Kommunstyrelsen
Kommunledningskontoret
Kommunikation och delaktighet
Pia Karjalainen Thunström 016-710 12 88

Datum
2023-05-15

Diarienummer
KSKF/2022:432

Handlingsnummer
2023:100

Kommunstyrelsen

Stöd för digital arbetsplats - Microsoft 365

Förslag till beslut

1. Införande av Microsoft 365 (M365) inom kommunstyrelsens ansvarsområde godkänns.
2. Kommunledningskontoret får i uppdrag att genomföra konsekvensbedömningar för att besluta om vilka komponenter inom M365 som kan användas.
3. Kommunledningskontoret får i uppdrag att säkerställa att medarbetare inom förvaltningen har rätt anvisningar och kompetens för hantering av information inom de komponenter som görs tillgängliga inom ramen för M365.
4. Kommunledningskontoret får i uppdrag att följa rättsläget.
5. Kommunledningskontoret får i uppdrag att tillsammans med servicenämnden ta fram en strategi för att kunna lämna M365 om rättsläget förändras.
6. Kostnaden för införandet belastar kommunledningskontorets ram.

Sammanfattning

Eskilstuna kommun har planerat sedan år 2016 att över tid gå från egen drift till molntjänster. Införande av valda delar av M365 innebär en övergång från drift i egna serverhallar till M365. Då M365 är en molntjänst i tredje land så krävs enligt kommunfullmäktiges beslut 21 oktober 2021 § 205 (KSKF/2021:98) att nämnden i sitt personuppgiftsansvar beslutar om införandet.

Kommunen har under många år använt Microsoft som leverantör för ett flertal olika IT-komponenter och basinfrastruktur. Precis som kommunen och övriga IT-leverantörer har Microsoft alltmer gått över till molntjänster. Microsoft erbjuder den mest konkurrenskraftiga lösningen avseende bland annat kontorsstödsprodukter som exempelvis Officepaketet, Teams, etcetera.

I takt med den ökade digitalisering i samhället är det viktigt att skydda IT-systemen mot dataintrång. M365 ger kommunen kontroll och skydd mot skadlig kod, säkerhetsluckor och cyberattacker och hjälper till att skydda Eskilstuna kommun och kommunens data.

Beslutet om ett införande utgör en väsentlig grund för Eskilstuna kommuns IT-arkitektur och säkerhet, kommunens informationsförsörjning & digitala infrastruktur samt delar av kommunens framtida IT-infrastruktur.

Då M365 innebär en övergång till molntjänst i tredje land så har jurister konsulterats för att bedöma riskerna med denna övergång i relation till de fördelar som det ger kommunen. Juristerna rekommenderar att Eskilstuna kommun bör utifrån en proportionerlig helhetsbedömning och med accepterande av ett visst mått av risk, med stöd av Eskilstunas program för digital transformation med uppsatta mål för digital arbetsplats samt behovsanalys av digital arbetsplats och arbetsmiljö och med ett beaktande av organisatoriska och tekniska skyddsåtgärder och utkomster från genomförd konsekvensbedömning avseende dataskydd – att implementera och tillhandahålla ett användande av plattform M365.

Ärendebeskrivning

Eskilstuna kommun har sedan år 2016 ett licensavtal som är baserat på molntjänster med leverantören Microsoft. Avtalet med Microsoft löper ut i april 2025 vilket innebär att kommunen står i ett vägskäl och behöver beslut om att bryta licensavtalet eller gå över till valda delar av M365 molntjänster. Då M365 är en molntjänst i tredje land krävs att nämnden i sitt personuppgiftsansvar beslutar om införandet.

Beslutet innebär att utifrån kommunfullmäktiges molntjänstbeslut 21 oktober 2021 § 205 (KSKF/2021:98) bedöma om, och i så fall hur och när kommunen kan implementera valda delar av M365 som molnlösning med tillhörande risker, åtgärder och konsekvenser för informationssäkerhet, säker IT-drift, digital arbetsplats/arbetsmiljö och ekonomi – för att kunna dra nytta av moderna digitala tjänster för medarbetarna.

Ärendet har beretts av en styrgrupp med representanter från Eskilstuna kommun med sakkunskap inom digital arbetsplats, digital arbetsmiljö, IT, digitalisering och attraktiv arbetsgivare.

Styrgruppen har tagit stöd av ramavtalade Ateas jurister, vilka är specialiserade inom informationssäkerhet, IT-rättsjuridik och cybersäkerhet för att få en objektiv bedömning och analys av de legala – regelefterlevnads resonemang – dataskydds och andra juridiska frågeställningar, risk och nytta perspektiv, samt proportionalitets bedömning ställt i relation till de IT- och processuella tjänster som Microsoft tillhandahåller för kommun och myndigheter som nyttjar deras molntjänster.

Inom Ateas uppdrag har en konsekvensbedömning genomförts av själva plattformen M365, en så kallad DPIA (Data protection impact assesment), vilken även inkluderat en riskanalys, i enlighet med General Data Protection Regulation (GDPR), där dataskyddssamordnare, informationssäkerhetssamordnare, verksamhetsrepresentant och objektägare digital plattform deltog. Utredningens slutsatser har sedan analyserats och sammanställts av Ateas jurister till ett beslutsunderlag för att ge rätt juridiska förutsättningar om ett införande av plattformen M365.

Bakgrund

Tillvägagångssättet som leverantörer inom IT-branschen tillhandahåller tjänster på är och har under en längre tid varit på väg att förändras. Tjänsterna går från att ha varit

lokalt installerade, även kallat för ”on-premesis” förkortat ”on-prem”, till att tillhandahållas i molntjänster. Den här förändringen ser kommunen inom alla sektorer men det är främst förändringen inom området kontorsstödstjänster från Microsoft som just nu driver behovet av att möjliggöra IT-drift i molntjänster som lyder under lagstiftning från tredje land.

Användare i kommunens organisation har över tid byggt upp kompetens och kunskaper kring många av alla Microsofts produkter, dessa utgör en viktig grund i mycket av den administration som sker inom kommunen idag och tillför stora värden.

Kommunens IT-infrastruktur är byggd på lösningar från Microsoft med en IT-funktion som är uppbyggd av kompetens på Microsofts produkter.

Beslutet om ett införande utgör en väsentlig grund för Eskilstuna kommuns IT-arkitektur och säkerhet, kommunens informationsförsörjning & digitala infrastruktur samt delar av kommunens framtida IT-infrastruktur, samt för att nå de mål och effekthemtagning för programmet Effektivare administration.

Ur ett medarbetar- och verksamhetsbehovsperspektiv skapar ett införande av M365 förutsättningar för en god intern service genom en modern, sömlös digital arbetsplats för att kunna stödja och underlätta för dem som arbetar närmast våra invånare, kunder och besökare.

Eskilstunas kommuns IT-drift i molntjänster (KSKF/2021:98)

Eskilstuna kommuns digitalisering är ett av kommunens verktyg för att förbättra förutsättningarna för att fortsatt kunna bedriva välfärd och möta de utmaningar som uppstår i och med de pågående demografiska förändringarna i samhället. För att eliminera hinder för kommunens digitala utveckling togs ett inriktningsbeslut av kommunfullmäktige 21 oktober 2021 § 205 (KSKF/2021:98), gällande IT-drift i molntjänster som är taget utifrån juridiska, tekniska och ekonomiska aspekter.

Beslutet innebär att kommunen så långt det är möjligt ska välja informationslagring i europeiska molntjänster. Men, där det inte är möjligt kan kommunen använda molntjänster som lyder under lagstiftning från tredje land, men endast för information som enligt kommunens modell för informationsklassning klassas som öppen (0) eller intern (1), förutsatt att lämpliga tekniska och organisatoriska åtgärder vidtagits. Det ankommer på alla användare att respektera regler och riktlinjer, samt att kommunen behöver i den grad det är görligt tillse att tillräckliga automatiska skyddsmekanismer implementeras.

Genom att medvetet och systematiskt arbeta med att motverka risker minimeras den reella risken för röjande av information som lyder under Dataskyddsförordningen (GDPR) och Offentlighets- och sekretesslagen (OSL 2009:400).

Office365 och Microsoft365

Office 365 (O365) är en fortsättning på tidigare ”Officepaket” med bland annat Word, Excel och Power Point. Varje år paketerar Microsoft dock in allt fler applikationer/programvara och idag ingår flera samarbetstjänster, till exempel

OneDrive, Teams, Planner, samt Outlook som ett komplett kontorsstöd och för kommunikation med omvärlden. Eskilstuna kommun har som en följd av pandemin ett intermistiskt beslut om användandet av MS Teams till och med 2023-06-01.

Microsoft 365 är ett paket med tjänster som inkluderar förutom allt innehåll i O365, även operativsystemet Windows 10, Mobilitet och Säkerhetsverktyg. Med Mobilitet och Säkerhet hjälper dessa i huvudsak till att skydda kommunen som organisation och vårt data. De ger kontroll över alla enheter (surfplattor, PC/datorer och telefoner) och skyddar oss mot skadlig kod, säkerhetsluckor och cyberattacker med säker inloggning och autentisering med multifaktorsfunktionalitet, samt verktyg för modern IT-drift för att kunna managera klienter, mjukvara, applikationer.

Lagligheten

Eskilstuna kommun har tagit stöd av ramavtalade Ateas jurister vilka är specialiserade inom informationssäkerhet, IT-rättsjuridik och cybersäkerhet. Dessa har sammanställt bilagan ”Slutrapport – Eskilstuna kommun: Beslutsunderlag Plattform M365” med syfte att ge rätt juridiska förutsättningar att fatta beslut om ett införande.

Beslutsunderlagets främsta syfte är att ”fastslå” hur Eskilstuna kommun bör ställa sig till en implementering och användning av plattformen M365 - kontorsstödsplattform och tillika molntjänsten Microsoft M365.

Underlaget ska ses mot bakgrund av de regel efterlevnadsresonemang – dataskydds och andra juridiska frågeställningar - som M365 belyser. Det är primärt skrivet med beaktande av Dataskyddsförordningen (DSF) och Offentlighets- och sekretesslagen (OSL). Det ska särskilt framhållas att rättsläget inte är helt tydligt, utan lämnar utrymme för tolkningar av aktuell lagstiftning och fastställda rekommendationer från Europeiska dataskyddstyrelsen (EDPB). Det är emellertid viktigt att noga och fortlöpande följa rättsutvecklingen inom området.

Vidare ska underlaget också ses i ljuset av Eskilstunas digitala transformation och till det, de kopplade behov och nyttor kommunen har av denna tjänst för en vidare utveckling servicen till medborgarna och till medarbetarnas digitala arbetsplats.

Kärnfrågan är om, i så fall på vilka grunder och med vilket stöd, Eskilstuna kommun, kan besluta om en implementering och ett tillhandahållande av Plattformen M365 som huvudsaklig konstorsstödsplattform för Eskilstuna kommuns samtliga förvaltningar.

