Tilläggsyrkande/ Socialdemokraterna, Vänsterpartiet, Miljöpartiet

2024-01-05 Ärende nr 27

Yrkande angående – Hemställan från nämnden för intraservice att utreda ansvarsfördelning av personuppgiftsbehandlingar i gemensamma tjänster

Förslag till beslut

I kommunstyrelsen:

1. Stadsledningskontoret får i uppdrag att fördjupa samverkan med förvaltningen för intraservice kring personuppgiftsbehandlingar i gemensamma tjänster och återkomma till kommunstyrelsen med redovisning av hur arbetet fortlöper.
2. Hemställan från nämnden för intraservice att utreda ansvarsfördelning av personuppgiftsbehandlingar i gemensamma tjänster och tjänster tillhörande digital infrastruktur avslås.

Yrkandet

Stadsledningskontoret föreslår att hemställan avslås med hänvisning till att det bedrivs ett arbete tillsammans med förvaltningen för intraservice i syfte att klarlägga hur intraservice respektive stadsledningskontoret och kommunstyrelsen ser på vissa personuppgiftsbehandlingar som involverar två eller fler nämnder och styrelser.

Från intraservice sida uppfattar man brister i samverkan och ser behov av förtydligad ansvarsfördelning. Med hänsyn till att ärendet berör väsentliga frågor med bäring på datasäkerhetslagstiftning och korrekt hantering av personuppgifter så ser vi behov av fördjupad samverkan och återredovisning till kommunstyrelsen.

Yrkande Sverigedemokraterna

2023-12-05 Ärende nr SLK-2023-00665

Yrkande angående – Hemställan från nämnden för intraservice att utreda ansvarsfördelning av personuppgiftsbehandlingar i gemensamma tjänster

Förslag till beslut

I kommunstyrelsen:

1. Stadsledningskontoret får i uppdrag att i samverkan med Intraservice hålla en muntlig redovisning för kommunstyrelsen samt tillhandahålla ett skriftligt underlag.

Yrkandet

Stadsledningskontoret bedriver ett arbete tillsammans med förvaltningen för intraservice (Intraservice) i syfte att klarlägga hur Intraservice respektive stadsledningskontoret och kommunstyrelsen ser på vissa personuppgiftsbehandlingar som involverar två eller fler nämnder och styrelser. Exempelvis Intraservice behandlingar av personuppgifter kopplad till digital infrastruktur och säkerhet samt stadsledningskontorets och kommunstyrelsens behandlingar kopplade till vissa gemensamma system i staden.

Kommunstyrelsen ska enligt kommunallagen leda och samordna förvaltningen av kommunens angelägenheter samt ha uppsikt över övriga nämnder och gemensamma nämnders verksamhet.

En muntlig redovisning bör hållas för kommunstyrelsen samt ett skriftligt underlag tillhandahållas. Genom detta håller kommunstyrelsen sig uppdaterad och informerad.

För att säkerställa uppsiktsnivån ska som minimum följande redovisas:

- aktuell status samt uppföljning av mål
- klarläggandearbetets kvalitet
- intern kontroll och efterlevnad

Göteborgs Stad

Tjänsteutlåtande
Utfärdat 2023-11-16
Ärendenummer SLK-2023-00665

Handläggare
Magnus Junsäter, Linn Samuelsson
Telefon: 031-368 02 27
E-post: fornamn.efternamn@stadshuset.goteborg.se

Hemställan från nämnden för intraservice att utreda ansvarsfördelning av personuppgiftsbehandlingar i gemensamma tjänster

Förslag till beslut

I kommunstyrelsen:

Hemställan från nämnden för intraservice att utreda ansvarsfördelning av personuppgiftsbehandlingar i gemensamma tjänster och tjänster tillhörande digital infrastruktur avslås.

Sammanfattning

Enligt dataskyddslagstiftningen ansvarar varje nämnd och styrelse för att bedöma personuppgiftsansvaret för egen del. En av frågorna som varje nämnd eller styrelse behöver bedöma är i vilken roll en viss personuppgiftsbehandling görs; som personuppgiftsansvarig, personuppgiftsbiträde eller gemensamt personuppgiftsansvar. För vissa behandlingar krävs samverkan och samordning av arbetet nämnder och styrelser emellan.

Stadsledningskontoret bedriver ett arbete tillsammans med förvaltningen för intraservice (Intraservice) i syfte att klarlägga hur Intraservice respektive stadsledningskontoret och kommunstyrelsen ser på vissa personuppgiftsbehandlingar som involverar två eller fler nämnder och styrelser. Det handlar exempelvis om Intraservice behandlingar av personuppgifter kopplad till digital infrastruktur och säkerhet samt stadsledningskontorets och kommunstyrelsens behandlingar kopplade till vissa gemensamma system i staden.

Stadsledningskontorets bedömning är att ett uppdrag till kommunstyrelsen att utreda ansvarsfördelning av personuppgiftsbehandlingar i gemensamma tjänster och tjänster tillhörande digital infrastruktur inte är nödvändigt med hänvisning till redan pågående arbete. Det är även viktigt att respektive nämnd eller styrelse tar eget ansvar för att kartlägga och bedöma hur personuppgiftsbehandlingar ska hanteras och att samverkan sker med andra berörda nämnder eller styrelser i de fall där ansvaret för personuppgiftsbehandlingen inte är tydligt.

Bedömning ur ekonomisk dimension

Stadsledningskontoret ser inte att hemställan om ett uppdrag att utreda ansvarsfördelning av personuppgiftsbehandlingar i gemensamma tjänster och tjänster tillhörande digital infrastruktur ger några betydande ekonomiska konsekvenser. Tydlig ansvarsfördelning av personuppgiftsbehandlingar kan på sikt skapa effektivare arbetsprocesser och minska

administration i samband med vidareutveckling eller nyutveckling av system. Detta bedöms dock inte avhängigt uppdraget som föreslås, då frågan om personuppgiftsansvar ändå är reglerad i lagstiftning och det är tydligt utpekat att varje nämnd och styrelse ska bedöma personuppgiftsansvaret för egen del.

Bedömning ur ekologisk dimension

Stadsledningskontoret har inte funnit några särskilda aspekter på frågan utifrån denna dimension

Bedömning ur social dimension

Dataskyddslagstiftningen ställer krav på organisationer och företag att behandla personuppgifter på ett lagligt och korrekt sätt. Grundläggande bestämmelser om rätt till privatliv och skydd för personuppgifter ligger till grund för den närmare lagstiftningen om behandling av personuppgifter som till exempel dataskyddsförordningen. Tydlig ansvarsfördelning av personuppgiftsbehandlingar är viktigt för att säkerställa att behandlingar sker korrekt och att personuppgifter hanteras på ett ändamålsenligt och säkert sätt.

Bilaga

Nämnden för intraservice handlingar 2023-06-21 § 127

Ärendet

Nämnden för intraservice beslutade 2023-06-21 § 127 att hemställa till kommunstyrelsen att utreda ansvarsfördelning av personuppgiftsbehandlingar i gemensamma tjänster och tjänster tillhörande digital infrastruktur.

Beskrivning av ärendet

I samband med nämndens för intraservice behandling av ställningstagande gällande konsekvensbedömning av risker kopplade till förvaltningens personuppgiftsbehandlingar i Digitala navet hemställde även nämnden till kommunstyrelsen att utreda ansvarsfördelning av personuppgiftsbehandlingar i gemensamma tjänster och tjänster tillhörande digital infrastruktur. Bakgrund till hemställan är att Intraservice anser att ansvarsförhållanden gällande vilken part som ska anses vara personuppgiftsansvarig, personuppgiftsbiträde eller om det råder delat personuppgiftsansvar är fortsatt oklara tills dess att detta är utrett och fastställt.

Stadsledningskontoret finner att underlaget i intraservice tjänsteutlåtande inte beskriver bakgrund, syfte eller pågående arbete utifrån hemställt uppdrag särskilt väl. Det finns därmed skäl att sätta frågan i ett större sammanhang.

