Kommunstyrelsen

2022-05-23
TJÄNSTESKRIVELSE
Dnr: KFKS 2021/1333

Ställningstagande avseende användning av molntjänster från leverantörer hemmahörande i tredjeland

Förslag till beslut

Kommunstyrelsens arbetsutskott föreslår kommunstyrelsen besluta följande.

Kommunstyrelsen beslutar att användning av de administrativa molnbaserade systemen Google Workspace for Education och Office 365 fortsatt får ske med de förbehåll och riskminimerande åtgärder som anges i tjänsteskrivelse daterad den 23 maj 2022.

Kommunstyrelsen beslutar att ge stadsledningskontoret i uppdrag att ta fram vägledning för hantering av framtida upphandlingar av IT-tjänster där leverantören (eller underleverantören) är hemmahörande i tredjeland med utgångspunkt i att all behandling av personuppgifter enbart får ske inom EU/EES.

Kommunstyrelsen beslutar att ge stadsledningskontoret i uppdrag att fortsatt bevaka frågan om användning av molntjänster från leverantörer hemmahörande i tredjeland och återkomma till kommunstyrelsen med förslag på reviderat beslut om förutsättningarna förändras.

Sammanfattning

Den 16 juli 2020 beslutade EU-domstolen i domen Schrems II att underkänna avtalet mellan EU och USA som möjliggjorde överföring av personuppgifter till USA. Domen innebär att det i dagsläget praktiskt inte är möjligt att använda amerikanskägda molntjänster där personuppgifter riskeras att överföras till USA.

Utifrån en bedömning av kommunens uppdrag som helhet och risker för enskilda bedöms vissa administrativa molnbaserade system fortsatt kunna användas under förutsättning att vissa riskminimerande åtgärder vidtas i enlighet med tjänsteskrivelse daterad den 23 maj 2022. Därutöver föreslås stadsledningskontoret får i uppdrag att ta fram vägledning för hantering av framtida upphandlingar av IT-tjänster där leverantören eller underleverantören är hemmahörande i tredjeland med utgångspunkt i att all behandling av personuppgifter enbart får ske inom EU/EES.

Ärendet

Bakgrund

Kommunen använder idag flera typer av molntjänster och IT-tjänster i sina verksamheter. Utifrån de krav som ställs i dataskyddsförordningen (GDPR), som reglerar hanteringen av personuppgifter, innebär en användning av molntjänster att kommunen anlitar ett personuppgiftsbiträde som behandlar personuppgifter för kommunens räkning. Kommunen är alltid ansvarig för personuppgifterna även när detta sker hos ett biträde och måste därmed säkerställa att hanteringen sker lagenligt. Det finns dessutom krav på att enbart anlita personuppgiftsbiträden som kan ge tillräckliga garantier för att GDPR följs och enskildas grundläggande fri- och rättigheter skyddas[1].

Syftet med GDPR är just att skydda enskildas fri- och rättigheter och därför innehåller lagstiftningen även regler om när det är tillåtet att överföra personuppgifter till ett land utanför EU/EES[2] (s.k. tredjelandsöverföring) eftersom det innebär en risk att rättigheterna undergrävs.

I dagsläget finns flera amerikanska molntjänstleverantörer på marknaden där personuppgifter antingen överförs eller kan komma att överföras till USA. En överföring av personuppgifter sker inte enbart när uppgifterna skickas eller lagras utanför EU/EES, utan även när åtkomst till uppgifterna ges genom exempelvis fjärråtkomst vid ett supportärende. Till personuppgifter räknas dessutom all typ av information som kan kopplas till en enskild individ, dvs. även metadata och data om enskilda användares användning av IT-tjänster är personuppgifter.