Problematiken utgörs av de ifrågasättande som följer av det faktum att M365 är en molntjänst, ägd och levererad av ett USA-ägt företag, Microsoft, vars moderbolag lyder under amerikansk övervaktningslagstiftning vilket försvåras av en avsaknad av rättsliga möjligheter för en registrerad att utöva sin rätt i enlighet med DSF.

Juristernas rekommendationer är:
Eskilstuna kommun bör utifrån en proportionerlig helhetsbedömning och med accepterande av ett visst mått av risk,

- med stöd i programmet för digital transformation
- den verksamhets- och behovsanalys som genomförts

- de mål Eskilstuna kommun satt upp för en digital arbetsplats
- med ett beaktande av organisatoriska och tekniska skyddsåtgärder och utkomster från genomförd DPIA,

implementera och tillhandahålla ett användande av plattform M365.

Överväganden ska göras med en nödvändig, rimlig och proportionerlig avvägning mellan skyddet för personuppgifter, en sammanhängande tolkning av ändamålen med informationen i systemet samt verksamheternas behov och den registrerades intressen.

En implementering och ett tillhandahållande av plattformen M365 bör, åtminstone inom en överskådlig framtid, ses som en nödvändig förutsättning för att Eskilstuna kommun på ett rimligt sätt skall kunna fullgöra sina uppdrag och åligganden som följer av annan lagstiftning än Dataskyddsförordningen (DSF), så som exempelvis kommunallagen. Idag finns, såvitt känt, inte en likvärdig 1:1plattform/tjänsteplattform som MS365.

Eskilstuna kommun bör vid användande av ytterligare tjänster i M365 genomföra nödvändiga konsekvensbedömningar, främst utifrån GDPR, men också utifrån andra eventuella lagstiftningar som kan påverkas vid ett i anspråkstagande av en tjänst.

Eskilstuna kommun bör i sitt kontinuerliga utvecklingsarbete följa rättsutvecklingen avseende tredjeland problematiken, då det i dagsläget inte finns någon direkt praxis, och marknaden utifrån andra möjliga tekniska och funktionella lösningar.

Vidare bör Eskilstuna kommun, vid behov, anpassa och eventuellt ompröva sitt ställningstagande, särskilt om rättsläget förändras på ett genomgripande sätt.

Information och uppgifter som omfattas av OSL ska inte hanteras i en molntjänst där leverantören inte är svensk och omfattas av det straffrättsliga skydd för uppgiftshanteringen som tillämpningen av OSL medför. Material som faller under OSL ska inte hanteras i M365.

Eskilstuna kommun bör också som ett led i sin strävan att på bästa sätt efterleva regelverket med dess nuvarande tolkning, initiera ett arbete om en Exit strategi som en åtgärd att hantera risk, en så kallad ”fall back” plan för kommunen, vilken påvisar en ansvarstagande och modern kommun.

Bemötande av DSO: s rekommendationer

Eskilstuna kommuns dataskyddsombud (DSO) har inkommit med skrivelse med anledning av genomförd DPIA och beslut om införande av M365. (Se bilaga)

Delar av de synpunkter som DSO har framfört har korrigerats i DPIA: n.

DSO påtalar vikten av att de registrerade behöver få information om vad införande av M365 innebär. Vid införandet ska samtliga medarbetare få såväl information om registrering och även utbildning i användande av M365.

Kommunledningskontoret delar vidare DSO: s synpunkter om att varje nämnd ska genomföra nya DPIA för att bedöma de risker som finns inom respektive nämnd för användning av de olika tjänsterna inom M365.

DSO har påtalat att användningen av Azure som del av M365 kan innebära hantering av personuppgifter av barn, d.v.s. elevers användarkonton, vilket kan innebära känsliga uppgifter. Kommunledningskontoret menar dock att användningen av Azure per definition inte behöver medföra hantering av känsliga personuppgifter. Det är beroende av vilka Microsoftkomponenter som används av de olika förvaltningarna. Skolnämnderna har beslutat införa stöd från Microsoft för skolan, vilket in sin tur kan medföra att uppgifter om elevers användarkonton hanteras i tredjelandslösningar. Där ser kommunledningskontoret att skolnämnderna behöver se över om det kan förekomma risker i informationshanteringen. Införande av M365 inom kommunstyrelsens ansvarsområde kommer inte medföra hantering av känsliga personuppgifter.

DSO påtalar om en olämplighet att nyttja Atea för rekommendationer rörande användningen av M365. Kommunledningskontoret delar inte DSO:s synpunkter. Atea är Eskilstuna kommuns ramavtalade licenspartner för alla våra IT-komponenter, oavsett leverantör, och har den bästa kompetensen för denna typ av analyser.

Alternativa lösningar

eSam är ett samarbete mellan flera svenska statliga myndigheter med syfte att hitta alternativa kollaborativa verktyg inom den europeiska marknaden, främst digitala samarbetsplattformar. Eskilstuna kommuns egen utredning ”Alternativ till digital samarbetsplattform” (2022-11-07) konstaterar att en digital samarbetsplattform utifrån eSams förslag med flera olika lösningar av flera olika leverantörer som ett alternativ till en helhetslösning till Microsoft leder till konsekvenser vad avser kostnad, digital mognad, kompabilitet, kvalité, kommunikation samt för samarbeten utanför Eskilstuna kommuns egen verksamhet.

Konsekvenser av att backa ur Microsoft

Befintligt avtal med Microsoft riskerar att brytas då en tidigare överenskommelse med leverantören har träffats om att Eskilstuna kommun förbinder sig att över tid bruka molntjänster framöver. Genom att ligga kvar i lösningar som inte är moderna och i fas med marknadens erbjudande ökar kommunen sitt digitala arv vilket medför ökade kostnader för införande av nya.

I det fall det beslutas att inte gå in i molntjänsten krävs att Eskilstuna kommun i god tid avtalar om nya licenser av Microsoft (s.k. ”on-prem licenser” vilka lagrar all information lokalt) samt snarast identifierar konsekvenser av att inte införa en helhetslösning. Alternativet med lokal lagring kommer att leda till ökade licenskostnader, ökade driftskostnader och mer intern förvaltning. En licenshantering som återgår till att all information lagras lokalt leder till avsaknad av till exempel Teams.

Eskilstuna kommun behöver identifiera flera olika lösningar som tillsammans skapar en helhetslösning, finna möjligheter för kompabilitet och integrationer. De alternativa lösningarna ska upphandlas och implementeras - innan licensavtalet löper ut.

Inom IT-branschen saknas erfarenheter vad avser omställning och implementering av flera olika lösningar av flera olika leverantörer som alternativ till en helhetslösning som med Microsoft.

Ur ett medarbetar- och verksamhetsperspektiv kommer ersättningar med flera nya och olika lösningar med stor sannolikhet att medföra en rörig digital arbetsmiljö. Dessa kommer att kräva nya kompetensbehov; från IT ut till användare och i verksamheten plus ökade kostnader i omställning och utbildning.

Konsekvenser av ett införande

M365 förutsätter att samtliga nämnder beslutar om ett införande för att kunna bibehålla befintligt licensavtal. Med M365 inkluderas Office 365, operativsystemet Windows 10, Mobilitet (inklusive Teams) och Säkerhet.

M365 införs som en hybridlösning vilket ger fortsatt möjlighet att lagra skyddsvärd information lokalt. Det finns möjlighet till licensieringsnivåer som ger utökad funktionalitet för säkerhet som kan beslutas och aktiveras av varje nämnd. Anses detta nödvändigt ökar licenskostnaderna i olika grad beroende på vilken typ av licens som ska utökas med en extra säkerhet.

Behovet av investeringar i egen infrastruktur minskar i förhållande till dagens on-prem lösning med vilken information lagras lokalt. IT-kostnaderna kan fördelas på ett mer linjärt sätt i relation till antal användare än dagens on-prem lösning som kräver investeringar i IT-infrastruktur. Investeringsbehovet kopplat till kontorsstödstjänster kommer sjunka med tiden.

Samtliga nämnder behöver dock genomföra konsekvensbedömningar (så kallad DPIA) för att besluta om vilka komponenter inom M365 som kan användas inom respektive nämnd.

Säkerhet

I takt med den ökade digitalisering i samhället är det viktigt att skydda IT-systemen mot dataintrång. De senaste åren har det skett många incidenter av varierande omfattning i samhällets IT-system, något som visar hur viktigt hög säkerhet och kvalitetssäkrade processer är för att skydda vår information. Microsoft är ett av världen största It-företag med 3 500 säkerhetsexperter runt om i världen som arbetar dygnet runt veckans alla dagar med att skydda de tjänster deras kunder nyttjar. Microsofts tjänster användas av flera hundra miljoner människor, banker, sjukhus och myndigheter över hela världen.

Finansiering

Den bedömda kostnaden för införande av M365 i hela kommunen är 4,8 miljoner kronor, varav 2,2 miljoner kronor för 2023 och 2,6 miljoner kronor för 2024. Kostnaden belastar kommunstyrelsens ram.

Den ekonomiska effekthemtagningen blir från 2025 0,9 miljoner kronor årligen. Därutöver tillkommer andra ekonomiska effekthemtagningar som en följd av införande av M365 på mellan 5-10 miljoner kronor årligen.
Nyttor och kostnader för enskilda nämnder kan variera beroende på mognadsgrad och utvecklingspotential.
Potentialen i nyttor ligger i att verksamheten kan utnyttja de applikationer som finns i M365 molntjänst för utveckling av digitalisering på en nivå som inte har varit möjlig tidigare utan större insatser.

Att fortsätta med så kallad on prem-lösningar på egna servrar skulle däremot öka licenskostnaderna med över 10 miljoner kronor

Kommunledningskontorets bedömning

Kommunledningskontorets sammanfattande bedömning är att följa de rekommendationer som tagits fram av jurister och beskrivits i denna tjänsteskrivelse samt i bilagd rapport, samt att ett införande av M365 är en nödvändig förutsättning för att Eskilstuna kommun på ett rimligt sätt skall kunna fullgöra sina uppdrag och åligganden.

Konsekvenser för hållbar utveckling och en effektiv organisation

Eskilstuna kommun behöver möta både den ökade digitaliseringen i samhället och inre ökade förväntningar av en modern digital arbetsplats. Att fortsätta nyttja Microsoft som IT-plattform och implementera M365 bidrar till att öka organisationens inre effektivitet för medarbetare och verksamheter.

En intern service för medarbetare och verksamheter genom en modern och sömlös digital arbetsplats är en förutsättning för att stödja och underlätta för dem som arbetar närmast våra invånare, kunder och besökare och bidra till en god arbetsmiljö.

Ett serviceinriktat förhållningssätt ska gälla såväl inom den egna organisationen, mellan verksamheter inom kommunkoncernen, och till de som nyttjar kommunens service och tjänster - oavsett tid, plats eller verksamhet. En modern digital arbetsplats med användarvänlig och sömlösa funktioner bidrar till en god digital arbetsmiljö samt bidrar till en attraktiv arbetsgivare.

Med införandet följer dock ett krav på att använda molntjänsterna enligt kommunens beslutade riktlinjer och anvisningar för informationssäkerhet för att säkerställa medarbetares och invånares integritet och att noga och fortlöpande följa rättsutvecklingen inom området.