Ansvar och roller i dataskyddslagstiftningen

I Sverige och EU är dataskyddsförordningen (GDPR) den huvudsakliga lagstiftningen för skydd av personuppgifter. Dataskyddslagstiftningen ställer krav på organisationer och företag att behandla personuppgifter på ett lagligt och korrekt sätt. Grundläggande bestämmelser om rätt till privatliv och skydd för personuppgifter, som dataskyddsförordningen, ligger till grund för den närmare lagstiftningen om behandling av personuppgifter. Behovet av ett starkare lagligt skydd för personuppgifter har ökat stort med digitaliseringen i samhället.

I dataskyddsförordningen är det reglerat att organisationer och företag kan behandla personuppgifter i olika roller. Vilken roll som en organisation har vid behandlingen av personuppgifter styr vilka åtaganden och skyldigheter organisationen har för den aktuella behandlingen. De olika roller som en organisation kan ha är personuppgiftsansvarig och personuppgiftsbiträde. Om man är personuppgiftsansvarig kan ansvaret i vissa fall dessutom vara gemensamt med annan personuppgiftsansvarig.

Skillnaderna med personuppgiftsansvarig, personuppgiftsbiträde eller gemensamt personuppgiftsansvar

Personuppgiftsansvarig enligt dataskyddsförordningen är ”en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter”. I en kommunal verksamhet är personuppgiftsansvaret enligt dataskyddsförordningens bestämmelser knutet till respektive nämnd och styrelse för de personuppgifter som förekommer i den egna verksamheten. Det gäller exempelvis uppgifter om den egna personalen och de uppgifter om personer som förekommer i ärenden hos nämnden eller styrelsen. Den som är personuppgiftsansvarig kan överlåta den faktiska behandlingen av personuppgifter men personuppgiftsansvaret kan aldrig överlåtas.

Personuppgiftsbiträde enligt dataskyddsförordningen är ”en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning”. Ett personuppgiftsbiträde finns alltid utanför den

personuppgiftsansvarigas organisation. I kommunal verksamhet kan ett personuppgiftsbiträde vara en helt extern aktör eller en annan nämnd eller styrelse i den egna kommunala koncernen. Ett företag som anlitas för att lagra uppgifter åt ett annat är ett exempel på personuppgiftsbiträde. Molntjänstföretag som anlitas för att hantera och lagra personuppgifter är att anse som personuppgiftsbiträden åt den personuppgiftsansvarige.

Om två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med, och medlen för, behandlingen ska de vara gemensamt personuppgiftsansvariga.

Det kan i vissa fall vara svårt att göra bedömningen i vilken roll man som organisation behandlar personuppgifter. Men i de allra flesta fall är det enkelt. Alla personuppgifter som behövs i verksamheten är man som utgångspunkt personuppgiftsansvarig för.

Myndigheters ansvar kopplat till behandling av personuppgifter

Personuppgiftsansvaret enligt dataskyddslagstiftningen ansvarar varje nämnd och styrelse för att bedöma för sin egen del. Arbetet genomförs vanligtvis – och lämpligen – med en kartläggning av den egna verksamhetens behandling av personuppgifter. Kartläggningen av personuppgiftsbehandlingar i en verksamhet är en viktig grund för allt annat arbete kopplat till kraven i dataskyddslagstiftningen. Genom kartläggningen kan organisationen bland annat fånga upp vilka personuppgiftsbehandlingar som görs och i vilken roll, dokumentera behandlingarna i ett så kallat behandlingsregister enligt dataskyddsförordningen, redovisa sina behandlingar för de som berörs i olika informationstexter, med mera.

Bedömning av personuppgiftsansvar i praktiken

En av frågorna som varje nämnd/styrelse behöver bedöma är i vilken roll en viss personuppgiftsbehandling görs; som personuppgiftsansvarig, personuppgiftsbiträde eller kanske med ett gemensamt personuppgiftsansvar. Som nämnts ovan är denna bedömning i de flesta fall enkel att göra. Men det finns exempel på personuppgiftsbehandlingar där bedömningen inte är så enkel. Situationer där bedömningen kan vara svårare är exempelvis då flera juridiskt åtskilda verksamheter, såsom olika nämnder, har tillgång till samma uppgifter eller då sättet att behandla uppgifterna har bestämts av någon annan än den egna nämnden. Den egna nämnden/styrelsen kan i denna typ av situationer vara i behov av att stämma av närmare med annan nämnd eller styrelse och därigenom få en bättre helhetsbild av personuppgiftsbehandlingen, för att kunna göra sin bedömning. Det är också viktigt för staden som helhet att nämnder och styrelser har en gemensam bild av hur personuppgiftsansvaret fördelar sig mellan dem.

I de fall som nämnderna/styrelserna ställs inför en svår bedömning där personuppgiftsansvaret inte enkelt kan bedömas utan avstämning med annan nämnd eller styrelse gällande dennes behandling behöver det som utgångspunkt ske samverkan.

Pågående arbete avseende personuppgiftsansvar

Arbetet med att bedöma rollerna i olika personuppgiftbehandlingar sker – och behöver ske – på olika håll i staden. Det är viktigt att varje nämnd och styrelse tar sitt ansvar och bedömer de personuppgiftsbehandlingar som förekommer i deras verksamheter. Detta arbete är respektive nämnd och styrelse skyldiga att göra enligt dataskyddslagstiftningen. Arbetet är också en viktig förutsättning för att samverkan ska kunna ske beträffande de personuppgiftsbehandlingar där det finns överlappningar med andra nämnder och styrelser. Såvitt stadsledningskontoret känner till pågår arbete i nämnder och styrelser

med bedömning av deras respektive personuppgiftsbehandlingar. I detta arbete finns enligt uppgift även dataskyddsombud på Dataskyddsenheten tillgängliga för rekommendationer och viss vägledning.

Stadsledningskontoret bedriver internt ett dataskyddsarbete med en etablerad intern dataskyddsorganisation för att uppfylla kraven i dataskyddslagstiftningen. Identifieringen av alla stadsledningskontoret/kommunstyrelsen personuppgiftsbehandlingar, inklusive de behandlingar som överlappar med andra nämnder och styrelser, ingår i detta arbete.

När det gäller den centrala samordningen och samverkan mellan nämnder och styrelser i frågor gällande personuppgiftsbehandling som berör flera av dem, är det inte känt för stadsledningskontoret i vilken omfattning detta sker. Eftersom behovet finns och skyldigheten att samverka gäller, bör det ske.

Stadsledningskontorets bedömning

Inom ramen för leverans och användning av de gemensamma tjänsterna, som i nuläget levereras av tre olika nämnder i staden (nämnden för intraservice, nämnden för demokrati- och medborgarservice samt inköp och upphandlingsnämnden), förekommer mängder av personuppgiftsbehandlingar. För merparten av personuppgiftsbehandlingarna är personuppgiftsansvaret enkelt att bedöma och det görs inom ramen för respektive nämnds eller styrelses interna dataskyddsarbete. Men för några personuppgiftsbehandlingar i de gemensamma tjänsterna är bedömningen av hur personuppgiftsansvaret fördelar sig svårare att göra. För dessa behandlingar krävs samverkan och en samordning av arbetet nämnder och styrelser emellan.

Förvaltningen för intrasevice rekommenderar nämnden för intraservice att hemställa till kommunstyrelsen att prioritera utredningen av vilken part som ska anses vara personuppgiftsansvarig, personuppgiftsbiträde eller om det råder delat personuppgiftsansvar. Stadsledningskontoret är av uppfattningen att detta är ett arbete som redan pågår och har svårt se att detta skulle vara ett nytt uppdrag som tillkommer. Av Intraservice bedömning framgår en rekommendation att hemställa en prioritering av ett uppdrag, men av beslutssatsen framgår det som ett nytt uppdrag som hemställan gäller.

