bedömts fungera betydligt bättre än det äldre systemet från såväl informationssäkerhets-, dataskydds- som kommunikativt perspektiv. Revisorskollegiet har fått underhands-information om införandet av den kungemensamma tjänsten och behovet att upprätta en konsekvensanalys vid sitt sammanträde den 17 oktober 2023.

Revisorskollegiets personuppgiftsansvar

Stadsrevisionen i Göteborgs Stad granskar årligen all verksamhet i Göteborgs Stad i enlighet med lag och god sed. Ytterst ansvariga för denna verksamhet är de 22 förtroendevalda revisorerna i Staden. Revisorernas gemensamma förvaltning hanteras i enlighet med revisorernas reglemente av revisorskollegiet. Kollegiet består av 7 ordinarie ledamöter och 4 ersättare som utsetts bland revisorerna av kommunfullmäktige och kan i många stycken jämföras med en kommunal nämnd. Kollegiet företräder revisorerna i förvaltningsfrågor och utgör därigenom anställningsmyndighet, arkivansvarig och personuppgiftsansvarig för stadsrevisionens verksamhet.

Krav på konsekvensanalys och beredningen av förslaget

Innan ett nytt IT-system ska tas i bruk så åligger det en personuppgiftsansvarig att pröva om användningen av det kommer att innebära behandling av personuppgifter som sannolikt leder till en hög risk för fysiska personers rättigheter enligt dataskyddsförordningen (GDPR). Om prövningen visar att så är fallet ska den personuppgiftsansvarige göra en konsekvensbedömning i enlighet med artikel 35 i förordningen. En sådan konsekvensbedömning syftar till att klargöra vilka risker som finns för integritetsskyddet, hur den personuppgiftsansvarige hanterat dessa risker samt dokumentera den personuppgiftsansvariges arbete kopplat till hanteringen. Om konsekvensbedömningen slutligen visar att där finns särskilt höga kvarstående risker som inte hanterats på ett tillfredsställande sätt ska den personuppgiftsansvarige även rådgöra särskilt med tillsynsmyndigheten (Integritetsskyddsmyndigheten - IMY) i enlighet med artikel 36 innan systemet tas i bruk och några personuppgiftsbehandlingar därmed utförs.

Enligt artikel 35.2 ska den personuppgiftsansvarige rådfråga dataskyddsombudet vid genomförande av en konsekvensbedömning avseende dataskydd. I Göteborgs Stad finns stadsgemensamma dataskyddsombud för stadens verksamheter som utses av kommunstyrelsen och är placerade vid Dataskyddsenheten. Organisatoriskt tillhör denna enhet nämnden för intraservice. I samband med att dataskyddsförordningen infördes 2018 fattade revisorskollegiet beslut om att revisorernas förvaltning av oberoende- och granskningsskäl inte skulle anlita dataskyddsombud via kommunstyrelsen/Dataskydds-

enheten. Som en konsekvens av detta ställningstagande utsågs ett internt dataskyddsombud för stadsrevisionen.

Arbetet med att ta fram konsekvensbedömningen för Digitala navet har utförts av en arbetsgrupp vid revisionskontoret som letts av undertecknad i rollen som administrativ chef och dataskyddsansvarig tjänsteperson. Övriga personer i gruppen har varit kommunikationsansvarig samt registrator. Stadsrevisionens dataskyddsombud har också ingått i arbetsgruppen i en stödjande och rådgivande roll.

Vid den inledande utredningen av behovet av att ta fram en konsekvensbedömning har det konstaterats att ett sådant behov finns i enlighet med dataskyddsförordningens regelverk. Vid arbetet med att ta fram förslaget till konsekvensbedömning har det vidare konstaterats att sådana särskilt höga kvarstående risker som kan antas utlösa skyldighet att samråda med tillsynsmyndigheten i enlighet med artikel 36 *inte* föreligger.

I förslaget till konsekvensbedömning har arbetsgruppen vidare gjort vissa väsentligare iakttagelser och bedömningar. Dessa beskrivs vidare under egna rubriker nedan:

Ansvar kopplat till användning av IT-system i den kommungemensamma miljön

Det är alltid den personuppgiftsansvarige som är ansvarig för att föreskrivna krav för personuppgiftsbehandling enligt dataskyddsförordningen följs och upprätthålls för en verksamhet. Detta kan innebära särskilda utmaningar i en kommun där drifts- och utvecklingsansvar för gemensamma IT-system ligger utanför den personuppgiftsansvariges kontroll. Detta är fallet i Göteborgs Stad där detta ansvar vilar på nämnden för intraservice medan personuppgiftsansvaret primärt vilar på den verksamhet som använder ett kommungemensamt system.

Det är då – ur dataskyddssynpunkt – mycket viktigt att den personuppgiftsansvarige så långt det är möjligt eftersträvar att tillförsäkra sig kontroll över och insikt i hur personuppgiftsbehandlingar görs i de system som tillhandahålls av nämnden för intraservice. Detta arbete behöver också dokumenteras så det framgår att det gjorts, för att den personuppgiftsansvariges ansvarsskyldighet att kunna uppvisa följsamhet mot förordningens regelverk ska kunna mötas. En konsekvensbedömning ska också i sig själv redogöra för vilka risker som identifierats och hur de bedömts och hanterats i de system som utför behandlingarna. Annorlunda uttryckt ska en registrerad (det vill säga den vars personuppgifter behandlas) med ledning av en konsekvensbedömning kunna ta del av all information som krävs för att själv förstå vilka behandlingar som sker och att den personuppgiftsansvarige vidtagit nödvändiga åtgärder för att begränsa de risker som finns. Arbetsgruppen har därför valt att – mot bakgrund av att det Digitala navet utgörs av en SharePoint baserad applikation som fungerar i Office 365-miljö - innefatta en omfattande teknisk redovisning för hur de underliggande systemen för tjänsten fungerar ur dataskyddssynpunkt. Denna redovisning bygger på underlag som framtagits av nämnden för intraservice och även använts vid denna nämnds egen konsekvensbedömning för Digitala navet.