KOMMUNLEDNINGSKONTORET

Tommy Malm Eva Norberg

Kommundirektör Kommunikationsdirektör

Beslutet skickas till:
Samtliga nämnder

Dataskyddsombudets rekommendationer gällande M365 Azure

Av beslutsunderlaget för Plattform M365 framgår att man vill använda plattformen M365. Det arbete som har gjorts som inför beslutsunderlaget är dock gjort kring Azure som är en grundläggande funktion vid användning av M365 och dess kontorstjänster. Azure är en katalogtjänst för lagring av användaridentiteter, grupper, datorer, skrivare mm. Nästa steg är sedan att koppla på andra tjänster.

Ett led i arbetet har varit att göra en DPIA, dvs en konsekvensbedömning. Den görs enligt krav i dataskyddsförordningen för att bedöma risker, ta fram åtgärder och bedöma om den tilltänkta behandlingen av personuppgifter lever upp till dataskyddsförordningen.

Enligt artikel 35 i dataskyddsförordningen ska den personuppgiftsansvarige rådfråga dataskyddsombudet vid genomförande av en konsekvensbedömning avseende dataskydd. Fördelen med att involvera sitt dataskyddsombud är att få stöd under arbetet, få den bedömd när den kan anses tillräckligt väl genomförd. Så har inte skett då jag fick den för kännedom när den ansågs vara klar. Jag har dock därefter granskat den och lämnat synpunkter och rekommendation om komplettering och fortsatt arbete innan slutsatser kan dras om risker. DPIA:n var vid tillfället inte godkänd.

I slutrapporten står det att det framgår av DPIA:n att det inte finns några påtagliga risker vad avser behandling av personuppgifter i Azure AD. Jag kan dock konstatera att arbetet inte har kommit så långt att den slutsatsen kan dras. När jag tog del av DPIA:n fanns det brister och den behövde därför kompletteras och utvecklas. Några av bristerna följer här:

- DPIA:n var inte skriven så att en utomstående kan förstå.
- Personuppgifterna var inte korrekt dokumenterade utan skyddsvärdet är högre än vad som framgår.
- Uppgift om personuppgiftsansvarig är inte korrekt då det endast är nämnder som kan vara personuppgiftsansvariga i kommunen.
- Risknivån har bedömt utan att erforderliga analyser har gjorts. DPIA:n behöver utvecklas och det har inte gjorts någon analys av överföringen till tredje land. För det krävs en s k TIA (Transfer Impact Assessment) för vart och ett av de länder som personuppgifter förs över till. Utöver USA kan det tillkomma länder för support och annat dataflöde. Dessa behöver identifieras.

- Beslut har fattats att förhandssamråd inte behövs då risker inte anses höga och att åtgärder vidtagits. För att risk ska kunna bedömas behöver adekvata analyser ha gjorts, vilket inte är fallet. Tillräckligt med risker har inte tagits upp och därför finns inte heller tillräckliga åtgärder redovisade.
- Rättslig grund behöver förtydligas.
- Andra sätt att göra behandlingen har inte beskrivits. Alternativ och skillnader behöver beskrivas.
- Hur de registrerade ska informeras behöver beskrivas.
- Extra skyddsåtgärder tas fram vid en TIA. Tillräckliga skyddsåtgärder är inte möjligt att tillämpa pga globalt uppsatta system och support i tredjeländer där personuppgifter görs tillgängliga i klartext.
- Viktiga risker saknas i riskdokumentationen.

Enligt det inriktningsbeslut som togs i KF hösten 2021 så framgår det bl a att Eskilstuna kommun i första hand ska använda inomeuropeiska montjänster för informationslagring, om alternativ inte finns så ska inte information över skyddsnivå 0 och 1 lagras i molntjänster som lyder under lagstiftning från tredjeland samt att personuppgifter inte får vara känsliga eller extra skyddsvärda.

Om beslut tas enligt beslutsunderlaget bryter det mot det beslut som togs i KF hösten 2021 då alla personuppgifter som rör barn, dvs personer under 18 år, klassas som extra skyddsvärda. Om det framgår att elever går i förskoleklass, vilket jag inte har fått bekräftat, så klassas de som känsliga personuppgifter.

Jag vill även påtala det olämpliga i att använda den tilltänkta leverantören för att göra analyser och ta fram underlag samt rekommendationer inför beslut, vilket har varit fallet här.

EU-kommissionen arbetar på ett beslut om adekvat skyddsnivå för överföring av personuppgifter till USA. Europaparlamentet har nu i maj publicerat en resolution där de uppmanar kommissionen att säkerställa att det blir ett ramverk som håller för prövning då de fortfarande ser brister. Det är därmed oklart när ett beslut om adekvat skyddsnivå gällande USA kan finnas på plats.

Slutsats och rekommendation

Då DPIA inte är tillräckligt genomarbetad, viktiga risker inte hanterats och det inte har gjorts någon analys av överföringen till tredje land, samt att man inte har undersökt om andra tredjeländer än USA är aktuella för tjänsten kan inte adekvat riskbedömning och dokumentation anses finnas för Azure.

Det framgår inte av underlaget vilka eller hur många tjänster som kommer att tillkomma vid ett införande av MS365. Varje tjänst kräver sitt analysarbete då de skiljer sig åt vad gäller behandling av personuppgifter och ändamål. Gjord analys och riskbedömning gäller inte dessa. Omfattningen av vad ett beslut om införande av Azure/M365 leder till är därför okänt. Det kommer dock att leda till ett omfattande dataskyddsarbete.

Det bryter mot inriktningsbeslutet i KF då informationens skyddsvärde är högre än vad som beslutats och adekvata analyser inte har gjorts.

Då M365 ännu inte lever upp till dataskyddsförordningen hjälper det inte om riskerna eventuellt skulle visa sig vara låga eftersom dataskyddsförordningen är en lag och som sådan behöver efterlevas. Europeiska Dataskyddsstyrelsen, EDPB, påtalar vikten av efterlevnad i sin rapport om den samordnade action som EU:s tillsynsmyndigheter gjorde 2022 vad gäller offentliga organisationers användning av molntjänster "2022 Coordinated Enforcement Action Use of cloud-based services by the public sector", där de skriver följande:
"The EDPB therefore underlines the need for public bodies to act in full compliance with the GDPR when using cloud-based products or services."

Min rekommendation är därför:

- att ett adekvat arbete med objektiva analyser i form av DPIA och TIA utförs så att adekvat dokumentation och åtgärder tas fram
- att det förtydligas vilka tjänster som tillkommer och omfattningen av dessa
- att dataskyddsförordningen efterlevs

Eskilstuna 2023-05-15

Tjänsteskrivelse - bemötande av Dataskyddsombudets (DSO) kommentarer avseende följande dokument;

- Slutrapport – Azure AD **(beslutsunderlag)**
- Genomförd DPIA inklusive dess bilaga **Azure AD**

Beslutsunderlagets främsta syfte är att ”fastslå” hur Eskilstuna kommun, KLK som ansvarig för det kommunövergripande IT & Digitaliseringstjänsterna, bör ställa sig till en implementering och användning av plattformen M365 - kontorsstödsplattform och tillika molntjänsten Microsoft M365, där Azure AD är den absolut grundläggande förutsättningen för användandet av plattformens tjänster.

Inkomna kommentarer från DSO överensstämmer i stora drag med tidigare synpunkter avgivna från DSO över andra liknande genomförda konsekvensbedömningar i kommunen. Det finns därför ingen anledning att i detta skede bemöta kommentarerna i detalj.

Det som i stora drag framhålls från DSO är att det är olagligt då tillräcklig skyddsnivå för registrerades personuppgifter inte är för handen enligt DSO. Vidare framhålls att materialet är ofullständigt I sina stycken och behöver kompletteras.
I föreliggande slutrapport med dess bilaga, DPIA, är det utförligt beskrivet de juridiska överväganden som behöver genomföras i ett fall som detta, vilket också omfattar den Europeiska Dataskyddsstyrelsen rekommendationer i denna fråga avseende tredjelandsöverföring.

Vad avser kommentarer kring “skyddsvärda uppgifter”, elever/barn <18 år, så hanteras dessa personuppgifter redan av kommunen i implementerade lösningar, exempelvis Intune. Frågan får därför anses belyst och avgjord.

Av den genomförda DPI: an framgår att de personuppgifts risker som ett implementerade av Azure AD skulle utgöra är av acceptabel nivå för de registrerade. Riskanalysen är genomförd med deltagare från Eskilstuna kommuns verksamheter och utgör deras bedömningar av risker.

Av slutrapportens Executive Summary ska det särskilt framhållas att i förevarande fall bör Eskilstuna kommun **utifrån en proportionerlig helhetsbedömning och med accepterande av ett visst mått av risk genomföra en implementering av Azure AD, utgörande en förutsättning för plattformen M365 som sådan.**

Materialet bedöms utgöra ett tillräckligt underlag för att Eskilstuna kommun ska kunna fatta ett beslut i föreliggande frågeställning.

Värt att också framhållas är att följa den pågående rättsutvecklingen i den juridiska frågan där så sent som den 8 maj 2023 EU-kommissionären för konkurrens och den digitala agendan uttalade att ett nytt Data Protection Framework (DPF) mellan EU och USA, är nära förestående. Utmaningar kopplade till tredjelands överföringar till USA torde därefter vara lösta.

Vidare uppmanas Eskilstuna kommuns nämnder, såsom varande ansvariga för sina respektive personuppgiftsbehandlingar, genomföra erforderliga DPI: or för nya tjänster.

DPIA-Konsekvensbedömning avseende dataskydd

Plattform M365

Innehållsförteckning

1 Övergripande information

Här uppges uppgifter om detta dokument, personuppgiftsbehandlingens identitet, ansvariga för behandlingen och medverkande vid utformningen av behandlingen.

Personuppgiftsbehandlingens identitet *Ange benämning av personuppgiftsbehandling, ett unikt id för att identifiera personuppgiftsbehandlingen samt eventuell version.*
Plattformen M365 (Azure AD personuppgifter)

Personuppgiftsansvarig(a) för personuppgiftsbehandlingen *Ange information om personuppgiftsansvarig eller gemensamt personuppgiftsansvariga.*
Kommunstyrelsen, Eskilstuna kommun **Företrädare för kommunen Niklas Narvell, IT-chef**

Verksamhet(erna) där behandlingen utförs *Ange den verksamhet där behandlingen utförs, exempelvis enhet, verksamhetsområde.*
Eskilstuna kommuns IT avdelning och Microsoft

Medverkande	
Ansvarig *Person/roll (inkl. kontaktuppgifter) med mandat att för personuppgiftsansvarigs räkning överväga, besluta och i förekommande fall fastställa konsekvensbedömning enligt artikel 35. Informationsägare eller annan roll. Se delegationsordning (verkställighet).*	IT-chef Niklas Narvell
Andra medverkande *T.ex. processansvarig, verksamhetsutvecklare, IT-strateg, informationssäkerhetsspecialist, IT-säkerhetsspecialist och personuppgiftsbiträden.*	Dataskyddssamordnare Robert Marcinkiewicz, Förvaltningsjurist SF. Rafaela Svéd, IT-säkerhetssamordnare Carolina Bengtsson, SEF, Informationssäkerhetssamordnare Rimona Hussni, VOF
Dataskyddsombud (*) (**Obligatorisk**) *Inkl. kontaktuppgifter. Dataskyddsombudet, om sådant är utsett, ska alltid rådfrågas vid konsekvensbedömning (se avsnitt 7.1).*	Charlotte Nilsson (DSO), SEF, ej kallats till DPIA-workshop.
Registrerades medverkan (**Obligatorisk information**) *Enligt artikel 35.9 ska synpunkter inhämtas från de registrerade eller deras företrädare när det är lämpligt. Om registrerade inte tillfrågas ska en motivering ges till beslutet (se avsnitt 5.4).*	Synpunkter har inte inhämtats från de registrerade. Representanter från de olika verksamheterna inom kommunen har medverkat vid DPIA-workshop av denna DPIA. Vidare har HR inkluderats i styrgruppen.