Stadsledningskontoret bedriver arbete tillsammans med Intraservice i syfte att klarlägga hur intraservice respektive stadsledningskontoret och kommunstyrelsen ser på vissa personuppgiftsbehandlingar som involverar två eller fler nämnder och styrelser. Det handlar exempelvis om Intraservice behandlingar av personuppgifter kopplade till digital infrastruktur och säkerhet samt stadsledningskontorets och kommunstyrelsens behandlingar kopplade till vissa gemensamma system i staden. Behovet av samordning och samverkan i dessa frågor är stort. Att arbetet får fortsätta med hög prioritet är därför viktigt, liksom att även övriga nämnder och styrelser som berörs bjuds in till detta arbete. Stadsledningskontorets uppfattning är att det arbete som genomförs i samverkan mellan Intraservice och stadsledningskontoret bör kunna utgöra modell för arbetet med samordning av dataskyddsarbete i staden.

Stadsledningskontorets bedömning är att ett uppdrag till kommunstyrelsen att utreda ansvarsfördelning av personuppgiftsbehandlingar i gemensamma tjänster och tjänster tillhörande digital infrastruktur inte är nödvändigt då det finns ett pågående arbete avseende personuppgiftsansvar.

Det är även svårt för kommunstyrelsen att utreda och definiera hur en annan myndighet ska hantera och ansvara för personuppgiftbehandlingar den myndigheten gör. Det finns en risk att ansvarsfrågan gällande vem som är ansvarig att kartlägga och definiera personuppgiftsbehandlingar i stället blir otydlig, då ansvaret ska ligga på respektive nämnd eller styrelse. Det är viktigt, som redan påpekats, att respektive nämnd eller styrelse tar eget ansvar att kartlägga och bedöma hur personuppgiftsbehandlingar ska hanteras, samt att samverkan sker med andra berörda nämnder eller styrelser i de fall där ansvaret för personuppgiftsbehandlingen inte är tydligt.

Jonas Kinnander	Eva Hessman
Direktör Ärende och utredning	Stadsdirektör

Tjänsteutlåtande
Utfärdat 2023-06-12
Diarienummer 0564/22

Handläggare
Anna-Lena Björk
Telefon: 079 060 61 83
E-post: anna.bjork@intraservice.goteborg.se

Beslut om Intraservice konsekvensbedömning samt egen användning av nya intranätet Digitala Navet

Förslag till beslut

I nämnden för Intraservice

1. Godkänner konsekvensbedömningen och därmed användandet av Digitala navet för nämnden för Intraservice.
2. Förvaltningen för Intraservice uppdras att ta fram en utträdesstrategi för IT-produkter som används i gemensamma tjänster och tjänster tillhörande digital infrastruktur i de fall leverantören enligt tredje lands rättsordning kan åläggas en skyldighet att lämna ut kundens uppgifter till en myndighet i tredje land i strid med svensk rättsordning.
3. Hemställer åt kommunstyrelsen att utreda ansvarsfördelning av personuppgiftsbehandlingar i gemensamma tjänster och tjänster tillhörande digital infrastruktur

Sammanfattning

Inför att en verksamhet ska påbörja en ny personuppgiftsbehandling där det kan förekomma risker för de registrerade ska en konsekvensbedömning genomföras. Inför lansering av Digitala navet har förvaltningen nu genomfört en konsekvensbedömning för Intraservice egen användning av digitala navet.

Göteborgs stad har sedan 2019 utvecklat ett nytt intranät för stadens chefer och medarbetare. Arbetet grundar sig på tidigare genomförda analyser kring nuvarande intranät, omvärldsbevakning samt hur området som sådant har utvecklats sedan staden etablerade det nuvarande intranätet.

2016 startade ett program med syfte att införa Office 365 i staden. Arbetet syftade till att skapa förutsättningar för att jobba med en digital arbetsplats. Programmet hade som syfte att tillsammans med stadens verksamheter på bästa sättet få ut de nyttor och effekter som den digitala arbetsplatsen förväntas skapa för medarbetare och chefer.

Under tiden som arbetet med Office 365 och Digitala navet pågick förändrades de juridiska förutsättningarna för användandet av molntjänster.

Intraservice står nu inför lansering av Digitala navet som tjänst till stadens användare och därmed även ett eget användande.

Rekommendation ifrån dataskyddsombuden är att först utreda personansvarsfrågan samt att se till att tillräckliga skyddsåtgärder är på plats. Detta är utifrån de förutsättningar som finns just nu inte möjligt. Arbete pågår kring båda punkterna. Utifrån nuvarande situation med föråldrat intranät som inte lever upp till behoven vare sig utifrån teknik eller innehåll, samt behov av nya funktioner från verksamheten, finns ett stort behov att gå vidare med lanseringen samtidigt som vi jobbar vidare.

Sett till riskerna som förvaltningen identifierat och sett till behovet och nyttan landar vi i rekommendation att vi bör gå vidare med att godkänna att inleda personuppgiftshanteringen och lansera det digitala navet.

I syfte att omhänderta de risker som kopplar till tredjelandsöverföring och personuppgiftsansvar föreslår förvaltningen att nämnden ger förvaltningen i uppdrag att utreda en utträdesstrategi samt hemställa till kommunstyrelsen att utreda personuppgiftsansvarsfrågan. Dessa frågor går inte att bedöma ur tjänstens perspektiv då påföljderna påverkar hela Göteborgs stad och flertalet tjänsteleveranser inom förvaltningen och måste utredas ur ett helhetsperspektiv.

Bedömning ur ekonomisk dimension

Göteborgs Stads policy för kommunikation slår fast att staden ska arbeta på ett systematiskt och öppet sätt för att sprida information, kunskaper och erfarenheter internt och externt. Vi utvecklar och effektiviserar kommunikationen genom att använda en gemensam kommunikationsplattform för alla förvaltningar och bolag.

Digitala navet ska göra det lättare för medarbetaren att arbeta i digitala miljöer och skapa förutsättningar till att förenkla arbetet. Detta bidrar till en mer effektiv organisation och effektiva arbetssätt.

Utvecklingen av Digitala navet har tagit hänsyn till de arkitekturella principer som framgår av Göteborgs Stads riktlinje för IT- och verksamhetsarkitektur, där det bland annat framgår att staden ska återanvända arkitekturella resurser. Digitala navet baseras på Microsoft 365 plattformen som redan används av staden och det har därmed inte uppstått något behov av upphandling av särskild plattform för det nya intranätet.

Bedömning ur ekologisk dimension

Förvaltningen/bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension

Bedömning ur social dimension

Kommunikation och tillgänglighet skapar möjligheter till ökad transparens och insyn i information och beslut. Det stärker demokratin. Digitala navet är ett modernt verktyg för att ge medarbetaren tillgång till relevant och aktuell information, som hen behöver för att kunna utföra sina arbetsuppgifter. Med Digitala navet kan förvaltningen på ett bättre sätt möte de behov som tillgänglighetslagstiftningen från 2018 lyfter. Det handlar till exempel om att det finns stödverktyg som kan läsa upp information.

Ett tydligare ansvar för informationen på varje sida i Digitala navet höjer kvaliteten och aktualiteten på innehållet. Arbetet med texterna, tydligare ansvar, nya rutiner för livscykelhantering och den utökade utbildningen för redaktörerna höjer även den språkliga kvaliteten på informationen. Detta är bra för alla medarbetare, men specifik

gynnar det språksvaga grupper så som användare med svenska som andraspråk. I syfte att främja fredliga och inkluderande samhällen framgår det i mål 16.10 för Agenda 2030 att samhällen ska säkerställa allmän tillgång till information och skydde de grundläggande friheterna. Digitala navet har utvecklats för att möta behovet av kvalitetssäkrad information till stadens anställda och är därmed en del av måluppfyllnaden.

Samverkan

Ärendet samverkas i den fackliga samverkansgruppen 2023-06-15.