Tredjelandsöverföring till USA efter Schrems II-domen

Den 16 juli 2020 meddelade EU-domstolen dom i det som kallas Schrems II-målet. Domstolen underkände det så kallade Privacy Shield-avtalet som dittills kunnat användas som stöd för att överföra personuppgifter till USA. Som skäl för domstolens bedömning att avtalet skulle underkännas angavs att amerikansk underrättelselagstiftning är för långtgående och att medborgare från EU saknar medel för att hävda sina rättigheter i USA. Domen underkände inte standardavtalsklausulerna (Standard Contractual Clauses, SCC) som också används för att överföra uppgifter till USA men fastställde samtidigt att det inte enbart räcker att avtala om ett skydd för enskildas personuppgifter, detta skydd måste också finnas i praktiken. Detta innebär att överföring till USA inte får ske utan att ytterligare åtgärder vidtagits för att skydda enskildas rättigheter i praktiken. Åtgärderna måste således råda bot på de brister i rättsläget i USA som domen tar upp, dvs. hindra amerikanska underrättelsetjänster från att ta del av uppgifter och ge enskilda effektiva

[1] Artikel 28, GDPR
[2] Se Kapitel V i dataskyddsförordningen.

rättsmedel i USA. Om åtgärderna inte råder bot på dessa brister är inte tredjelandsöverföringen tillåten.

Praxis och vägledning sedan Schrems II-domen

Den praxis och vägledning som hittills offentliggjorts av tillsynsmyndigheterna tydliggör att en överföring till USA eller anlitande av ett amerikanskt personuppgiftsbiträde enbart kan ske om åtgärder vidtas som hindrar amerikansk underrättelsetjänst från åtkomst till personuppgifterna.

I november 2020 publicerade EDPB (Europeiska dataskyddsstyrelsen), där samtliga EU-länders tillsynsmyndigheter på dataskyddsområdet ingår, en rekommendation[3] om vilka åtgärder anses vara tillräckliga för att en tredjelandsöverföring ska vara tillåten. I rekommendationerna anges bland annat att ett scenario där en molntjänstleverantör som lyder under utländsk lagstiftning som anses vara för långtgående (exempelvis den lagstiftning i USA som nämns i Schrems II-domen) och där leverantören måste behandla personuppgifter i klartext för att tillhandahålla tjänsten. I detta scenario uppfylls inte kraven på tillräckliga åtgärder och en överföring skulle inte vara tillåten i detta fall. I de flesta fall behöver amerikanska molntjänstleverantörer behandla personuppgifterna i klartext för att tjänsten överhuvudtaget ska fungera.

I Sverige har Integritetsskyddsmyndigheten (IMY) i två beslut avrått från användning av amerikanska personuppgiftsbiträden[4]. I ett beslut om Region Skånes planerade användning av nytt journalsystem avrådde IMY från att använda ett amerikanskt och ett indiskt personuppgiftsbiträde. I ett annat beslut gällande Stockholm stads planerade införande av Office 365 avrådde IMY från fortsatt införande då staden inte gjort analyser om personuppgiftsbiträdet gett garantier för att GDPR följs och enskildas rättigheter skyddas.

Under våren 2022 har ett antal tillsynsmyndigheter i EU fattat beslut i ärenden rörande Google analytics[5]. Överföringen av personuppgifter har i dessa situationer inte ansetts uppfylla kraven i GDPR då Google omfattas av lagstiftning i USA som ger amerikanska myndigheter rätt att övervaka enskilda och de åtgärder som vidtagits har inte varit tillräckliga för att hindra övervakningen.

Den 25 mars 2022 meddelade EU-kommissionen och USA om att de kommit överens om en principöverenskommelse för ett nytt avtal för överföring av personuppgifter

[3] Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_sv

[4] Beslut med diarienummer DI-2021-1513 och DI-2021-2983.

[5] Beslut har hittills fattats av Österrikes tillsynsmyndighet DSB (https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal), av franska tillsynsmyndigheten CNIL (https://noyb.eu/en/update-cnil-decides-eu-us-data-transfer-google-analytics-illegal) och Liechtensteins tillsynsmyndighet Datenschutzstelle (https://iapp.org/news/a/liechtenstein-dpa-urges-organizations-to-use-alternative-solutions-to-google-analytics/)

mellan EU och USA, kallat Trans-Atlantic Data Privacy Framework. Det finns dock inget konkret avtal på plats ännu och de två avtal som tidigare funnits, Privacy Shield och Safe Harbor har båda upphävts i EU-domstol. För att ett framtida avtal ska kunna användas för överföring av personuppgifter till USA måste det adressera de brister som EU-domstolen tagit upp i sina domar för att det inte ska upphävas igen.