2 Sammanfattning

Sammanfattning av konsekvensbedömningen *Fylls i sist, mycket kan hämtas från avsnitt 6.*
De förekommande personuppgifterna genererar en viss risk, se nedan. Risken bedöms vara av sådan art att den registrerades rättigheter inte torde äventyras. Respektive personuppgiftsansvarig ska genomföra en egen DPIA. Denna DPIA avser Azure AD.

Sammanställning av beslut under konsekvensbedömningens gång		
Beslut om konsekvensbedömning	☒ JA ☐ NEJ	*Kommentar/motivering*
Om konsekvensbedömning genomförts, är risknivå sänkt till acceptabel nivå?	☒ JA ☐ NEJ	Ja, genom tekniska samt organisatoriska skyddsåtgärder.
Dataskyddsombudet har rådfrågats	☒ JA ☐ NEJ	*Kommentar/motivering* Dataskyddsombudet har mottagit konsekvensbedömningen den 3 maj 2023.
Dataskyddsombudets rekommendationer godtogs (om nej, motivera)	☒ JA ☐ NEJ	*Kommentar/motivering* Dataskyddsombudet (DSO) har mottagit konsekvensbedömningen. DSO har möjlighet att granska konsekvensbedömningen. Eventuellt yttrande eller frågeställningar avseende denna konsekvensbedömning ska besvaras av personuppgiftsansvarig.
Beslut om förhandssamråd	☐ JA ☒ NEJ	*Kommentar/motivering* Behandlingen leder inte till en hög risk för de registrerades fri- och rättigheter. Risker kan begränsas tillräckligt genom tekniska och organisatoriska säkerhetsåtgärder med tanke på tillgänglig teknik och kostnader.
Har förhandssamråd genomförts och risker sänkt till acceptabel nivå?	☐ JA ☒ NEJ	*Kommentar/motivering* Ej aktuellt, förhandssamråd har ej genomförts.
Gå vidare med personuppgiftsbehandlingen	☒ JA ☐ NEJ	Se ovan rubrik ”Beslut om förhandssamråd”

3 Om konsekvensbedömning

Enligt artikel 35.1 i dataskyddsförordningen är den personuppgiftsansvarige skyldig att inför en ny personuppgiftsbehandling utföra en konsekvensbedömning om en behandling sannolikt leder till en hög risk för fysiska personer rättigheter och friheter. En konsekvensbedömning kan också behöva göras om risken för en pågående personuppgiftsbehandling ändras.

En konsekvensbedömning är en process för att beskriva personuppgiftsbehandlingen, bedöma om den är nödvändig och proportionell och för att hantera risker för fysiska personers rättigheter och friheter som uppkommer genom behandlingen, genom att bedöma dessa risker och bestämma vilka åtgärder som ska vidtas. Genom en konsekvensbedömning kan man som personuppgiftsansvarig visa för de registrerade att man uppfyller de krav som ställs i dataskyddsförordningen, bland annat det grundläggande ansvaret vad gäller efterlevnad av förordningen som ligger på den personuppgiftsansvarige enligt artikel 24.1[1] i dataskyddsförordningen.

I artikel 35 hänvisas till en sannolikt hög risk ”för enskildas rättigheter och friheter”. Hänvisningen till de registrerades ”rättigheter och friheter” avser i första hand dataskydd och integritet, men kan även omfatta andra grundläggande rättigheter såsom yttrandefrihet, tankefrihet, fri rörlighet, förbud mot diskriminering, rätt till frihet, samvete och religion.

Konsekvenser för den registrerade kan orsakas både med avseende på utförandet av behandlingen, men även på behandlingens karaktär. I skäl 75[2] i dataskyddsförordningen beskrivs behandlingar som kan medföra risker och olika typer av konsekvenser för fysiska personers rättigheter och friheter. Skador som kan uppkomma kan vara fysiska, materiella eller immateriella och kan exempelvis leda till diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, obehörigt hävande av pseudonymisering eller annan betydande ekonomisk eller social nackdel, om registrerade kan berövas sina rättigheter och friheter eller hindras att utöva kontroll över sina personuppgifter.

Det finns olika metoder för att genomföra en konsekvensbedömning, men i artikel 35.7[3] stadgas fyra grundläggande krav i dataskyddsförordningen på vad en konsekvensbedömning ska innehålla.

1. En systematisk beskrivning av den planerade behandlingen och behandlingens syfte.
2. En bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftena.
3. En bedömning av riskerna för de registrerades rättigheter och friheter.
4. De åtgärder som planeras för att hantera riskerna och för att visa att dataskyddsförordningen efterlevs.

---

[1] I artikel 24.1 stadgas att ”[m]ed beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning. Dessa åtgärder ska ses över och uppdateras vid behov”.
[2] Se bilaga A.
[3] Se också skäl 84 och 90 i dataskyddsförordningen.

Som komplement till dataskyddsförordningens minimikrav har Artikel 29-gruppen[4] tagit fram kriterier för konsekvensbedömning i dokumentet Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, antagna den 4 april 2017.[5] Dessa kriterier klargör de grundläggande kraven i förordningen, men erbjuder tillräckligt utrymme för olika genomförandeformer. Kriterierna kan användas för att visa att en viss metod för konsekvensbedömning uppfyller de krav som ställs i förordningen.

Det finns situationer när en konsekvensbedömning inte behöver göras. Det gäller dels om det redan har gjorts en konsekvensbedömning för en behandling som är mycket lik den planerade behandlingen. Då kan resultatet från den tidigare konsekvensbedömningen kan användas. En konsekvensbedömning behöver inte heller genomföras om den planerade personuppgiftsbehandlingen inte sannolikt leder till en hög risk för enskildas fri- och rättigheter eller om det gäller behandlingar som har kontrollerats av en tillsynsmyndighet eller ett dataskyddsombud i enlighet med artikel 20 i direktiv 95/46/EG (dataskyddsdirektivet, det vill säga före dataskyddsförordningens ikraftträdande) och vars genomförande inte har ändrats sedan föregående kontroll.

[4] Artikel 29-gruppen är den oberoende europeiska arbetsgruppen som behandlade frågor om integritetsskydd och skydd av personuppgifter fram till den 25 maj 2018 (införande av den allmänna dataskyddsförordningen). Artikel 29-gruppen har ersatts av Europeiska dataskyddsstyrelsen (European Data Protection Board, förkortad EDPB).
[5] Kriterierna återfinns i bilaga B.

4 Tröskelanalys

Som framgått ovan ska den personuppgiftsansvarige enligt artikel 35.1 i dataskyddsförordningen inför en ny personuppgiftsbehandling (eller vid förändringar av risker avseende en pågående behandling) utföra en konsekvensbedömning om behandlingen sannolikt leder till en hög risk för fysiska personer rättigheter och friheter. Om en behandling inte sannolikt leder till en hög risk för enskildas fri- och rättigheter, behöver en konsekvensbedömning inte göras. För att ta reda på om den nya behandlingen medför en sådan risk genomförs en så kallad tröskelanalys.

Tröskelanalysen består av nio kriterier, framtagna av Integritetsskyddsmyndigheten (IMY) med stöd av Artikel 29-gruppens riktlinjer[6]. Kriterierna pekar på när en konsekvensbedömning måste genomföras innan personuppgiftsbehandlingen påbörjas.[7]

Om den planerade behandlingen uppfyller minst två av de nio kriterierna ska generellt sett en konsekvensbedömning genomföras. Även ett (1) kriterium kan tyda på att en konsekvensbedömning behöver genomföras, beroende på riskerna för de registrerades fri- och rättigheter avseende personuppgifternas behandling. En konsekvensbedömning kan således komma att behöva genomföras även om endast ett av kriterierna är uppfyllt.[8]

En behandling kan omvänt uppfylla två eller fler kriterier, men den personuppgiftsansvarige kan ändå göra bedömningen att den ”sannolikt inte leder till en hög risk”. I sådana situationer bör den personuppgiftsansvarige motivera och dokumentera anledningarna till att en konsekvensbedömning inte utförs, och inkludera/registrera dataskyddsombudets synpunkter.[9] Vid tveksamhet om konsekvensbedömning ska genomföras eller inte är rekommendationen från IMY att man genomför en konsekvensbedömning.

Nedan presenteras den tröskelanalys som genomförts inom ramarna för plattformen M365

Övergripande information	
Personuppgiftsansvarig	Kommunstyrelsen, Eskilstuna kommun
Kontaktuppgifter	KLK Eskilstuna kommun, 631 86 Eskilstuna
Företrädare	IT-chef Niklas Narvell
Dataskyddsombud	Charlotte Nilsson, ej närvarande

[6] Artikel 29-gruppen, Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, Antagna den 4 april 2017.
[7] Förteckning enligt artikel 35.4 i Dataskyddsförordningen, dnr DI-2018-13200, 2019-01-16. https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/konsekvensbedomningar-och-forhandssamrad/forteckning-over-nar-en-konsekvensbedomning-ska-goras/
[8] Artikel 29-gruppen, Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, Antagna den 4 april 2017, s. 12.
[9] Artikel 29-gruppen, Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, Antagna den 4 april 2017, s. 13.