Bilagor

Bilaga 1 Konsekvensbedömning för personuppgiftsbehandling i Digitala navet

Bilaga 2 Bildspel

Tjänsteutlåtande 0227/21 ”Redogörelse för Intraservices arbetssätt och metod för utveckling av Kommungemensamma interna tjänster med stöd av molntjänstleverantörer”. Sammanträde 2021-06-17 § 111, 0227/21.

Protokollsutdrag nämnden för Intraservice 2022-10-26 § 211 Information om fortsatt arbete kring Office 365 som kommungemensam intern tjänst 0426/22.

Protokollsutdrag nämnden för Intraservice 2022-12-21 § 264 Arbetssätt kring Office 365 som kommungemensam tjänst och inför införande av Digitala Navet 0426/22.

Protokollsutdrag 2016-08-23 § 78 Införande av Office 365 0349/16

Protokollsutdrag 2021-06-17 § 111 Redogörelse för Intraservice arbetssätt och metod för utveckling av Kommungemensamma interna tjänster med stöd av molntjänstleverantörer

Protokollsutdrag 2022-10-26 § 210 Fördjupad analys av rapporten "Digital samarbetsplattform för offentlig sektor"

Skrivelse till nämnden för Intraservice gällande ärendet ”Intraservice egen användning av nya intranätet Digitala Navet och förvaltningar och bolags egen användning av denna tjänst” 2023-06-14

Skickas till

Kommunstyrelsen

Ärendet

Nämnden för Intraservice ska ta ställning Intraservice egen användning av Digitala Navet.

Beskrivning av ärendet

Göteborgs Stad ska ersätta det nuvarande intranätet med Digitala navet. Intranätet/Digitala navet är en av stadens tre prioriterade kanaler för kommunikation, enligt Göteborgs Stads policy för kommunikation.

Intraservice levererar intranätet/Digitala navet som en gemensam tjänst till förvaltningar och bolag i Göteborgs Stad. Intraservice är som egen förvaltning också pilot för införandeprojektet. Planen är att Intraservice ska kunna införa Digitala navet i den egna förvaltningen under oktober 2023.

Tjänsten Digitala navet levereras av avdelningen gemensamma tjänster. Förvaltningens kommunikationsavdelning leder införandeprojektet på Intraservice egen förvaltning.

Inför införandet av Digitala navet behöver nämnden ta ställning till en konsekvensbedömning av riskerna kopplat till förvaltningens personuppgiftsbehandlingar i Digitala navet.

Bakgrund

Intranätet är en av stadens prioriterade kommunikationskanaler. Hit vänder sig medarbetare bland annat för information om rättigheter, skyldigheter, arbetssätt och rutiner, nyheter och krisinformation.

Digitala navet är ett modernt verktyg för intranät och har större möjligheter än nuvarande intranät att målgruppsanpassa information. I Digitala navet finns en tydlig ämnesstruktur, som ska göra det enkelt för chefer och medarbetare att hitta information de behöver för att utföra sina arbetsuppgifter. Utöver det gemensamma innehållet i ämnesstrukturen finns aktuell information i form av nyheter och inlägg under rubrikerna Nyheter, Kommande händelser, Nytt från och Vi delar med oss. Medarbetare ser dessa inlägg utifrån organisatorisk tillhörighet, roll eller hur redaktören har valt att tagga inlägget.

Syftet med Digitala navet är att skapa nyttor för medarbetare, chefer och förvaltningen genom att:

- tillgängliggöra information om arbetssätt, rättigheter och skyldigheter kopplat till anställning, stöd och support i arbetet, pågående uppdrag och förändringar i staden.
- möjliggöra för medarbetare att kunna ta del av aktuell information på förvaltningen och för hela Göteborgs Stad.
- möjliggöra informationsspridning vid kris eller större händelse.
- samla länkar och enkel tillgång till verktyg och IT-stöd.

- tillgängliggöra information om stadens organisation och struktur samt kontaktpersoner för olika frågor.
- stärka och bygga den gemensamma bilden av Göteborgs Stad.

I nuvarande intranät finns brister:

- Strukturen gör det svårt att kvalitetssäkra innehållet. Det saknas också rutiner för livscykel hantering och gallring. Det gör innehållet mindre pålitligt.
- Det är svårare och tar längre tid att hitta information. Den är uppdelad på flera ställen och sökfunktionen är sämre. Det gör den mindre effektiv för medarbetarna att använda.
- Verktyget är långsamt och opålitligt. Det gör det mindre effektiv att arbeta med.
- Varken verktyget eller arbetssätten uppfyller de krav som ställs på tillgänglighet enligt Lag om tillgänglighet i digital offentlig service (2018:1937).

Innehållet och informationen i Digitala navet håller högre kvalitet än det nuvarande intranätet och uppfyller också lagkraven på tillgänglighet. För redaktörerna är verktyget också pålitligare och mer smidigt att arbeta i än nuvarande intranät. Digitala navet innebär också förutsättningar för mer effektiva arbetssätt för kommunikation i staden. Nuvarande intranät innebär en mängd dubbelpublicering, eftersom varje förvaltning behöver publicera till exempel HR-information på egna sidor. Digitala navet bygger på gemensamt innehåll för staden och minskar därmed det administrativa arbetet med att publicera och uppdatera information på sidorna.

Utvecklingen av Digitala Navet

Under 2019 - 2020 genomfördes en förstudie med syfte att skapa förutsättningar för utveckling av ett nytt intranät i Göteborgs Stad. Arbetet tog sin utgångspunkt i tidigare genomförda förstudier samt en omvärldsbevakning, som även analyserade på hur andra organisationer arbetat med liknande projekt.

Inom ramen för förstudien gjordes också en analys kring hur intranät som förekomst har förändrats från att vara till största delen en sändande kanal till att bli en mer integrerad del i en digital arbetsplats. Utifrån förstudien startades ett utvecklingsprojekt. I samband med uppstarten sommaren 2020 formulerades två effektmål för projektet:

- Medarbetare och chefer upplever det digitala navet som mer relevant, aktuellt och funktionellt än det gamla intranätet.

- Det digitala navet bidrar till att göra det lättare för medarbetaren att arbeta i digitala miljöer och skapar förutsättningar till att förenkla arbetet.

Effektmålen förtydligades i följande nyttor:

- Lätt att hitta, agera och göra rätt
- Tillgång och koll på informationsflödet
- Bidra till att förenkla, effektivisera vardagen
- Veta vad som gäller i Staden
- Effektivare innehållsproduktion, minskad dubbel publicering
- Lättare att dela och samarbeta kring information

Val av Sharepoint som plattform för nytt intranät

I förstudien undersökte deltagarna hur utveckling av ett intranät kan genomföras. Förstudien undersökte möjligheter att utveckla en helt egen lösning samt alternativ för att köpa in färdig lösning från leverantör.

En faktor som förstudien hade att ta hänsyn till var det arbete som Intraservice påbörjade 2016 tillhörande införandet av tjänsten Office 365 som kommungemensam tjänst (§ 78, 0349/16). Införandet av Office365 var en del i att börja bygga en modern digital arbetsplats. Genom Office365 fick Göteborgs Stad tillgång till plattformen Sharepoint, som, förutom funktioner för dokumenthantering, även har funktioner för att utveckla ett modernt intranät.

Förstudien kom fram till att Intraservice själva skulle utveckla en lösning för intranät som baserades på Sharepoint. Lösningen skulle så långt möjligt använda standardfunktioner inom Microsofts lösningar. Förstudiens slutsats grundade sig på att det var det ekonomiskt bästa alternativet, samt att det också medförde att Intraservice inte skulle vara beroende av en extern leverantör som levererade en färdig systemlösning.

Schrems II-domen

Arbetet med att bygga det nya intranätet startade upp under hösten 2020 som ett tjänsteplansprojekt. Under sommaren 2020 föll den så kallade Schrems II-domen. Följden av detta blev en förändring av det juridiska skydd som tidigare funnits gällande dataöverföring med länder utanför EU/EES, bland annat USA.