Stadsledningskontorets utredning och bedömning

Mot bakgrund av rådande rättsläge gällande överföring av personuppgifter till tredjeland, främst USA, har personuppgiftsbiträden identifierats där personuppgifter överförs eller riskerar att överföras till utanför EU/EES. Dessa består huvudsakligen av administrativa molnbaserade system och beskrivs nedan.

Administrativa molnbaserade system

Kommunen använder idag två administrativa molnbaserade system, Google Workspace for Education och Office 365, som båda levereras av amerikanska leverantörer och där personuppgifter överförs eller riskerar att överföras till USA och potentiellt andra länder utanför EU/EES. Konsekvensbedömningar (DPIA) har genomförts för dessa system i syfte att identifiera riskminimerande åtgärder och sammanfattas nedan.

Google Workspace for Education

Google Workspace for Education är ett verktyg de kommunala skolorna använder för sitt pedagogiska arbete. De personuppgifter som behandlas i tjänsten är därmed all typ av information relaterat till detta, exempelvis kommunikation mellan elev/lärare och skolarbeten. Det ska tilläggas att personuppgifter innefattar all information som kan kopplas till en enskild individ, därmed behandlas även personuppgifter i form av data som genererats av själva användningen av tjänsterna. Personuppgifter kan även behandlas i supportärenden.

Avseende överföring av personuppgifter till USA och andra länder anger leverantören Google[6] att personuppgifter, inbegripet kunddata[7], diagnostik data[8] och data i supportärende, kan komma att behandlas i alla länder där Google har verksamhet. Det finns därmed ingen begränsning för var personuppgifterna kan behandlas. För överföringen av personuppgifter stödjer sig Google på standardavtalsklausuler (SCC) men som anförs ovan är det inte enbart tillräckligt att avtala om ett skydd för enskildas fri- och rättigheter, skyddet måste finnas i praktiken. Då Google både överför uppgifter till USA och behandlar personuppgifter i klartext samt omfattas av den lagstiftning som EU-domstolen ansåg vara för långtgående kan inte de åtgärder som Google vidtagit vara tillräckliga för att uppfylla kraven i dataskyddsförordningen (GDPR).

[6] Enligt Googles DPA (Data Processing Amendment), https://workspace.google.com/terms/dpa_terms.html
[7] Data som skickas, lagras eller tas emot via tjänsten.
[8] Data om användning av tjänsterna.

Googles avtal och villkor är ensidiga, vilket betyder att kommunen har begränsade möjligheter att påverka Googles hantering av personuppgifter. De riskminimerande åtgärder som vidtagits hittills är att minska hanteringen av personuppgifter i verktyget och stänga funktioner som inte behövs i det pedagogiska arbetet. Känsliga och extra skyddsvärda uppgifter är inte tillåtna i tjänsten[9] och rutiner för gallring av uppgifter finns upprättade. En revision av hela tjänsten genomfördes i början av 2022. Dessutom planeras fler erbjudas utbildning i hantering av personuppgifter i digitala tjänster och inställningar ses över för att säkerställa att integriteten skyddas så långt funktionerna tillåter.

Office 365

Office 365 är ett verktyg med ett antal olika tjänster som kommunens samtliga anställda kan använda i sitt arbete, bland annat finns e-post (Outlook) och samarbetsplattform (Teams) samt funktioner för dokumenthantering och delning (OneDrive och SharePoint). Såsom med Google Workspace omfattas personuppgiftsbehandlingen inte enbart av den information som användarna skickar, tar emot eller skapar utan också av data som genererats av användningen och av information i supportärenden.