Tröskelanalys [namn på behandling]		
Uppgift om:	**Behandling X**	**Behandling Y**
Ändamål med behandlingen	Tillhandahålla ett verktyg för att genomföra den kommunala strategin kring den digitala arbetsplatsen. Syftet med Azure AD är att hantera och organisera användare. Detta omfattar också kostnadsaspekter och behov samt beaktande av de samlade legala perspektivet för en kommun	
Kategorier av registrerade	Anställda, elever, konsulter, leverantörer	
Kategorier av personuppgifter	Förnamn, efternamn, visningsnamn, e-post, telefon nummer, grupp, titel	
Mottagare	IT-avdelningen, Eskilstuna kommun & Microsoft (uppgifterna läggs i Azure AD:et)	
Tredjelandsöverföring	Ja	
Grund för tredjelandsöverföring	Standardavtalsklausuler (SCC), organisatoriska och tekniska åtgärder	
Gallringsrutin	Pågående arbete	
Kriterier		
Behandlingen utvärderar eller poängsätter människor, till exempel ett företag som erbjuder genetiska tester till konsumenter för att bedöma och förutse risker för sjukdomar, ett kreditupplysningsföretag eller ett företag som profilerar internetanvändare.	☐ JA ☒ NEJ **Kommentar:**	☐ JA ☐ NEJ **Kommentar:**
Behandlar personuppgifter i syfte att fatta automatiserade beslut som har rättsliga följder eller liknande betygande följder för den registrerade.	☐ JA ☒ NEJ **Kommentar:**	☐ JA ☐ NEJ **Kommentar:**
Systematiskt övervakar människor, till exempel genom kameraövervakning av en allmän plats eller genom att samla in personuppgifter från internetanvändning i offentliga miljöer.	☐ JA ☒ NEJ **Kommentar:** Uppgifterna som behandlas i Azure AD innebär inte systematiskt övervakning.	☐ JA ☐ NEJ **Kommentar:**

Behandlar känsliga personuppgifter enligt artikel 9 eller uppgifter som är av mycket personlig karaktär, till exempel ett sjukhus som lagrar patientjournaler, ett företag som samlar in lokaliseringsuppgifter eller en bank som hanterar finansiella uppgifter.	☐ JA ☒ NEJ **Kommentar:** Se avsnitt 5.1 avseende attribut i AD.	☐ JA ☐ NEJ **Kommentar:**
Behandlar personuppgifter i stor omfattning.	☒ JA ☐ NEJ **Kommentar:**	☐ JA ☐ NEJ **Kommentar:"**
Kombinerar uppgifter från två eller flera behandlingar på ett sätt som avviker från vad de registrerade rimligen kunnat förvänta sig, till exempel när man samkör register.	☒ JA ☐ NEJ **Kommentar:** Flödet finns beskrivet i bilaga 1 "Skapa AD-konto"	☐ JA ☐ NEJ **Kommentar:**
Behandlar personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara, till exempel barn, anställda, asylsökande, äldre och patienter.	☒ JA ☐ NEJ **Kommentar:** Anställda och elever	☐ JA ☐ NEJ **Kommentar:**
Använder ny teknik eller nya organisatoriska lösningar, till exempel en sakernas internetapplikation (Internet of Things, IoT).	☒ JA ☐ NEJ **Kommentar:**	☐ JA ☐ NEJ **Kommentar:**
Behandlar personuppgifter i syfte att hindra registrerade från att få tillgång till en tjänst eller ingå ett avtal, till exempel när en bank granskar sina kunder mot en databas för kreditupplysning för att besluta om de ska erbjudas lån.	☐ JA ☒ NEJ **Kommentar:**	☐ JA ☐ NEJ **Kommentar:**
Övriga faktorer[10]	☐ JA	☐ JA

[10] Exempel på övriga faktorer som kan påverka bedömningen av om en konsekvensbedömning ska göras är om
- tjänsteleverantören omfattas av extraterritoriell lagstiftning oavsett var denne bedriver sin verksamhet i världen,
- det förekommer tredjelandsöverföring,
- behandlingen innefattar komplexa molntjänstavtal,
- leverantören anlitar ett flertal samarbetspartners med vilka denne delar registrerades uppgifter avseende olika ändamål, såsom marknadsföring, support, felsökning, forskning m.m.,
- det förekommer en stor mängd personuppgiftsbiträden och underbiträden i Sverige och utomlands, eller

	☒ NEJ **Kommentar:**	☐ NEJ **Kommentar:**
Beslut	☒ **Konsekvensbedömning ska genomföras.** ☐ **Konsekvensbedömning ska ej genomföras.**	
Motivering till beslut	Mer än två kriterier i tröskelanalysen har besvarats med Ja	

- det är stor förekomst av kakor (cookies) i leverantörens applikationer och websida som har andra funktioner än att bara vara nödvändiga för tjänstens funktionalitet, t.ex. marknadsföring och analys.

5 Konsekvensbedömning avseende dataskydd och förhandssamråd

5.1 Systematisk beskrivning av behandlingen och dess syften

Konsekvensbedömningen ska enligt artikel 35.7 a till att börja med innehålla en systematisk beskrivning av den planerade behandlingen och behandlingens syften. Beskrivningen anses tillräckligt omfattande för att kunna sägas uppfylla kraven i dataskyddsförordningen, om följande kriterier beaktas.

- Behandlingens art, omfattning, sammanhang och ändamål beaktas (skäl 90).
- Registrering av personuppgifter, mottagare och den period under vilken personuppgifterna kommer att lagras.
- En funktionell beskrivning av behandlingen tillhandahålls.
- De tillgångar som är nödvändiga för personuppgifterna (maskinvara, programvara, nätverk, personer, papper eller spridningskanaler för papper) är identifierade.
- Efterlevnad av godkända uppförandekoder beaktas (artikel 35.8).[11]

I det här avsnittet finns olika punkter samlade i olika tabeller, som underlag för att ge en beskrivning som beaktar kriterierna ovan. Uppge beskrivningar på tillräckligt detaljerad nivå för att kunna upptäcka om det finns brister i dataskyddet som kan ge upphov till händelser som riskerar de registrerade rättigheter och friheter. Redan befintliga beskrivningar kan användas, men se till att rätt version är kopplad till konsekvensbedömningsdokumentationen.

Beskrivning av behandling

I nedanstående tabell anges olika punkter med fokus på de två första kriterierna i punktlistan ovan, det vill säga behandlingens art, omfattning, sammanhang och ändamål samt registrering av personuppgifter, mottagare och den period under vilken personuppgifterna kommer lagras.

Uppgifter som ska finnas i registerförteckning enligt artikel 30 är markerade med (*).

Beskrivning av behandling	
Benämning på behandling	Plattformen M365 (Azure AD personuppgifter)
Personuppgiftsansvarig eller gemensamt personuppgiftsansvariga (*)	Kommunstyrelsen, Eskilstuna kommun
Dataskyddsombud (*)	Charlotte Nilsson, ej kallad till Workshop-DPIA
Ändamål (*)	Tillhandahålla ett verktyg för att genomföra den kommunala strategin kring den digitala arbetsplatsen. Detta omfattar också kostnadsaspekter och behov samt beaktande av de samlade legala perspektivet för en kommun
Kategorier av registrerade (*)	Anställda, elever, konsulter, leverantörer

[11] Se Artikel 29-gruppen, Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, Antagna den 4 april 2017, Bilaga 2.

Kategorier av personuppgifter (*)	Förnamn, efternamn, visningsnamn, e-post, telefon nummer, grupp, titel – se bilaga 1, tjänsteanteckning
Behandlas känsliga personuppgifter? (*, del av kategorier av personuppgifter)	Attribut finns i lokalt AD/Azure AD som består Skola-Klass. Av attribut kan det då framgå att en elev studerar i grundsärskola (namn på skolan kan indikera detta).
Behandlas personuppgifter som faller utanför kategorierna för känsliga personuppgifter, men som kan vara särskilt skyddsvärda eller har högt integritetsvärde för den registrerade?	Nej
Mottagare/Kategorier av mottagare (*) **inbegripet mottagare i tredjeländer**	Eskilstunas IT & Digitalisering och Microsoft
Sker överföringar till tredjeländer? Om ja, vilket tredje land? (*) Vilken överföringsmekanism används? Är en Transfer Impact Assessment (TIA) planerad att genomföras? Vilka säkerhetsåtgärder? (*)	Ja, till USA. Överföringsmekanism – SCC (Microsofts OST inkl DPA) Skyddsåtgärder – artikel 32. Det rättsliga läget har beskrivits i ”Slutrapport – Eskilstuna kommun: beslutsunderlag Azure AD, Plattform M365”. TIA har ej genomförts. Om en TIA ska genomföras kommer utredas. Exakt tidsaspekt för detta är för närvarande inte fastställt.
Tidsfrister/Lagringstid/Behandlingstid (*)	Pågående arbete inkl process
Om möjligt, allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder enligt artikel 32.1 (*)	Multifaktorsautentisering på administratörskonton, automatiserade processer för synk av konton. Dokumenterade rutiner för radering av konton. Behörighetsstyrning för administration av konton.
Omfattning. *T.ex. antal registrerade, mängden uppgifter, antal kategorier av uppgifter, varaktighet, geografisk omfattning.*	Ca 10 000 anställda, elever ca 20 000, leverantörer och konsulter (inga kända uppgifter)
Varifrån kommer uppgifterna? *Från registrerad/någon annanstans?*	I en onboarding i Personec (HR personalsystem), samt i skoladministrativ plattform. Se bilaga 1 ”Skapa AD-konto”
Annan information om behandlingen.	Eskilstuna kommun har genom att endast använda sig av ett begränsat antal personuppgifter i Azure AD, riskmitigerat sin behandling

Funktionell beskrivning av behandlingen

Infoga (eller bifoga) en schematisk bild över hur personuppgifterna flödar, som inkluderar externa mottagare för uppgifterna. Om uppgifter överförs till andra länder ska detta framgå av bilden.

Se bilaga 2

Den schematiska bilden kompletteras med en mer detaljerad beskrivning av dataflöden (mellan system och aktörer) och viss teknisk information i rutan nedan. Här anges till exempel överföring mellan olika interna och externa aktörer, överföring mellan olika rättssystem (tredje land), logiska

och tekniska beskrivningar, till exempel information om databaser, tabeller och fält innehållandes personuppgifter och hur personuppgifter flödar mellan olika parter och gränssnitt, inkluderat detaljer om portar, protokoll, API:er, och kryptering.

Beskrivning av dataflöden och viss teknisk information
• Användardata skapas i källsystem (Personalsystem/elevregister). Data hämtas från Skatteverket. • Data hämtas till identitetssynkmotor via webservice (krypterat med SSL). • Synkas till AD via identitetssynkmotor. • Synkas från AD till Azure AD via Azure AD Connect med TLS/SSL.

Den funktionella beskrivning kompletteras i rutan nedan med en beskrivning av process/rutin. Beskrivningen behövs för att kunna identifiera eventuella risker och även för att behandlingen ska utformas på ett sätt som tar hänsyn till skyddet av personuppgifter och risker för de registrerades rättigheter. Här kan refereras till befintliga modeller om sådana finns. Med fördel kan olika delar av behandlingen beskrivas, även genom hela livscykeln för uppgifter såsom insamling av personuppgifter, olika typer av hantering (till exempel sammanslagning, strukturering, hämtning, användning, ändring), överföringar, restriktioner (till exempel åtkomst), lagring och radering/gallring.

Beskrivning av process/rutin
AD-kontot inaktiveras (vid ex. avslut av anställning) vilket leder till att synkning till Azure AD inte sker. I Azure ligger det sedan i en ”papperskorg” i 30 dagar innan det raderas. I AD ligger det inaktivt i 90 dagar innan det tas bort helt. Det som finns kvar efter 90 dagar (i AD) är användarnamn och epostadress kopplat till personnummer så att en person kan få tillbaka dessa om de börjar på kommunen igen.

