Göteborgs Stad

2023-06-14 Nämnden för Intraservice

Skrivelse till nämnden för Intraservice gällande ärendet ”Beslut om Intraservice konsekvensbedömning samt egen användning av nya intranätet Digitala Navet”

Dataskyddsombudet är i sin roll skyldig att rapportera risker till högsta beslutsnivå. Det ingår i dataskyddsombudets ansvar att informera nämnden för Intraservice om bland annat risker för de personer vars personuppgifter behandlas (registrerade), som dataskyddsombudet uppmärksammar inom sitt uppdrag. Utifrån detta ansvar har dataskyddsombudet sammanställt denna skrivelse gällande ärendet ”Beslut om Intraservice konsekvensbedömning samt egen användning av nya intranätet Digitala Navet” (dnr 0564/22). Dataskyddsombudet vill med denna skrivelse informera nämnden dels om de risker för registrerade som dataskyddsombudet identifierat inom ramen för förvaltningens arbete med det digitala navet, dels om de risker för sanktionsavgifter som följer av att nämnden inte följer dataskyddsförordningen.

Ärendet

Förvaltningen för Intraservice har påbörjat ett arbete med en konsekvensbedömning avseende dataskydd för de personuppgiftsbehandlingar som införandet av det nya intranätet i staden innebär. Dataskyddsombudet är involverad i detta arbete[2] och har, enligt gängse process, lämnat en första omgång synpunkter på det framtagna underlaget (7/6 2023). Då förvaltningen valt att gå vidare med ärendet och föreslå nämnden att besluta om att godkänna konsekvensbedömningen innan underlaget färdigställts, och dataskyddsombudet kunnat lämna slutliga rekommendationer, bedömer dataskyddsombudet det nödvändigt att ställa en skrivelse till nämnden i ärendet. Detta utifrån att nuvarande underlag visar på att behandlingen medför höga risker för de registrerade, vilka förvaltningen ej kunnat presentera skyddsåtgärder för. Rekommendationerna i denna skrivelse är baserade på version 0.9 av konsekvensbedömningen (daterad 2023-05-24).

Tidigare lämnade rekommendationer

Dataskyddsombudet har sedan tidigare lämnat flera rekommendationer med relevans för såväl Digitala Navet som ärendet som helhet:

- September 2020: ”Information till personuppgiftsansvariga styrelser och nämnder med anledning av EU-domstolens dom i mål C-311/18 (Schrems II-målet)” till samtliga förvaltningar och bolag i Göteborgs Stad. Uppdatering maj 2022 med ytterligare rekommendationer för hanteringen av tredjelandsöverföringar efter

[2] Enligt artikel 35.2 GDPR ska den personuppgiftsansvarige rådfråga dataskyddsombudet vid genomförande av en konsekvensbedömning avseende dataskydd.

Schrems II, med bl.a. framtagen vägledning från Europeiska dataskyddsstyrelsen (EDPB).[3]

- Juni 2021: Skrivelse till nämnden för Intraservice. Syftet med skrivelsen var att uppmärksamma nämnden på de risker för registrerade som dataskyddsombudet identifierat utifrån den informationen i ärendet ”Redogörelse för Intraservice arbetssätt och metod för utveckling av Kommungemensamma interna tjänster med stöd av molntjänstleverantörer” (dnr 0227/21).
- Februari 2022: Rekommendation för det fortsatta arbetet med Digitala Navet lämnas till projektet. I denna rekommenderades att det Digitala Navet inte skulle lanseras i skarpt läge (med riktiga personuppgifter) förrän tredjelandsproblematiken med M365 utretts och beslut fattats om den fortsatta användningen av M365 på en övergripande nivå i staden.

Dataskyddsombudets rekommendationer

För beslutspunkt 1 gällande att godkänna konsekvensbedömningen och därmed användandet av Digitala navet för nämnden för Intraservice

En konsekvensbedömning ska uppfylla de kriterier som återfinns i art. 35 GDPR. Det är dessa kriterier som dataskyddsombudet tittar på vid bedömning om en konsekvensbedömning är tillräcklig eller ej. Utifrån förvaltningens framtagna underlag har dataskyddsombudet i denna skrivelse identifierat ett antal viktiga punkter som nämnden behöver få vetskap om för att kunna fatta ett välinformerat beslut.