Avseende tredjelandsöverföringen kan data överföras till USA eller andra länder utanför EU/EES beroende på typ av data (kunddata, diagnostik data eller supportdata) samt typ av tjänst[10]. Vilande kunddata lagras huvudsakligen inom Sverige eller EU/EES men övriga data kan överföras till USA eller andra länder där leverantören Microsoft har verksamhet. Microsoft stödjer sig på standardavtalsklausuler (SCC) för överföringen av personuppgifter, men som redan nämnts ovan behövs andra åtgärder än avtal för att skydda enskildas fri- och rättigheter. Såsom med Google Workspace överförs personuppgifter till USA och leverantören måste behandla personuppgifter i klartext för att tillhandhålla tjänsten samtidigt som de omfattas av den lagstiftning som EU-domstolen ansåg vara för långtgående. Därmed kan inte de åtgärder som Microsoft vidtagit vara tillräckliga för att uppfylla kraven i dataskyddsförordningen (GDPR).

I risk- och konsekvensbedömningen gällande tredjelandsöverföringen i Office 365 har ett antal funktioner som Microsoft erbjuder och som möjligen skulle kunna hindra leverantörens åtkomst till personuppgifter utvärderats, exempelvis kryptering. Dessa har inte ansetts vara tillräckliga åtgärder för att skydda personuppgifterna enligt EDPB:s rekommendationer och nuvarande praxis, såsom beskrivs under rubriken ”Praxis och vägledning sedan Schrems II-domen” ovan. Microsoft har annonserat att de avser erbjuda en tjänst som hindrar överföring av personuppgifter till utanför EU/EES, men

[9] För denna typ av information finns andra system som är lämpliga och säkra för detta ändamål, exempelvis systemstöd för elevhälsans dokumentation och systemstöd för elevdokumentation (exempelvis betyg och bedömningar).

[10] Beskrivning av hur Microsoft lagrar och hanterar data finns bland annat i Microsofts DPA (Data Protection Addendum, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?isToggleToList=True&lang=32) och Microsoft supportsidor (https://docs.microsoft.com/en-us/microsoft-365/enterprise/eu-data-storage-locations?view=o365-worldwide)

denna är planerad att lanseras först slutet av 2022 och det är oklart i detta skede om tjänsten löser de rättsliga frågorna kring överföring av personuppgifter. De riskminimerande åtgärderna består därmed i dagsläget av att inga känsliga och extra skyddsvärda personuppgifter får hanteras i tjänsten med kompletterande utbildning och rutiner för att detta följs.

Risker som inte bedömts i ärendet

I fråga om administrativa molnbaserade system såsom Google Workspace for Education och Office 365 finns andra integritetsrisker än de kopplat till tredjelandsöverföring. Dessa faller utanför ärendets omfattning och har därmed inte bedömts eller hanterats. Exempel på potentiella risker är exempelvis bristande transparens och ensidiga avtal/villkor. Båda systemen är integrerade i leverantörens andra tjänster och det är inte tydligt hur leverantörerna använder sig av personuppgifter för sina egna syften och hur personuppgiftsansvaret är fördelat. Dessutom kan leverantören ensidigt göra ändringar i personuppgiftsbiträdesavtal, villkor och tjänsten som helhet med begränsade möjligheter för kommunen att påverka utformningen av dessa.

Sammanvägd bedömning av risker och konsekvenser

Administrativa molnbaserade system, oavsett leverantör, är en förutsättning för att kommunen ska kunna arbeta digitalt. De system som används idag har använts länge och verksamheterna har utarbetat effektiva arbetssätt utifrån systemens funktionalitet. Det finns därmed starka praktiska och ekonomiska skäl att fortsätta använda just dessa system. Dessa system är också en förutsättning för att på ett effektivt sätt kunna samverka digitalt både internt inom kommunen men också med externa parter, då det i dagsläget saknas fullgoda svenska alternativa tjänster. Vidare kan vi konstatera att IT-marknaden i allt högre grad går mot molntjänster, varför det på sikt blir svårt att utesluta dessa lösningar helt. Utifrån en bedömning av kommunens uppdrag som helhet och risker för enskilda föreslås att kommunen fortsätter att använda de administrativa molnbaserade systemen Google Workspace for Education och Office 365. Detta sker med förbehållet att inga känsliga eller extra skyddsvärda personuppgifter får hanteras i tjänsterna.