Identifiera de tillgångar som behövs för att kunna genomföra behandlingen

I den här delen identifieras de tillgångar som är nödvändiga för personuppgifterna, det vill säga det fjärde kriteriet i punktlistan ovan. Detta avser maskinvara, programvara, nätverk, personer, papper eller spridningskanaler för papper. Till exempel ska det här framkomma om e-post används för att informera den registrerade i något ärende. Observera att även personer som är nödvändiga för personuppgifterna ska identifieras, vilket innebär att roller och funktioner inom organisationen som behövs för att genomföra behandlingen också omfattas av detta kriterium.

Identifiera de tillgångar som behövs för att kunna genomföra behandlingen
Azure AD

Efterlevnad av godkända uppförandekoder

Här redogörs för om det finns en uppförandekod (områdesspecifika bestämmelser kring personuppgiftsbehandlingar). Om ja, vilken? Om uppförandekod finns ska de tas i beaktande.

Uppförandekod
Nej: Microsoft har inga godkända uppförandekoder utifrån artikel 40, 42 samt 43 GDPR.

5.2 Behovet av och proportionaliteten hos behandlingen

5.2.1 Inledning

Utöver en systematisk beskrivning av den planerade behandlingen och dess syften ska konsekvensbedömningen också enligt artikel 35.7 b i dataskyddsförordningen innehålla en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftena. Detta omfattar en bedömning av hur de grundläggande dataskyddsprinciperna i artikel 5 i dataskyddsförordningen uppfylls, närmare bestämt principerna om

- Laglighet
- Ändamål
- Uppgiftsminimering
- Lagringsminimering[12]

Kravet på en bedömning av behovet av och proportionaliteten hos behandlingen omfattar också en bedömning av åtgärder som stärker den registrerades rättigheter. Åtgärderna kan vara organisatoriska, som framtagande av en rutin för handläggning och att utse ansvariga, och tekniska, till exempel att alla personuppgifter i ett system går att utsöka. För att åtgärderna ska kunna anses vara effektiva ska de utgå från behandlingen och dess ändamål.

5.2.2 Uppfyllande av grundläggande principer

Laglighet	
Rättslig grund för behandlingen (artikel 6) *Ange rättslig grund och motivera valet*	M*yndighetsutövning, Allmänt intresse, Avtal*
Rättslig grund för att behandla känsliga personuppgifter (artikel 9) *Ange rättslig grund och motivera valet*	N/*A*

Ändamål	
Ändamålet med behandlingen	Tillhandahålla ett verktyg för att genomföra den kommunala strategin kring den digitala arbetsplatsen. Detta omfattar också kostnadsaspekter och behov samt beaktande av de samlade legala perspektivet för en kommun
Finns andra sätt än den planerade behandlingen för att uppnå ändamålet?	Nej, inte ett 1:1 förhållande med motsvarande funktionalitet
Nödvändighet	
Om den <u>rättsliga grunden är samtycke</u>:	N/A

[12] Principerna som stadgas i artikel 5.1 a-f i dataskyddsförordningen är principen om laglighet, korrekthet och öppenhet, principen om ändamålsbegränsning, principen om uppgiftsminimering, principen om riktighet, principen om lagringsminimering och principen om integritet och konfidentialitet. I denna mall har endast de principer tagits med som anges i kriterierna för en tillräckligt omfattande konsekvensbedömning i Artikel 29-gruppens riktlinjer. (Se Artikel 29-gruppen, Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, Antagna den 4 april 2017, Bilaga 2.)

- Beskriv/motivera varför detta sätt att uppnå ändamålet har valts, snarare än något av de andra sätt som angetts ovan?	
Om den <u>rättsliga grunden är *annan* än samtycke</u>: **- Är behandlingen nödvändig för att uppnå ändamålet?** *Motivera* **- Beskriv/motivera varför detta sätt att uppnå ändamålet har valts, snarare än något av de andra sätt som angetts ovan?**	Tillhandahålla ett verktyg för att genomföra den kommunala strategin kring den digitala arbetsplatsen. Detta omfattar också kostnadsaspekter och behov samt beaktande av de samlade legala perspektivet för en kommun
Hur motverkas ändamålsglidning?	
Har ni identifierat alla ändamål för behandlingen?	Ja, såvitt känt
Är alla ändamål förenliga med det ursprungliga ändamålet?	Ja, såvitt känt
Finns det risk för att personuppgifter kommer att bli återanvända för andra ändamål (gradvis, ”obemärkt”)?	Nej mot bakgrund av vad som framkommit är detta redan reglerat
Hur begränsa till enbart det definierade ändamålet?	Systemkrav – Azure AD uppgifter har redan begränsats, policys

Uppgiftsminimering *Redogör för både tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna är adekvata, relevanta och inte för omfattande i förhållande till det specificerade ändamålet.*	
Är de kategorier av personuppgifter som behandlas tillräckliga för ändamålet?	Ja, såvitt känt
Behandlas fler kategorier av personuppgifter än nödvändigt för ändamålet?	Nej
Finns det tydliga instruktioner för vad som är obligatorisk information och frivillig information i exempelvis blanketter?	Såvitt känt är Azure AD:et uppsatt enligt instruktioner. Se bilaga 1
Finns kunskap om hur undvika identifiering (om nödvändigt) vid statistiska ändamål?	N/A

Lagringsminimering	
Finns det lagstadgad gallring för uppgifterna? Om ja, följs den?	Såvitt känt finns ingen lagstadgad gallringsregel för Azure AD uppgifter.
Hur länge behöver uppgifter lagras? *Ange för respektive ändamål*	Så länge som uppgifter om den registrerade behövs (kopplat till Personec och HR´s rutiner) Elevdata – så länge eleven har sin skolplikt enligt Skollagen
Kan det särskiljas olika lagringstid för olika delar av uppgifterna?	Inte av de aktuella Ad uppgifterna

Om uppgifterna inte kan raderas just nu, kan åtkomsten till dem stoppas?	Ja det kan de, de kan flyttas till ett ”mellanlager” – non accessable
Finns det automatisk radering/gallring av uppgifter?	Efter mellanlagring + 90 dagar

5.2.3 Bedömning av åtgärder som stärker den registrerades rättigheter

Information till den registrerade *Beskriv hur information om personuppgiftsbehandlingen utformats och kommer att lämnas till den registrerade.*	
Artikel 12 – Klar och tydlig information och kommunikation samt klara och tydliga villkor för utövandet av den registrerades rättigheter	Onboarding/HR rutiner
Artikel 13 – Information när registrerad själv lämnat uppgifterna	Se ovan
Artikel 14 – Information när uppgifterna inte erhållits från den registrerade	Alla uppgifter hämtas från system, se bilaga 1 ” Skapa AD-konto”

Rätt till tillgång och till dataportabilitet *Ange hur den registrerades rätt till tillgång och dataportabilitet säkerställs.*	
Artikel 15 – Rätt till tillgång	N/A
Artikel 20 – Rätt till dataportabilitet	N/A

Rätt till rättelse och radering *Ange hur den registrerades rätt till rättelse och radering säkerställs samt hur det säkerställs att personuppgifter som raderas inte går att återskapa.*	
Artikel 16 – Rätt till rättelse	Rättelse sker i HR personalsystem/Personec och Extens
Artikel 17 – Rätt till radering	Se ovan
Artikel 19 – Anmälningsskyldighet till mottagare	N/A

Rätt att göra invändningar och begränsning av behandling *Ange hur den registrerades rätt att göra invändningar och rätt till begränsning av personuppgiftsbehandling säkerställs.*	
Artikel 18 – Rätt till begränsning av behandling	N/A
Artikel 19 – Anmälningsskyldighet till mottagare	N/A
Artikel 21 – Rätt att göra invändningar	Detta styrs av gällande processer och krav

Förhållandet till personuppgiftsbiträden *Redovisa förhållandet till personuppgiftsbiträden (PuB-avtal)*	
Artikel 28 – Personuppgiftsbiträden	SCC inkl DPA (Microsoft)

Skyddsåtgärder för internationella överföringar *Om tredjelandsöverföring förekommer, beskriv överföringarna och ange vilka överföringsmekanismer som använts för överföringarna samt motivera varför dessa är tillämpliga.*	
Kapitel V	SCC, administrativa och tekniska säkerhetsåtgärder, Informationssäkerhets anvisning, risk resonemang

Förhandssamråd[13]	
Förhandsamråd vid behov (registrerade bör i vissa fall tillfrågas vid utformning av behandling)	N/A

Övrigt	
Artikel 22 – Rätt till att inte bli föremål för behandlingen enligt artikel 22 Automatiserat individuellt beslutsfattande, inbegripet profilering	N/A
Artikel 34 – Information till den registrerade om en personuppgiftsincident	Onboarding process /paket med information

5.2.4 Sammanfattning

Sammanfattande tabell
I rutan nedan sammanfattas bedömningen om personuppgiftsansvarig uppfyller de grundläggande principerna vid personuppgiftsbehandlingen. *Se till att sammanfattningen tydligt ger svar på behovet av och proportionaliteten hos behandlingen.*
De förekommande personuppgifterna genererar en viss risk, se nedan. Risken bedöms vara av sådan art att den registrerades rättigheter inte torde äventyras.
I rutan nedan sammanfattas bedömningen av planerade åtgärder för att stärka de registrerades rättigheter
Planeras inom återkommande rutin arbete, del i kontinuerlig uppföljning

5.3 Bedömning av risker för registrerades rättigheter och friheter

5.3.1 Inledning

Målet med en konsekvensbedömning avseende dataskydd är att minimera risker för den registrerades rättigheter och friheter. För att möjliggöra detta ska i samband med konsekvensbedömningen en riskbedömning göras, där man hanterar risker för kränkningar av den registrerades rättigheter och friheter, det vill säga risker som kan resultera i negativa konsekvenser för enskilda individer.

[13] Se bilaga D.

Riskbedömningsdelen av en konsekvensbedömning ska innehålla följande:

- Riskens ursprung (orsak/sårbarhet) (skäl 90 i dataskyddsförordningen).
- Identifiering av möjliga konsekvenser för den registrerades rättigheter och friheter vid händelser, däribland obehörig åtkomst, oönskad ändring och förlust av uppgifter.
- Identifiering av hot som kan leda till obehörig åtkomst, oönskad ändring och förlust av personuppgifter (personuppgiftsincident).
- Uppskattning av sannolikhetsgrad och konsekvensgrad (skäl 90 i dataskyddsförordningen).
- Fastställande av planerade åtgärder för att minska eller eliminera dessa risker (artikel 35.7 d i dataskyddsförordningen och skäl 90 i dataskyddsförordningen).[14]

Riskbedömningsdelen av en konsekvensbedömning kan av praktiska skäl genomföras samtidigt som en riskbedömning avseende informationssäkerhet. Det är dock viktigt att värdera och dokumentera de risker som tillhör konsekvensbedömningen separat. Detta för att riskbedömningen i samband med konsekvensbedömningen endast ska fokusera på risker för den registrerade och inte organisationen, eftersom det bara är den registrerades perspektiv som är av relevans i en konsekvensbedömning.

Hänvisa till aktuellt riskbedömningsdokument (diarienummer eller motsvarande beständigt referensnummer) eller bifoga riskerna och de riskreducerande åtgärderna i sin helhet till detta dokument. Se bilaga C till stöd vid genomförande.