Identifiera personuppgiftsbehandlingar

I tidigare lämnad rekommendation för hanteringen lyfte dataskyddsombudet att förvaltningen behövde identifiera vilka personuppgiftsbehandlingar som användandet av Digitala Navet innebär. Förvaltningen har därefter genomfört ett omfattande arbete för att kartlägga aktuella behandlingar. Det är positivt att förvaltningen utifrån detta kunnat identifiera ett antal behandlingar som förekommer, men beskrivningen av dessa bedöms behöva utvecklas i konsekvensbedömningen. Till exempel saknar dataskyddsombudet information om den personuppgiftsbehandling som innebär att intranätets innehåll anpassas utefter användaren.

Personuppgiftsansvar

Utöver att identifiera behandlingar rekommenderades förvaltningen även att utreda ansvarsfrågan, för att kunna avgöra vem/vilka som ansvarar för de olika behandlingarna. Dataskyddsombudet kan utifrån underlaget se att ansvarsfrågan fortfarande är outredd, vilket bedöms påverka konsekvensbedömningen då det är den som är personuppgiftsansvarig för en eller flera behandlingar som ska bedöma vilka risker och åtgärder som behöver vidtas och dokumentera detta. Eftersom förvaltningen uppger att det fortfarande är oklart vem eller vilka som är personuppgiftsansvariga för vilka behandlingar, ställer sig dataskyddsombudet därför frågande till i vilken roll som förvaltningen genomför konsekvensbedömningen. Mot bakgrund av hur beslutspunkten är formulerad ser dataskyddsombudet även risker med att nämnden kan komma att fatta beslut utanför sitt ansvarsområde. Vidare kan ett beslut om att ”godkänna

[3] Dataskyddsenhetens uppdaterade rekommendationer om tredjelandsöverföringar efter Schrems II (2022-05-09)

konsekvensbedömningen” riskera att leda till att nämnden tar på sig ett större personuppgiftsansvar än vad som avsetts.

Behandling av känsliga personuppgifter

I artikel 9 GDPR finns ett förbud mot att behandla så kallade känsliga personuppgifter, om inte ett tillämpligt undantag finns. Till denna kategori av personuppgifter hör bland annat uppgifter om facklig tillhörighet. Förbudet att behandla känsliga personuppgifter enligt förordning beror på att sådan behandling medför höga risker för de registrerade. Förvaltningen uppger att man kommer att behandla dessa uppgifter, trots att det saknas tillämpligt undantag för behandlingen. Om förvaltningen inte kan visa på att den avsedda behandlingen av känsliga personuppgifter är laglig innebär detta, utöver risker för de registrerade, även risk för sanktionsavgifter och skadestånd.

Dataskyddsombudet vill också lyfta att enligt stadens tidigare klassningsmodell placerades känsliga personuppgifter i informationsklass 2, och uppgifter i denna informationsklass ska enligt nuvarande regler inte hanteras i Sharepoint. Då Digitala Navet är en Sharepoint-lösning följer den förslagna behandlingen inte Stadens regler.

Förekomsten av tredjelandsöverföringar

Skyddet för personuppgifter garanteras inom EU få ett likvärdigt skydd tack vare GDPR. Om en personuppgiftsansvarig vill föra över personuppgifter utanför EU/EES innebär det att personuppgifterna riskerar få ett sämre skydd, och den personuppgiftsansvarige måste därför vidta åtgärder som säkerställer skyddet för den registrerade. Om skyddet inte kan säkerställas, innebär det att överföringen inte får göras.

Dataskyddsombudet bedömer att det i konsekvensbedömningen inte tydligt framgår när en tredjelandsöverföring av personuppgifter sker och vilka skyddsåtgärder som har vidtagits. Varför detta saknas ställer sig dataskyddsombudet frågande till då det utifrån såväl förvaltningens egna utredningar som separat information från Microsoft är tydligt att det sker tredjelandsöverföringar vid användning av M365. I nuvarande underlag bedöms förvaltningen inte ge nämnden en tydlig bild av de aktuella förutsättningar som föreligger i frågan.

Dataskyddsombudet bedömer vidare att förvaltningen inte har kunnat påvisa att man vidtagit tillräckliga skyddsåtgärder för att säkerställa skyddet för personuppgifterna med anledning av de faktiska, respektive potentiella, tredjelandsöverföringar som användningen av Sharepoint/M365 innebär. Detta innebär att om nämnden väljer att inleda behandlingen (dvs lansera Digitala Navet) innebär det samtidigt att nämnden väljer att frångå gällande dataskyddslagstiftning.

Riskbedömning

Dataskyddsombudet bedömer att förvaltningens riskbedömning har allvarliga brister. Det handlar främst om att det finns flera risker som har fått ett sänkt riskvärde till noll (0), trots att förvaltningen inte angett åtgärder för att minska risken. Ett riskvärde kan enbart ändras efter att förvaltningen bedömt de planerade åtgärderna. Att majoriteten av riskerna har värde noll (0) innebär att förvaltningen på felaktiga grunder identifierat att det enbart kvarstår ett fåtal höga risker. Dataskyddsombudets bedömning är att det finns flera risker med ett högre riskvärde än vad som anges.