I Sverige innebar Schrems II-domen att organisationer hade nya risker att ta ställning till. Ett antal organisationer valde att pausa/stoppa sina införande av lösningar som vars leverantörer hade sin hemvist i länder utanför EU/EES. Detta eftersom de bedömde det juridiska läget som alltför osäkert för att kunna införa dessa lösningar, exempelvis lösningar som levereras av Microsoft eftersom företaget är från USA.

De organisationer som redan infört lösningar såsom Office 365 behövde utreda om hur riskerna påverkar användandet. Alternativa lösningar eftersöktes och eSam började hösten 2021 arbeta med en rapport vars syfte var att presentera alternativa lösningar (se avsnitt Omvärldsbevakning).

I Göteborgs Stad är Office365 en kommungemensam intern tjänst sedan 2017. Schrems II-domen medförde att det fanns behov av att utreda hur riskerna påverkade användandet av tjänsten.

Intraservice arbetade med att analysera konsekvenserna av Schrems II samtidigt som Digitala navet fortsatte att utvecklas (§ 111, 0227/21). I analysarbetet tog Intraservice hänsyn till att Göteborgs Stad använt Office 365 sedan 2016 och att staden genomfört stora investeringar både i form av teknik och kompetens. Analysen tog också hänsyn till arbetssätt och användning, samt att flera verksamhetssystem hade etablerade integrationer med tjänsten Office 365. I analysen fastslogs att rättsläget kring användning av produkter som innebär tredje landsöverföring till USA var oklart. Förvaltningen bedömde i sitt utlåtande att “Office 365 är av sådan vikt för Intraservice och Göteborgs Stads verksamhet att den måste fortsätta användas trots (...) beskrivna risker.” I övrigt fastslog förvaltningen att det är upp till varje enskild personuppgiftsansvarig att bedöma om de risker som förknippas med tredjelandsöverföringen innebär att användningen av Office 365 måste upphöra.

Juridiska frågeställningar att ta hänsyn till

Juridisk bakgrund

Digitala navet vilar på plattformen Office 365, som är en molntjänst, som levereras av det amerikanska bolaget Microsoft. Offentliga myndigheters möjligheter att nyttja molntjänster från privata leverantörer på ett sätt som är förenligt med lag har givit upphov till diskussion som alltjämt är aktuell. Frågan i sig är bred och berör flera områden och juridiska frågeställningar, vilka också överlappar varandra där samma omständigheter har påverkan på flera områden och olika juridiska bedömningar. De olika frågeställningarna kan i huvudsak delas in i tre områden ur ett juridiskt perspektiv.

1. Tredjelandsöverföring (dataskyddsförordningen)

Frågeställningen gäller huruvida det är möjligt att använda molntjänstleverantörer som personuppgiftsbiträden för behandling av myndighetens personuppgifter, om leverantörens behandling av personuppgifterna innefattar en överföring av alla eller delar av personuppgifterna till ett tredje land (i dataskyddsförordningens mening ett land utanför EU/EES).

2. Bedömning av ett personuppgiftsbiträde (dataskyddsförordningen)

Frågeställningen gäller huruvida det är förenligt med dataskyddsförordningen att använda molntjänstleverantörer som lyder under lagstiftning i ett tredje land (ett land utanför EU/EES) som personuppgiftsbiträden, om leverantören enligt det tredje landets lagstiftning kan åläggas en skyldighet att lämna ut kundens uppgifter till en myndighet i det tredje landet. Det exempel som ofta lyfts fram är huruvida det är förenligt med dataskyddsförordningen att anlita en leverantör som på grund av koncernförhållande eller egen hemvist i USA lyder under amerikansk rätt såsom den så kallade CLOUD Act.

3. Röjandefrågan (Offentlighets- och sekretesslagen)

Frågeställningen gäller huruvida uppgifter röjs i offentlighets- och sekretesslagens (OSL) mening när de lämnas över till leverantören av en molntjänst. Detta får betydelse när stadens verksamheter i sin roll som myndighet ska behandla uppgifter i sådana molntjänster som nyttjas av staden som gemensamma tjänster och tjänster tillhörande digital infrastruktur.

Eventuella nya sekretessbrytande regler

Regeringen har på rekommendation från SOU 2021:97 - Säker och kostnadseffektivt it-drift lagt en proposition om sekretessbrytande regler för utkontraktering av IT-drift. I förslaget föreslås en ny generell sekretessbrytande regel införas i 10 kap. Offentlighets- och sekretesslagen (OSL) som medger att en myndighet överför sekretessuppgifter till annan myndighet eller organisation under förutsättningen att den mottagande myndigheten eller organisationen endast hanterar uppgifterna för teknisk bearbetning eller lagring.

Den nya sekretessbrytande regeln är unik i bemärkelsen att utlämnande inte förutsätter en noggrann prövning av om enskilda uppgifter i handlingarna omfattas av sekretess. Istället ska den utlämnande myndigheten genomföra en lämplighetsbedömning av utlämnandet av uppgiftsmängden i sin helhet. I författningskommentaren framgår att en sådan lämplighetsbedömning ska ha formen av en allriskbedömning och bland annat bör omfatta risk för att utlämnande myndighet förlorar kontroll över uppgiftsmängden i

förhållande till annan rättsordning, den allmänna cybersäkerheten hos mottagande organisation och uppgifternas samlade värde för den utlämnande organisationen.

Lagen föreslås träda i kraft den 1 juli 2023. Efter det behöver myndigheterna inom Göteborgs Stad genomföra ovan nämnda lämplighetsbedömning i förhållande till Intraservice och Microsoft som leverantör. Beroende på resultatet av lämplighetsbedömningarna finns det efter 1 juli möjlighet för Göteborgs Stad att lämna ut uppgifter som omfattas av sekretess till extern leverantör, i detta fall Microsoft.

Om lämplighetsbedömningen visar att det för hela eller delar av uppgiftsmängden föreligger hinder för utlämning behöver alternativa bearbetnings- och lagringslösningar införskaffas. Lämpligtvis bör Intraservice därför redan nu påbörja färdigställandet av en utträdesstrategi för de molntjänster som kan vara problematiska ur ett röjandeperspektiv.

Omvärldsbevakning

Nytt ramverk som skydd för tredjelandsöverföring

EU-kommissionen genomför just nu en process för godkännande av det nya ramverket EU-US data privacy framework. Godkännandet av ramverket förväntas vara klart i juli 2023. Om ramverket kommer på plats kan det komma att innebära en tillräcklig skyddsnivå för tredjelandsöverföring. Ramverket skulle i så fall innebära att risken för tredjelandsöverföring inte längre är problematisk ur ett dataskyddsperspektiv.

Intraservice förvaltning följer kontinuerligt utvecklingen på området och återkommer till nämnden när ny information uppkommer.

eSam

Nämnden för Intraservice beslutade 2022-05-25 § 133 att ge förvaltningen i uppdrag att genomföra en analys av rapporten ”Digital sammararbetsplattform för offentlig sektor” som publicerats av eSam under 2021. Beslutet grundade sig på ett yrkande från politiker. eSam är ett medlemsdrivet program för samverkan mellan 34 myndigheter. Samverkansprogrammet syftar till att utreda och ta fram rättssäkra digitala lösningar riktade mot privatpersoner och företag. Programmet samverkar också digitala lösningar för myndigheters utveckling och effektivisering.

Förvaltningen har genomfört en analys utifrån beslutet och i enlighet med intentionen i yrkandet.

Rapporten ”Digital samarbetsplattform för offentlig sektor” är en övergripande analys och ögonblicksbild över marknaden för tillgängliga lösningar för samarbetsplattformar för offentlig sektor.

Förvaltningens analys pekade på att eSams rapport inte tar upp de fulla konsekvenserna av att ersätta redan befintliga system eller ekosystem av tjänster. Utredning av detta behöver varje enskild organisation själva genomföra. Rapporten svarar heller inte på vilka typer av kostnader som en övergång till andra lösningar för med sig.