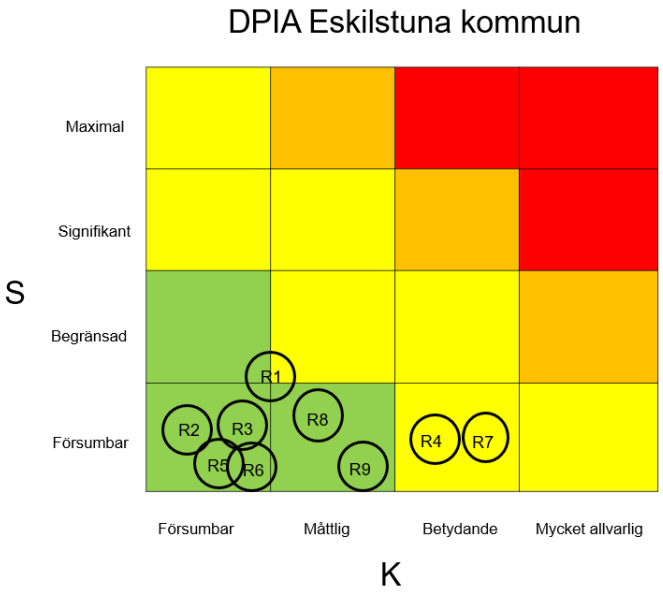
5.3.2 Riskdokumentation

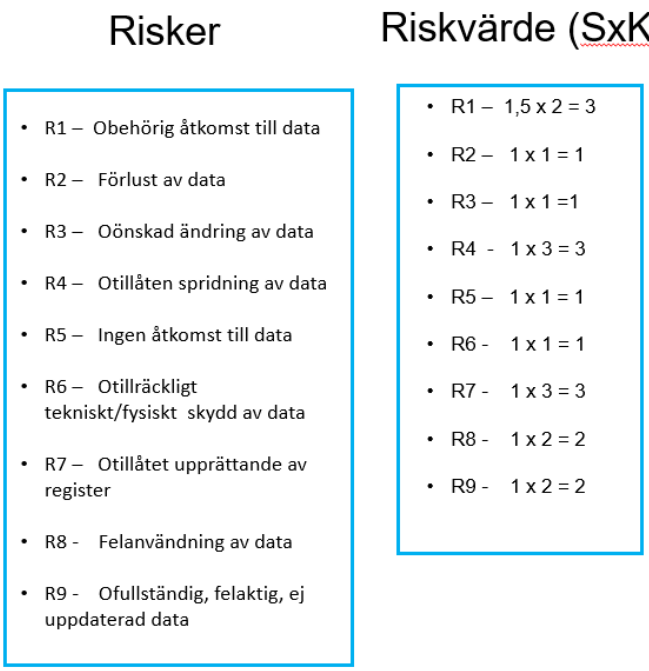
Identifiering av åtgärder för att hantera riskerna

Identifiera tekniska och organisatoriska åtgärder för att eliminera eller minska allvarsgrad av konsekvenserna och sannolikheten för riskerna.

[14] Artikel 29-gruppen, Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, Antagna den 4 april 2017, Bilaga 2.

ID	Personuppgifter som bedöms	Händelse	Orsak till händelsen	Sannolikhet	Konsekvens
R1	förnamn, efternamn, "visningsnamn", e-post, titel, tfn nr, grupp	Obehörig åtkomsttill data	Amerikanska myndigheter åtkomst till data begär ut uppgifter av Microsoft (MS)	Försumbar/Begränsad	Måttlig
R2	förnamn, efternamn, "visningsnamn", e-post, titel, tfn nr, grupp	Förlust av data	MS får en betydande störning vilken medför att Eskilstunas data går förlorad	Försumbar	Försumbar
R3	förnamn, efternamn, "visningsnamn", e-post, titel, tfn nr, grupp	Oönskad ändring av data	MS ändrar i Eskilstunas data utan att kommunen givit instruktioner om det	Försumbar	Försumbar
R4	förnamn, efternamn, "visningsnamn", e-post, titel, tfn nr, grupp	Otillåten spridning av data	MS publicerar/ använder uppgifterna för andra ändamål an vad som framgår av DPA/PuB	Försumbar	Betydande
R5	förnamn, efternamn, "visningsnamn", e-post, titel, tfn nr, grupp	Ingen åtkomst till data	Systemtekniskt fel kan förekomma	Försumbar	Försumbar
R6	förnamn, efternamn, "visningsnamn", e-post, titel, tfn nr, grupp	Otillräckligt tekniskt/fysiskt skydd av data	Otillräckligt tekniskt skydd – egen åtkomst, teknisk förmåga är stor, M365 använder state of the Art – kommunden kanske inte har alla förmågor	Försumbar	Försumbar
R7	förnamn, efternamn, "visningsnamn", e-post, titel, tfn nr, grupp	Otillåtet upprättande av register	Amerikanska myndigheter upprättar ett register	Försumbar	Betydande
R8	förnamn, efternamn, "visningsnamn", e-post, titel, tfn nr, grupp	Felanvändning av data	MS använder IP addresser och annan data på annat sätt än vad som stipuleras I DPA	Försumbar	Måttlig
R9	förnamn, efternamn, "visningsnamn", e-post, titel, tfn nr, grupp	Ofullständig, felaktig, ej uppdaterad data	Systemtekniska fel som PuA gör genomförs eller implemeteras inte	Försumbar	Måttlig





Planerade åtgärder

ID	Planerade åtgärder	Ev. fler kolumner med info om t.ex. ansvarig för åtgärd eller handlingsplan
	Pågående arbete avseende gallringsrutiner, processer	
	Eventuellt bör kommunen genomföra en transfer Impact Assessment (TIA) för Azure AD uppgifterna	
	Följa den rättsliga utvecklingen avseende tredjelands överföringar och bedöma eventuella åtgärder att vidta.	

5.3.3 Kvarstående höga risker

Dokumentera de risker från riskbedömningsdelen av konsekvensbedömningen som är fortsatt höga efter att riskreducerande åtgärder har vidtagits.

ID	Riskscenario *(hot, aktör och konsekvenser)*	Riskreducerande åtgärder	Riskvärde efter åtgärder	Kommentar
	Se ovanstående riskanalys. Några kvarstående höga risker har			

	inte bedömts finnas i analysen			

5.4 Medverkan från berörda parter

Enligt Artikel 29-gruppens riktlinjer omfattar minimikraven för innehållet i en konsekvensbedömning medverkan från berörda parter enligt följande.

- Rådfrågan av dataskyddsombudet (artikel 35.2).
- När så är lämpligt, inhämtning av synpunkter från de registrerade eller deras företrädare (artikel 35.9).

Om krav på en konsekvensbedömning föreligger, det vill säga om det sannolikt föreligger en hög risk för den registrerades rättigheter och friheter, ska dataskyddsombud enligt artikel 35.2 i dataskyddsförordningen rådfrågas om konsekvensbedömningen, vilket ska dokumenteras i denna ruta. Rutan får endast fyllas i av dataskyddsombudet.

Dataskyddsombudets bedömning och rekommendationer
Se skrivelse från DSO

Enligt artikel 35.9 i dataskyddsförordningen ska synpunkter inhämtas från de registrerade eller deras företrädare när det är lämpligt. Detta dokumenteras i nedanstående ruta.

Inhämtning av synpunkter från de registrerade eller deras företrädare	
Har ni rådgjort med registrerade eller deras företrädare?	☒ JA ☐ NEJ
Om ja: Redogör för dessa synpunkter.	Representanter har deltagit i denna DPIA, se ovan. HR har även inkluderats i styrgruppen.
Om nej: Motivera varför ni bedömer att det inte är lämpligt att inhämta eller följa synpunkter från de registrerade.	

6 Slutlig, sammantagen bedömning

De som genomfört konsekvensbedömningen ska här skriva en sammantagen bedömning med rekommendationer.

Sammantagen bedömning och rekommendationer
De förekommande personuppgifterna genererar en viss risk, se ovanstående analys. Risken bedöms vara av sådan art att den registrerades rättigheter inte torde äventyras. En rekommendation är att implementera och tillhandahålla en användning av Plattformen M365 med de noterade personuppgifterna i Azure AD för kommande tjänster i M365. Det ska noteras att respektive förvaltning inom kommunen måste själva ta ställning till hur de önskar använda plattformen och därmed vilken information som ska läggas i verktyget utifrån sin informationsklassificering samt att de dessförinnan genomför en DPIA.

Dataskyddsombudet har rådfrågats	☐ JA ☐ NEJ	*Kommentar/motivering* Se avsnitt 2
Dataskyddsombudets rekommendationer godtogs (**om nej, motivera**)	☐ JA ☐ NEJ	*Kommentar/motivering* Delar av de synpunkter som DSO har framfört har korrigerats i DPIA: n. DSO påtalar i sina rekommendationer vikten av att de registrerade behöver få information om vad det innebär. Vid övergång till M365 ska samtliga medarbetare få såväl information om registrering och även utbildning i användande av M365. Kommunledningskontoret delar DSO: s synpunkter om att varje nämnd ska genomföra nya DPIA för att bedöma de risker som finns inom respektive nämnd för användning av de olika tjänsterna inom M365. Kommunledningskontoret delar däremot inte DSO: s invändning att införande av M365 kommer innebära hantering av personuppgifter av barn. Däremot kan användandet av Azure för Microsoftprodukter inom skolan innebära risker för hantering av känsliga personuppgifter. Där ser kommunledningskontoret att skolnämnderna behöver se över informationshanteringen. DSO påtalar om en olämplighet att nyttja den tilltänkta leverantören för rekommendationer. Detta är felaktigt då det är Eskilstuna

		kommuns ramavtalade licenspartner Atea vilka nyttjats för att erhålla en opartisk analys och rekommendationer.
Beslut om förhandssamråd	☐ JA ☐ NEJ	*Kommentar/motivering*
Gå vidare med personuppgiftsbehandlingen	☐ JA ☐ NEJ	*Kommentar/motivering*

Bilaga A Refererade artiklar och skäl i dataskyddsförordningen

Artikel 5 i dataskyddsförordningen – Principer för behandling av personuppgifter

1. Vid behandling av personuppgifter ska följande gälla:
   a) Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (*laglighet, korrekthet och öppenhet*).
   b) De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska inte anses vara oförenlig med de ursprungliga ändamålen (*ändamålsbegränsning*).
   c) De ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (*uppgiftsminimering*).
   d) De ska vara riktiga och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål (*riktighet*).
   e) De får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, under förutsättning att de lämpliga tekniska och organisatoriska åtgärder som krävs enligt denna förordning genomförs för att säkerställa den registrerades rättigheter och friheter (*lagringsminimering*).
   f) De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (*integritet och konfidentialitet*).
2. Den personuppgiftsansvarige ska ansvara för och kunna visa att punkt 1 efterlevs (*ansvarsskyldighet*).