Eftersom omständigheter kan förändras vilket kan påverka denna sammanvägda bedömning, föreslås även att stadsledningskontoret löpande bevakar frågan och vid behov återkommer med förslag på förändringar till kommunstyrelsen.

Andra befintliga IT-tjänster med underleverantörer i tredjeland

Utöver molntjänster som kommunen själv tecknar avtal med, kan en IT-leverantör som kommunen har avtal med välja att använda sig av en underleverantör för lagring, drift eller liknande. Underleverantören kan vara etablerad utanför EU/EES vilket innebär att personuppgifter kan överföras till tredjeland och/eller underleverantören lyder under tredjelands lagstiftning med risk för tredjelandsöverföring.

I dessa fall rekommenderas i första hand en dialog med IT-leverantören om byte av underleverantör. I andra hand rekommenderas en risk- och konsekvensbedömning dokumenteras och där åtgärder vidtas för att minska riskerna för enskildas rättigheter.

Upphandling av nya IT-tjänster

Kommunen köper löpande upp IT-system och IT-tjänster som i någon mån har sin grund i molntjänstplattformar. I framtida inköp av IT-system och IT-tjänster är utgångspunkten att Nacka kommuns mall för personuppgiftsbiträdesavtal (PUB-avtal) används. Av mallen framgår att all behandling av personuppgifter ska ske inom EU/EES, dvs. personuppgifterna inte under några omständigheter får överföras till utanför EU/EES. Då det i vissa fall kan vara motiverat att frångå från denna princip, föreslås stadsledningskontoret få i uppdrag att ta fram vägledning med kriterier för i vilka situationer undantag är motiverat.

Dataskyddsombudets kommentar

Dataskyddsombudet (DSO) har varit delaktig i arbetet med framtagandet av underlaget till beslut. DSO har enligt GDPR i uppdrag att ge råd och stöd till kommunens nämnder och övervaka efterlevnaden av dataskyddslagstiftningen. DSO rekommenderar kommunen att inte använda molntjänster med- eller risk för tredjelandsöverföring på grund av att skyddet för enskildas fri- och rättigheter inte kan garanteras. I första hand bör alternativ till befintliga tjänster utredas då medborgare och anställda inte kan välja bort att få sina personuppgifter behandlade i tjänster som innebär att uppgifter överförs till utanför EU/EES där de inte kan utöva sina rättigheter. DSO vill också framföra att det finns andra integritetsrisker med molntjänster som bör utredas närmare. Framför allt gäller det standardiserade molntjänster där kommunen som personuppgiftsansvarig måste få insyn i hur personuppgifterna hanteras för att kunna säkerställa att all personuppgiftsbehandling sker transparent och lagenligt.

Ekonomiska konsekvenser

Förslag till beslut om att fortsätta använda administrativa molntjänstbaserade system bedöms inte få någon påverkan på befintlig budget. I risk- och konsekvens-bedömningarna har ett antal åtgärder identifierats som skulle kunna minska riskerna för enskildas fri- och rättigheter, men dessa åtgärder medför inga direkta höjda kostnader för tjänsterna. En otillåten behandling av personuppgifter enligt GDPR kan däremot leda till sanktionsavgifter upp till 10 miljoner för kommunen och skadeståndsanspråk från enskilda.

Konsekvenser för barn

Barns personuppgifter är särskilt skyddsvärda eftersom de kan ha svårt att själv förstå risker med en viss personuppgiftsbehandling. Barns personuppgifter förekommer i tjänster som omfattas av ställningstagandet, främst i Google Workspace for Education

som är det pedagogiska verktyget inom Välfärd skola men även i Office 365. Därmed finns även risker för barns fri- och rättigheter. Det fortsatta användandet av dessa administrativa molntjänstbaserade system sker med ett antal förbehåll och åtgärder som syftar till att minska riskerna för barns fri- och rättigheter.

Henrik Palmblad-Wennergren
Digitaliseringsdirektör
Stadsledningskontoret

Brita Molavi Rösblad
Enhetschef
Digitaliseringsenheten