Pågående arbete kopplat till PUB-PUA

Sedan 1 januari 2023 har staden en ny styrmodell för digital utveckling och förvaltning. Intraservices ansvar som leverantör regleras nu främst i Göteborgs Stads riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltning. Riktlinjen reglerar även roller och ansvar för utveckling, förvaltning och användning av gemensamma tjänster och tjänster tillhörande digital infrastruktur.

I den tidigare styrmodellen hade Intraservice enligt praxis rollen som personuppgiftsbiträde (PUB) för det som då kallades kommungemensamma interna tjänster. De verksamheter som använde tjänsterna ansågs vara personuppgiftsansvariga (PUA) för de personuppgifter som Intraservice behandlar inom tjänsten. Intraservice har därutöver varit personuppgiftsansvarig när förvaltningen själv använder en tjänst.

Denna praxis gäller inte längre i den nya styrmodellen. Sedan hösten 2022 pågår ett arbete med att utreda ansvarsfrågan för varje tjänst som Intraservice levererar till förvaltning och bolag i Göteborgs Stad. Målet är att för varje personuppgiftsbehandling inom respektive tjänst fastställa rollerna som personuppgiftsansvarig, personuppgiftsbiträde eller om det råder delat personuppgiftsansvar.

Fördelning av ansvar och roller

Intraservice har en pågående dialog med stadsledningskontoret gällande ansvarsfördelningen. I korthet uppstår en konflikt mellan de uppdrag kring säkerhet och utförande av tjänster som framgår av Intraservice reglemente och rollen som personuppgiftsbiträde. Intraservice är ansvarig för säkerheten i de gemensamma tjänsterna och IT-infrastrukturen men kan utifrån sin roll som personuppgiftsbiträde inte besluta om säkerhetsåtgärder som omfattar personuppgifter utan godkännande från samtliga nämnder och bolag.

Säkerhet i Göteborgs Stads IT-miljö utgår från ett holistiskt perspektiv. I arbetet med konsekvensbedömning och tillhörande riskanalyser för Digitala navet har projektet identifierat oklarheter kring ansvarsfördelning gällande personuppgiftsbehandlingar. Det är inte möjligt att ha särlösningar för enskilda nämnder och bolag, eftersom det skulle riskera säkerheten för övriga nämnder och bolag och för Intraservices IT-miljö som helhet. Intraservice måste kunna garantera att cybersäkerhetshot kan ageras på skyndsamt, i vissa fall inom ett par timmar. Ett förfarande där en eventuell säkerhetsåtgärd som omfattar personuppgifter behöver godkännas av samtliga nämnder och bolag riskerar att försena åtgärden.

Riskanalys och konsekvensbedömning

Intraservice som förvaltning

Riskanalys

När Intraservice i sin roll som tjänsteleverantör anlitar andra leverantörer, behöver förvaltningen bland annat ta ställning till och bedöma risker. Bedömningen av en viss leverantör, ett visst system eller leveranssätt från juridiskt perspektiv påverkas av ett flertal faktorer. Det handlar om allt ifrån vilken information och data som leveransen innehåller, vilken teknik som används, var data och information hanteras geografiskt, vilken leverantör vi har att göra med och vilka garantier som denne kan lämna, vilka säkerhetsåtgärder som är vidtagna eller som kan vidtas, med mera.

För en adekvat juridisk bedömning måste de faktiska omständigheterna för den enskilda tjänsten bedömas, både vid införandet och sedan löpande under tiden som tjänsten används. Sådana bedömningar ska göras för varje gemensam tjänst och tjänster tillhörande digital infrastruktur, för att uppfylla krav som ställs i lag, men också de krav som ställs kring ansvar, roller, hantering och beslut i stadens styrande dokument.

Ansvaret för att göra sådana bedömningar eller ge underlag till sådana bedömningar vilar till stor del på Intraservice som tjänsteleverantör och personuppgiftsbiträde. En riskanalys i dataskyddsförordningens mening innebär att man utgår från risker som kan drabba den registrerade. I denna riskanalys tas ingen hänsyn till risker som kan komma att drabba personuppgiftsansvarig eller personuppgiftsbiträde.

Riskbedömning utifrån andra perspektiv

Men det finns också bedömningar som måste göras och beslut som måste fattas av de personuppgiftsansvariga förvaltningar och bolag som kravställare och användare av tjänsten. Vid sidan av riskbedömning utifrån den registrerades perspektiv måste stadens verksamheter även ta ställning till andra delar, såsom utförande av det kommunala uppdraget och verksamheten som helhet. En riskbedömning från verksamhetens perspektiv innehåller även dessa perspektiv och behöver beakta åtaganden, lagstiftningar och förutsättningar som verksamheten omfattas av.

Det ska vara tydligt dokumenterat hur förvaltningen gör dessa bedömningar, både ur perspektivet som tjänsteleverantör och som användare och därmed personuppgiftsansvarig. Bedömningen bör beakta risk utan tjänst, risk med nuvarande tjänst och risk med införande av annan tjänst.

I samband med att bedömningar görs, eller då beslut ska fattas, ska Intraservices dataskyddsombud involveras och rådfrågas. I sin roll som tjänsteleverantör ska Intraservice även ge underlag till personuppgiftsansvariga förvaltningar och bolag som använder Intraservices tjänster som stödjer sig på så kallade molntjänstleverantörer. Detta för att förvaltningar och bolag som använder Intraservice tjänster ska kunna uppfylla sina åtaganden enligt artikel 28 i GDPR.

Artikel 28 i GDPR anger att om en behandling ska genomföras på en personuppgiftsansvarigs vägnar ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden (i detta fall Intraservice) som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att

behandlingen uppfyller kraven i denna förordning och säkerställer att den registrerades rättigheter skyddas.

Riskanalys dataskydd för Digitala navet

I sin roll som tjänsteleverantör har Intraservice genomfört en riskanalys dataskydd för tjänsten Digitala navet (se bilaga Digitala navet riskanalys dataskydd). Riskanalysen visar att tjänsten Digitala navet i stort sett delar de risker som finns för den underliggande tjänsten Office365. För risker kopplat till Office365 som underliggande tjänst, se *Office 365 Riskanalys dataskydd.* I riskanalysen för Digitala navet har arbetet med riskanalysen fokuserat på de underliggande risker som är förknippade med användningen av Office365, avgränsat till de funktioner som stödjer Digitala navet.

I riskanalysen för Digitala navet har Intraservice tagit hänsyn till hela användarprocessen, från anställning, upprättande av identitet, skapande av staden-konto och efterföljande hantering i användarkataloger, som är en förutsättning för att stadens användare ska kunna använda Digitala navet.

I riskanalysen har Intraservice identifierat 29 risker kopplade till Digitala navet (se bilaga 2). Två av dessa risker bedöms vara av sådan art att de på något sätt behöver åtgärdas eller på annat sätt omhändertas.

1. Risk kopplade till användare med sekretessmarkering
2. Risk kopplat till Microsofts nyttjande av underbiträdande som tekniskt kan ta del av Stadens personuppgifter.

Utöver ovanstående risker innebär ett användande av Digitala Navet att tjänsten ärver de risker som identifierats för den underliggande tjänsten Office 365:

1. Införandet av Digitala navet innebär en fortsatt användning av Office365.
2. Oklara roller för personuppgiftsbiträde och personuppgiftsansvarig. Det behöver redas ut och fastställas vilken part som är ansvarig för de personuppgiftsbehandlingar som förekommer i de tjänster som Digitala navet bygger på och är beroende av.

Konsekvensbedömnning Digitala navet

Konsekvensbedömningen hanterar perspektivet Intraservices personuppgiftsbehandling i Digitala navet i rollen som *användare* av tjänsten Digitala navet – inte personuppgiftsbehandling i rollen som tjänsteleverantör av tjänsten Digitala navet. Eftersom Intraservice har båda rollerna (användare och tjänsteleverantör) är det viktigt att hålla isär perspektiven för att lättare förstå vilken personuppgiftsbehandling man syftar på.