Kvarstående osäkerhet runt fördelning av personuppgiftsansvar i Staden

Nämnden för intraservice arbetar med att anpassa sin verksamhet till ”Göteborgs Stads /nya/ riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltning”. Ett led i detta arbete innefattar en förändring av det tidigare gällande

syndsättet i Staden att nämnden med stöd av sitt uppdrag - som beslutats av fullmäktige - fungerar som personuppgiftsbiträde i förhållande till övriga verksamheter i Staden.

Det har då i sin tur inneburit att detta beslut medgett ett undantag från det normala kravet enligt dataskyddsförordningen som innebär att en personuppgiftsansvarig som anlitar ett personuppgiftsbiträde, också ska sluta ett särskilt avtal med instruktioner för hur personuppgifter ska hanteras av biträdet.

Den nya inriktningen via riktlinjen enligt ovan är att personuppgiftsansvaret efter utredning ska fördelas på ett tydligare sätt i staden vid användning av olika system och applikationer och att separata personuppgiftsbiträdesavtal ska slutas mellan verksamheter i Staden och nämnden för intraservice. Då arbetet inte är färdigställt innebär det en otillfredsställande situation för stadsrevisionen, liksom för andra verksamheter i staden.

Dataskyddsombudet har påtalat att utvecklingen i denna del behöver följas noga så att korrekt utformade personuppgiftsbiträdesavtal kan slutas med nämnden för intraservice snart det kan ske. Utkast till personuppgiftsbiträdesavtal som hittills presenterats av nämnden har inte varit utformade i enlighet med dataskyddsförordningens krav då de saknat underlag för instruktioner respektive tydliga hänvisningar till vilka underbiträden nämnden använder sig av.

Överföring av personuppgifter till tredje land

Vid överföring av personuppgifter till land utanför EU/EES (tredje land) kräver dataskyddsförordningen att det mottagande landet har en skyddsnivå för personuppgifterna och de registrerades intressen som motsvarar vad som gäller för där förordningen är direkt tillämplig. Om det finns ett giltigt så kallat "adekvansbeslut" det vill säga ett beslut av EU-kommissionen att mottagarlandet (det tredje landet) har en sådan adekvat skyddsnivå så kan den personuppgiftsansvarige stödja sig på det och göra överföringen utan risk att bryta mot förordningen.

Under nämnden för intraservice arbete med att ta fram Digitala navet har det saknats ett giltigt adekvansbeslut för Förenta staterna (USA), vilket i sig varit problematiskt då viss överföring sker vid användning av underliggande system i Office 365-plattformen.

Från och med den 10 juli 2023 gäller dock ett nytt adekvansbeslut. Beslutet gäller inte generellt för alla typer av överföringar av personuppgifter till USA utan att är begränsat till att gälla överföringar som sker till organisationer etablerade där och som omfattas av det nya ramverket "EU-US data privacy framework." Ramverket är en mekanism för självcertifiering där de organisationer som vill delta får genomgå en särskild process för att godkännas. Certifieringen gäller för ett år i taget och kan därefter förnyas via ytterligare en process. Företaget Microsoft, som ansvarar för Office 365 är certifierade och omfattas därmed av adekvansbeslutet.

Det är dock inte självklart att adekvansbeslutet kommer att gälla om EU-domstolen prövar det. Det finns tydliga signaler att det kommer att utmanas i framtiden, vilken innebär en risk för att det i likhet med tidigare liknande (föregående adekvansbeslut) avseende USA kan komma att upphävas av domstolen. Det finns också en risk att Microsoft inte alltid kommer att vara certifierade under EU-US data privacy framework.

Dataskyddsbudeten har därför lyft att det därför är av stor vikt att stadsrevisionen, liksom övriga personuppgiftsansvariga som arbetar i/med Office 365-baserade system/applikationer – noga bevakar den fortsatta utvecklingen runt dessa frågor.

Begränsning av information i det Digitala navet

Arbetsgruppen har konstaterat att användning av det Digitala navet kan innebära många fördelar ur kommunikationssynpunkt då det ger stadens verksamheter och medarbetare enkel tillgång till stora informationsmängder. Detta innebär samtidigt risker ur integritets- och dataskyddssynpunkt. Revisionsdirektören har därför i dialog med arbetsgruppen och inom ramen för arbetet med att ta fram förslaget till konsekvensbedömning med hänvisning till detta beslutat att begränsa informationsmängden om den egna verksamheten i det Digitala navet. Funktioner som kommentarsfält och liknande i systemet kommer inte heller att aktiveras hos stadsrevisionen av samma skäl.

Arbetsgruppens bedömning är att framtaget förslag till konsekvensbedömning nu motsvarar dataskyddsförordningens krav och avspeglar såväl identifierade integritetsrisker som åtgärder för att hantera dessa på ett korrekt sätt.

Förutsatt att revisorskollegiet godkänner konsekvensbedömningen i egenskap av personuppgiftsansvarig för stadsrevisionens verksamhet kan revisionsdirektören fatta efterföljande beslut om lansering/driftsättning av IT-systemet Digitala navet.

Förslag till beslut

Revisionskontorets förslag är att revisorskollegiet fattar beslut att godkänna framtagna konsekvensbedömning enligt dataskyddsförordningen, som avser de personuppgiftsbehandlingar som kommer att ske i IT-systemet Digitala navet.

Linda Bengtsson

Cecilia Bokenstrand

Administrativ chef

Revisionsdirektör