Utöver ovan ställer sig dataskyddsombudet frågande till förvaltningens resonemang kring att utelämna de risker som kommer ifrån användningen av en amerikansk

molntjänstleverantör (Microsoft). Dataskyddsombudet har sedan sommaren 2020 regelbundet lyft frågan om tredjelandsöverföringar till förvaltningen. Förvaltningens svar har återkommande varit att man väljer att avvakta och se vad som händer i stället för att agera. Detta förhållningssätt har inneburit att de risker som föreligger för registrerade fortlöpt utan åtgärder under tiden. Utifrån underlaget är dataskyddsombudets uppfattning att samma strategi tycks fortsätta gälla, eftersom förvaltningen fortsatt väljer att inte adressera grundproblematiken utan i stället skjuta frågan ytterligare på framtiden. Dataskyddsombudet är medvetet om att det handlar om andra värden än enbart skyddet för den personliga integriteten, men vill ändock påpeka att ekonomiska incitament eller nya funktionaliteter inte kan motivera ett fortsatt förhållningssätt som innebär att man frångår gällande lagstiftning. Dataskyddsombudet ser även behov av att påpeka att denna problematik inte är unik för Digitala Navet utan att samma problem finns för övriga M365-produkter, inklusive Outlook och Teams.

Begära förhandssamråd

I riskhanteringsavsnittet har förvaltningen identifierat tre kvarstående höga risker. Den personuppgiftsansvarige ska/är skyldig att samråda med tillsynsmyndigheten om en konsekvensbedömning avseende dataskydd visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken. Från denna regel i GDPR finns inget undantag. Dataskyddsombudet har tidigt i processen informerat förvaltningen om att ett sådant förhandssamråd kommer behöva begäras i det fall kvarstående höga risker finns, och hänvisat till bland annat det förhandssamråd som Stockholms Stad begärde i en liknande fråga.

Av vad som framgår av underlaget har förvaltningen dock bedömt att detta inte är nödvändigt, trots de kvarstående höga riskerna. Dataskyddsombudet vill därför påtala att denna hantering strider mot kraven i GDPR. Vid ett förhandssamråd kan tillsynsmyndigheten ge råd om hur förvaltningen ska kunna gå vidare med behandlingen. Tillsynsmyndighet kan också utfärda varningar, reprimander och föreläggande, samt förbjuda en behandling. Dataskyddsombudet bedömer att förvaltningens beslut om att inte begära förhandssamråd, innebär att förvaltningen riskerar att gå vidare med en behandling som inte uppfyller kraven i GDPR. Det kan på sikt innebära att tillsynsmyndigheten ålägger förvaltningen att upphöra med behandlingen eller att betala sanktionsavgifter.

Sammanfattande rekommendationer

Dataskyddsombudet avråder nämnden för Intraservice från att införa det Digitala Navet och därigenom inleda personuppgiftsbehandlingen utifrån följande;

a) Konsekvensbedömningen uppfyller inte kraven enligt GDPR och utgör därför inte ett korrekt beslutsunderlag. Allvarligast är att de höga risker som kvarstår ej tydligt framgår av underlaget.

b) Personuppgiftsansvarsfrågan är fortfarande inte utredd, vilket innebär att nämnden i ett beslut om att godkänna konsekvensbedömningen och inleda behandlingen egentligen inte vet vad beslutet innebär för nämnden framåt.

c) Förvaltningen har inte kunnat påvisa att man kunnat vidta tillräckliga skyddsåtgärder för att säkerställa skyddet för personuppgifterna med anledning av de faktiska, respektive potentiella, tredjelandsöverföringar som användningen av Sharepoint/M365 innebär.

Detta innebär att om nämnden väljer att inleda behandlingen (dvs lansera Digitala Navet) innebär det samtidigt att nämnden väljer att frångå gällande dataskyddslagstiftning.

Vidare ser dataskyddsombudet ett behov av att, i relation till Digitala Navet, uppmärksamma nämnden på att det föreslagna beslutet kan komma att uppfattas som ett s.k. ”inriktningsbeslut” för förvaltningens arbete med molntjänster och tredjelands-överföringar, samt även stärka det redan starka beroende som förvaltningen uppfattas ha till den aktuella leverantören.

Dataskyddsenheten

GÖTEBORGS STAD