Konsekvensbedömningen utgår från riskbedömning som redovisar 35 risker (se bilaga 1 konsekvensbedömning).

Riskhantering har skett i två omgångar:

Risker 1–6 hanterades i december 2022 och januari 2023

Risker 7–35 hanterades under maj (4,5, 8 och 15 maj 2023)

Riskerna är indelade i risker för Intraservice som personuppgiftsansvarig (PUA) och risker för Intraservice som personuppgiftsansvarig för den egna förvaltningen men personuppgiftsbiträde (PUB) för andra förvaltningar.

Risker för Intraservice som PUA: risker kopplade till personuppgiftsbehandlingen Informera och kommunicera i Digitala navet gäller enbart Intraservice som egen förvaltning. Dessa risker behöver andra verksamheter ta ställning till för sitt eget innehåll i Digitala Navet.

Risker för Intraservice som PUA i den egna förvaltningen men PUB för andra: risker kopplade till personuppgiftsbehandlingen Tillhandahålla och utveckla Digitala navet är risker som är relaterade till Intraservice tjänst (inkluderat cybersäkerhet) och för att stödja eventuellt riskidentifiering av andra verksamheter gällande egna ställningstaganden för användning av Digitala Navet.

Riskerna med publicering av personuppgifter i Digitala navet bedöms som låga utifrån att det inte är några känsliga personuppgifter som publiceras.

Lansering av digitala navet innebär fortsatt användning av den etablerade tjänsten Office 365 och risker kopplat till den tjänsten. Dessa risker beskriv i Riskanalys Office 365, där risker kring bland annat ”tredjelandsöverföring” finns. Risker kopplade till de underliggande tjänsterna berör hela staden. De kan inte bedömas enskilt utifrån Digitala navet utan tillhör den samlade riskbilden för Intraservice som förvaltning och tjänsteleverantör.

I konsekvensbedömningen för Digitala navet bedöms följande risker som kvarstående med hög risk:

Risk 17 – Spridning av data till olämpliga underleverantörer på grund av ensidig förändring av vilka underleverantörer de använder, med dålig transparens från Microsofts sida, är värderad utifrån antagandet att uppgifter kunde överföras till Kina. Risken är under utredning.

Risk 10 – Personer inom Intraservice som får sekretessmarkering under sin anställning riskerar att synliggöras (möjliga att identifiera). Risken är under utredning och förslag finns på åtgärder som minskar risken.

Risk 5 – Lansering av digitala navet innebär fortsatt användning av Office 365 och dess underliggande risker.

Intraservice som tjänsteleverantör

Intraservice har beskrivit rättsläget kring användande av molntjänster och överföring av personuppgifter till tredje land i ett tidigare tjänsteutlåtande (diarienummer 0227/21 *Redogörelse för Intraservice arbetssätt och metod för utveckling av Kommungemensamma interna tjänster med stöd av molntjänstleverantörer*, daterat 2021-05-25). I detta tjänsteutlåtande beskrevs också konsekvenserna av att avsluta eller begränsa användande av de molntjänster som nyttjas av staden i kommungemensamma interna tjänster.

Förvaltningen står 2023 inför motsvarande utmaningar som vid tidpunkten då föregående tjänsteutlåtande presenterades för nämnden för Intraservice. I det tidigare tjänsteutlåtande (maj 2021) informerades nämnden för Intraservice om förslag till arbetssätt och metodik för att hantera utmaningar i samband med användande av molntjänster i kommungemensamma interna tjänster.

I oktober 2022 informerade förvaltningen nämnden för Intraservice om fortsatt arbete kring Office 365 som kommungemensam intern tjänst. (2022-10-26 § 211, 0426/22) Nämnden fick då information om att det i samband med uppdateringen av riskanalysen för tjänsten Office365 hade konstaterats att tjänstedokumentationen för behövde kompletteras med beskrivning av de personuppgiftsbehandlingar, risker och säkerhetsåtgärder som är kopplade till dessa. Sedan november 2022 pågår ett för Intraservice nytt arbetssätt. Detta nya arbetssätt har tagits fram i samråd med tjänsteorganisationen internt på Intraservice och dataskyddsombud.

Arbetssätt för molntjänster

Det arbetssätt som förvaltningen använder sig av sedan november 2022 kopplat till utveckling och leverans av gemensamma tjänster och tjänster tillhörande digital infrastruktur som stödjer sig på så kallade molntjänstleverantörer, har sin grund i de krav som ställs på Intraservice tjänsteleverans. Förvaltningens tjänster ska både säkerställa att Göteborg Stad kan bedriva de verksamheter som staden är förpliktigad att bedriva enligt lag, och att verksamheterna kan leva upp till de krav som finns i den lagstiftning som tjänsterna omfattas av.

Enligt detta arbetssätt ska Intraservice i första hand använda inomeuropeiska molntjänster. Men inom ramen för de gemensamma tjänsterna och tjänsterna tillhörande digital infrastruktur förekommer icke-europeiska alternativ. Dessa tjänster är förknippade med integritetsrisker som kontinuerligt måste utvärderas, reduceras eller så långt det är möjligt elimineras.

Utifrån ovanstående beskrivna läge har förvaltningen kommit fram till följande arbetssätt kopplat till utveckling och leverans av gemensamma tjänster och tjänster tillhörande digital infrastruktur som stödjer sig på så kallade molntjänstleverantörer.

1. Intraservice ska inom ramen för sin leverans av gemensamma tjänster och tjänster tillhörande digital infrastruktur fortsätta leverera och nyttja molntjänster som innebär och kan innebära att lagefterlevnad ej kan säkerställas i samband med tredjelandsöverföring av personuppgifter, om sådana tjänster uppfyller följande krav:

a. Mottagande verksamhet har fattat beslut om fortsatt leverans och nyttjande. Detta beslut gäller i så fall tills vidare.

b. Nyttjandet av tjänsterna begränsas enligt punkt 2 - 6 nedan.

2. Intraservice ska fortsätta arbetet med att utreda, analysera och riskbedöma säkerheten, samt tydliggöra brister i följsamhet till lag avseende leverans av molntjänster med risk för eller konstaterad tredjelandsöverföring enligt punkt 1, och om möjligt åtgärda identifierade säkerhetsrisker.

3. Där det inte går att införa kompletterande skyddsåtgärder, som kan garantera en adekvat personuppgiftshantering, ska Intraservice fortsätta arbetet med att utreda, analysera och riskbedöma säkerheten och tydliggöra eventuella brister i följsamhet till lag avseende alternativa tjänster till redan befintliga molntjänster med risk för eller konstaterad tredjelandsöverföring.

4. Intraservice ska begränsa leverans och nyttjande av redan införda molntjänster med risk för eller konstaterad tredjelandsöverföring så att endast information som inte omfattas av sekretess eller utgör känsliga personuppgifter hanteras i dessa tjänster. Verksamheter som använder sådana molntjänster ska informeras om detta.

5. Intraservice ska avveckla molntjänster med risk för eller konstaterad tredjelandsöverföring som inte längre kan användas enligt bedömning gjord enligt punkt 1 ovan.

6. Intraservice ska inte införa fler molntjänster som innebär och kan innebära att lagefterlevnad ej kan säkerställas i samband med tredjelandsöverföring av personuppgifter, om inte

    a. det är absolut nödvändigt för verksamheten,

    b. inga andra rimliga alternativ finns att tillgå

    c. mottagande verksamhet har fattat beslut om leverans och nyttjande.

Fortsatt användning av molntjänster under vissa förutsättningar

Ovanstående arbetssätt utgår från dem vi är till för - förvaltningar och bolag i Göteborgs Stad - i förlängningen medborgarna som ska kunna förvänta sig en god kommunal service. Intraservice ska ha fortsatt förmåga att leverera tjänster i enlighet med förvaltningens uppdrag, samtidigt som vi i så stor utsträckning som möjligt beaktar och agerar på de risker och aspekter som finns med molntjänster där det kan konstateras att överföring sker av personuppgifter till tredje land, eller där risk finns för detta.

Detta innebär att fortsatt användning av tjänster som stödjer sig på molntjänstleverantörer kan ske under vissa förutsättningar. Utvecklingen av Digitala navet påbörjades innan ovanstående arbetssätt togs fram. Digitala navet vilar på den befintliga tjänsten Office365 och innebär alltså inte en ny molntjänstleverantör för Göteborgs Stad.

Arbetet med att finna hållbara lösningar framöver fortgår, både inom staden och på nationell och internationell nivå. Förvaltningen arbetar kontinuerligt med omvärldsbevakning och olika alternativ tas fram, analyseras och bedöms utifrån hur rättsläget utvecklas.

Utträdesstrategi

I enlighet med Stadens riktlinjer för informationssäkerhet ska nämnder och bolag säkerställa att en avvecklings eller utträdesstrategi upprättas redan i samband med anskaffande av IT-stöd. Digitala navet och Microsoft 365 saknar idag en sådan strategi. Digitala navet är en tillämpning av Sharepoint som staden själva har utvecklat och det finns därför anledning att tillämpa kravet om utträdesstrategi på den underliggande plattformen istället för på intranätet som sådant. En utträdesstrategi för Microsoft 365 bedöms inte rymmas inom mandatet för projektet för Digitala navet och bör därför upprättas i särskild ordning.

Förvaltningen bedömer att en utträdesstrategi för molntjänster bör upprättas i förebyggande syfte för de IT-produkter som riskerar att utsätta Stadens information för främmande rättsordning. En utträdesstrategi innebär att Staden har valmöjligheter vid förändrat omvärldsläge, förändrad lagstiftning eller vid väsentliga förändringar i produkten från leverantören som är oacceptabla utifrån Stadens riktlinjer och politiska mål. I dagsläget har Intraservice ingen plan för hur ett eventuellt utträde ur enskilda företags IT-lösningar skulle kunna genomföras. Det innebär i förlängningen att Staden agerar reaktivt vid ny lagstiftning eller produktförändringar i stället för att kunna ställa krav och vara proaktiva.

Förvaltningens bedömning

Inför införande av det nya intranätet Digitala navet har Intraservice genomfört riskanalys och konsekvensbedömning.

Konsekvensbedömningen utgår från Intraservices egen användning av Digitala navet och presenterar vilka risker som finns med att behandla personuppgifter inom ramen för Digitala navet och de underliggande delarna i tjänsten Office 365. Konsekvensbedömningen anger därtill vilka åtgärder som vidtas för att hantera de risker som riskanalys påvisat tillhörande Digitala navet. Konsekvensbedömningen hanterar inte de risker som är kopplade till de underliggande tjänsterna i Office 365, eftersom dessa risker inte kan hanteras enskilt utifrån Digitala navet. Dessa risker måste hanteras utifrån hela tjänsteleveransen Office 365.

Nämnden för Intraservice behöver ta ställning till genomförd konsekvensbedömning och de föreslagna personuppgiftsbehandlingarna. Ett godkännande vilar på att nämnden accepterar de tre kvarstående riskerna som identifierats i konsekvensbedömningen samt de ej ännu genomförda riskåtgärderna.

Nämnden för Intraservice behöver ta ställning till Intraservices egen användning av Digitala navet. Ett godkännande innebär att nämnden för Intraservice accepterar det arbetssätt tillhörande molntjänster som finns beskrivet i detta tjänsteutlåtande.

Ett godkännande innebär även att nämnden för Intraservice accepterar att ansvarsförhållanden är fortsatt oklara tills dess att detta är utrett och fastställt. Med oklara ansvarsförhållanden avses frågan vilken part som ska anses vara personuppgiftsansvarig, personuppgiftsbiträde eller om det råder delat personuppgiftsansvar.

En återremittering av ställningstagandet till Intraservice egen användning av Digital Navet innebär fortsatt användning av det nuvarande intranätet, med de tekniska och redaktionella skulder det innebär.

Intraservice har idag ingen rekommenderad alternativ plattform för ett nytt intranät. Arbetet med att byta ut intranätet skulle då börja om från början med en ny förstudie som utreder lämpliga alternativ.

Risken med att inte gå vidare är också att stadens verksamheter i stället för att fortsätta använda gamla intranätet försöker skapa sig egna parallella intranät. En sådan situation, med flera egna separata intranät riskerar att skapa ytterligare merkostnader för staden som helhet. Det underminerar också en av stadens prioriterade kommunikationskanaler och en av våra prioriterade kommunikationskanaler vid kris. Medarbetarna riskerar då att inte nås av viktig information.

Förvaltningen rekommenderar också att nämnden för Intraservice ger förvaltningen i uppdrag att ta fram en utträdesstrategi kring fortsatt användning av tjänsten Office365 och användningen av molntjänster.

Förvaltningen rekommenderar därutöver att nämnden för Intraservice hemställer till kommunstyrelsen att prioritera utredningen av vilken part som ska anses vara personuppgiftsansvarig, personuppgiftsbiträde eller om det råder delat personuppgiftsansvar.

Malin Lundqvist
Avdelningschef digital infrastruktur

Peter Söderström
Förvaltningsdirektör

Utdrag ur Protokoll
Sammanträdesdatum: 2023-06-21

Beslut om Intraservice konsekvensbedömning samt egen användning av nya intranätet Digitala Navet

§ 127, 0564/22

Beslut

I nämnden för Intraservice

1. Godkänner konsekvensbedömningen och därmed användandet av Digitala navet för nämnden för Intraservice.
2. Förvaltningen för Intraservice uppdras att ta fram en utträdesstrategi för IT-produkter som används i gemensamma tjänster och tjänster tillhörande digital infrastruktur i de fall leverantören enligt tredje lands rättsordning kan åläggas en skyldighet att lämna ut kundens uppgifter till en myndighet i tredje land i strid med svensk rättsordning.
3. Hemställer åt kommunstyrelsen att utreda ansvarsfördelning av personuppgiftsbehandlingar i gemensamma tjänster och tjänster tillhörande digital infrastruktur

Underlag för beslut

Tjänsteutlåtande 2023-06-12

Bilaga 1 Konsekvensbedömning för personuppgiftsbehandling i Digitala navet

Bilaga 2 Bildspel

Tjänsteutlåtande 0227/21 ”Redogörelse för Intraservices arbetssätt och metod för utveckling av Kommungemensamma interna tjänster med stöd av molntjänstleverantörer”. Sammanträde 2021-06-17 § 111, 0227/21.

Protokollsutdrag nämnden för Intraservice 2022-10-26 § 211 Information om fortsatt arbete kring Office 365 som kommungemensam intern tjänst 0426/22.

Protokollsutdrag nämnden för Intraservice 2022-12-21 § 264 Arbetssätt kring Office 365 som kommungemensam tjänst och inför införande av Digitala Navet 0426/22.

Protokollsutdrag 2016-08-23 § 78 Införande av Office 365 0349/16

Protokollsutdrag 2021-06-17 § 111 Redogörelse för Intraservice arbetssätt och metod för utveckling av Kommungemensamma interna tjänster med stöd av molntjänstleverantörer

Protokollsutdrag 2022-10-26 § 210 Fördjupad analys av rapporten "Digital samarbetsplattform för offentlig sektor"

Skrivelse till nämnden för Intraservice gällande ärendet ”Intraservice egen användning av nya intranätet Digitala Navet och förvaltningar och bolags egen användning av denna tjänst” 2023-06-14

Protokollsutdrag skickas till

Kommunstyrelsen

Dag för justering

2023-06-26

Vid protokollet

Sekreterare

Angela Moussallem

Ordförande

Bertil Lidfeldt (S)

Justerande

Henrik Sjöstrand (M)