Artikel 6.1 i dataskyddsförordningen – Laglig behandling av personuppgifter

1. Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:
   a) Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.
   b) Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås. c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.
   c) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.
   d) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

e) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

Led f i första stycket ska inte gälla för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter.

Skäl 4 i dataskyddsförordningen

Behandlingen av personuppgifter bör utformas så att den tjänar människor. Rätten till skydd av personuppgifter är inte en absolut rättighet; den måste förstås utifrån sin uppgift i samhället och vägas mot andra grundläggande rättigheter i enlighet med proportionalitetsprincipen. Denna förordning respekterar alla grundläggande rättigheter och iakttar de friheter och principer som erkänns i stadgan, såsom de fastställts i fördragen, särskilt skydd för privat- och familjeliv, bostad och kommunikationer, skydd av personuppgifter, tankefrihet, samvetsfrihet och religionsfrihet, yttrande- och informationsfrihet, näringsfrihet, rätten till ett effektivt rättsmedel och en opartisk domstol samt kulturell, religiös och språklig mångfald.

Skäl 75 i dataskyddsförordningen

Risken för fysiska personers rättigheter och friheter, av varierande sannolikhetsgrad och allvar, kan uppkomma till följd av personuppgiftsbehandling som skulle kunna medföra fysiska, materiella eller immateriella skador, i synnerhet om behandlingen kan leda till diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, obehörigt hävande av pseudonymisering eller annan betydande ekonomisk eller social nackdel, om registrerade kan berövas sina rättigheter och friheter eller hindras att utöva kontroll över sina personuppgifter, om personuppgifter behandlas som avslöjar ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse eller medlemskap i fackförening, om genetiska uppgifter, uppgifter om hälsa eller sexualliv eller fällande domar i brottmål samt överträdelser eller därmed sammanhängande säkerhetsåtgärder behandlas, om personliga aspekter bedöms, framför allt analyser eller förutsägelser beträffande sådant som rör arbetsprestationer, ekonomisk ställning, hälsa, personliga preferenser eller intressen, tillförlitlighet eller beteende, vistelseort eller förflyttningar, i syfte att skapa eller använda personliga profiler, om det sker behandling av personuppgifter rörande sårbara fysiska personer, framför allt barn, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.

Skäl 84 i dataskyddsförordningen

I syfte att sörja för bättre efterlevnad av denna förordning när behandlingen sannolikt kan innebära en hög risk för fysiska personers rättigheter och friheter, bör den personuppgiftsansvarige vara ansvarig för att en konsekvensbedömning utförs avseende dataskydd för att bedöma framför allt riskens ursprung, art, särdrag och allvar. Resultatet av denna bedömning bör beaktas vid fastställandet av de lämpliga åtgärder som ska vidtas för att visa att behandlingen av personuppgifter är förenlig med denna förordning. I de fall en konsekvensbedömning avseende dataskydd ger vid handen att uppgiftsbehandlingen medför en hög risk, som den personuppgiftsansvarige inte kan begränsa genom lämpliga åtgärder med avseende på tillgänglig teknik och genomförandekostnader, bör ett samråd med tillsynsmyndigheten ske före behandlingen.

Skäl 90 i dataskyddsförordningen

I sådana fall bör den personuppgiftsansvarige före behandlingen, med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt upphovet till risken, göra en konsekvensbedömning avseende dataskydd i syfte att bedöma den höga riskens specifika sannolikhetsgrad och allvar. Konsekvensbedömningen bör främst innefatta de planerade åtgärder, skyddsåtgärder och mekanismer som ska minska denna risk, säkerställa personuppgiftskyddet och visa att denna förordning efterlevs.

Bilaga B Minimikrav för konsekvensbedömning

Artikel 35.7 i dataskyddsförordningen
Bedömningen ska innehålla åtminstone

a) en systematisk beskrivning av den planerade behandlingen och behandlingens syften, inbegripet, när det är lämpligt, den personuppgiftsansvariges berättigade intresse,
b) en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftena,
c) en bedömning av de risker för de registrerades rättigheter och friheter som avses i punkt 1, och
d) de åtgärder som planeras för att hantera riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna och för att visa att denna förordning efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.

Artikel 29-gruppens riktlinjer[15]
Arbetsgruppen föreslår följande kriterier som kan användas av personuppgiftsansvariga för att bedöma huruvida en konsekvensbedömning, eller en metod för att utföra en konsekvensbedömning, är tillräckligt omfattande för att iaktta förordningen:

- En systematisk beskrivning av behandlingen tillhandahålls (artikel 35.7 a):
  - Behandlingens art, omfattning, sammanhang och ändamål beaktas (skäl 90).
  - Registrering av personuppgifter, mottagare och den period under vilken personuppgifterna kommer att lagras.
  - En funktionell beskrivning av behandlingen tillhandahålls.
  - De tillgångar som är nödvändiga för personuppgifterna (maskinvara, programvara, nätverk, personer, papper eller spridningskanaler för papper) är identifierade.
  - Efterlevnad av godkända uppförandekoder beaktas (artikel 35.8).
- En bedömning av behovet av och proportionaliteten hos behandlingen (artikel 35.7 b):
  - De planerade åtgärderna för att visa att förordningen efterlevs har fastställts (artikel 35.7 d och skäl 90), med beaktande av följande:
    - Åtgärder som bidrar till att behandlingen är proportionell och nödvändig på grundval av
      - särskilda, uttryckligt angivna och berättigade ändamål (artikel 5.1 b),
      - laglig behandling (artikel 6),
      - adekvata, relevanta och inte för omfattande uppgifter (artikel 5.1 c),
      - begränsad lagringstid (artikel 5.1 e).
    - Åtgärder som stärker de registrerades rättigheter:

[15] Artikel 29-gruppen, Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, Antagna den 4 april 2017, bilaga 2.

- Information till den registrerade (artiklarna 12, 13 och 14).
- Rätt till tillgång och till dataportabilitet (artiklarna 15 och 20).
- Rätt till rättelse och radering (artiklarna 16, 17 och 19).
- Rätt att göra invändningar och till begränsning av behandling (artiklarna 18, 19 och 21).
- Förhållandet till personuppgiftsbiträden (artikel 28).
- Skyddsåtgärder för internationella överföringar (kapitel V).
- Förhandssamråd (artikel 36).

- Hantering av risker för de registrerades rättigheter och friheter (artikel 35.7 c):
  - Uppskattning av riskens ursprung, art, särdrag och allvar (se skäl 84) eller, mer specifikt, för varje risk (obehörig åtkomst, oönskad ändring och att uppgifter försvinner) ur de registrerades perspektiv:
    - Beaktande av riskens ursprung (skäl 90).
    - Identifiering av möjliga konsekvenser för de registrerades rättigheter och friheter vid händelser, däribland obehörig åtkomst, oönskad ändring och förlust av uppgifter.
    - Identifiering av hot som kan leda till obehörig åtkomst, oönskad ändring och förlust av uppgifter.
    - Uppskattning av sannolikhetsgrad och allvar (skäl 90).
  - Fastställande av planerade åtgärder för att hantera dessa risker (artikel 35.7 d och skäl 90).
- Medverkan från berörda parter:
  - Rådfrågan av dataskyddsombudet (artikel 35.2).
  - När så är lämpligt, inhämtning av synpunkter från de registrerade eller deras företrädare (artikel 35.9)."

Bilaga C Bedömning av allvarsgrad och sannolikhetsnivå

Bedömning av allvarsgrad och sannolikhetsnivå - utgå från förutbestämda bedömningskriterier.

Med GDPR och EDPB:s riktlinjer som grund, och metod för risk- och konsekvensbedömning inom informationssäkerhet som inspiration ges här ett förslag på nivåer för bedömning av allvarsgrader för konsekvenser för en behandling, och sannolikhetsnivå för att hot/händelse ska ske som ligger till grund för konsekvensen.

Bestäm först bedömningsnivåer för allvarsgrad och sannolikhet (jmf med Informationssäkerhet.se - Stöd för systematiskt arbete med informationssäkerhet i organisationer (informationssakerhet.se)), till exempel:

Allvarsgrad/Bedömning av konsekvens om den sker (inom parantes IMY:s nivåer vid personuppgiftsincidentsanmälan)	Beskrivning (generell, behöver bedömas med avseende på olika rättigheter och friheter)	Sannolikhetsnivå Sannolikhet att hot/händelse som medför risk sker
1 Försumbar (Obetydlig)	Försumbar skada eller kränkning för de registrerade	1 Försumbar
2 Måttlig (Begränsad)	Måttlig skada eller kränkning för de registrerade.	2 Begränsad
3 Betydande (Betydande)	Betydande skada eller kränkning för de registrerade	3 Signifikant
4 Mycket allvarlig (Mycket allvarlig)	Mycket allvarlig skada eller kränkning för de registrerade	4 Maximal

Bilaga D Förhandssamråd

Om personuppgiftsansvarig inte kan genomföra åtgärder som kan minska risken för de registrerades rättigheter för behandlingen, och ändå vill påbörja behandlingen eller genomföra ändring av behandling som ger högre risk, kan ett förhandssamråd begäras med IMY.

Innan begäran av förhandssamråd ska

- En gedigen konsekvensbedömning genomföras och dokumenteras.
- Kvarstående risker redogöras.
- Beskrivning ske för varför riskerna inte kunnat åtgärdas.

Se Förhandssamråd - Integritetsskyddsmyndigheten (imy.se)

Där finns bland annat en blankett för begäran av förhandssamråd. Dokumentationen av konsekvensbedömning ska skickas med till IMY som bilaga.

Uppgjord av		Nr		
Emil Lindqvist				
Godkänd av		Datum	Rev	Referens
Niklas Narvell/Pia Thunström		2022-11-07		

Eskilstuna kommun

Utredning digital samarbetsplattform

Uppgjord av		Nr		
Emil Lindqvist				
Godkänd av		Datum	Rev	Referens
Niklas Narvell/Pia Thunström		2022-11-07		

Sammanfattning

Eskilstuna kommun behöver utreda vilken samarbetsplattform som kan medverka till kommunens önskan om ökat samarbete via digitala plattformar som kan stödja; chatt, videokonferens och dokumentdelning. I dagsläget är det MS Teams som gäller för de dokument och den dokumentation som är av säkerhetsklass 0 och 1.

Arbetet bygger på, intervjuer, analyser och erfarenheter som tar stöd från vår egen verksamhet men också externa parter. Utredningen visar att det finns alternativ till en digital samarbetsplattform som bygger på inom-europeiska lösningar och tillgodoser våra grundläggande behov ur ett produktperspektiv men medför konsekvenser ur ett funktionsperspektiv. Utifrån kravspecifikationen har två lösningsförslag beaktats.

Att byta digital samarbetsplattform som eventuellt tar stöd från flera olika lösningar leder till konsekvenser vad avser kostnad, digital mognad, kompabilitet, kvalité, kommunikation och samarbete utanför vår egen verksamhet.

Att byta ut etablerade lösningar är förenat med ökade kostnader då flera systemlösningar behöver kombineras. Behovet av Microsofts andra produkter kommer kvarstå oberoende till den digitala samarbetsplattformen, delvis beroende på nuvarande avtalstid.

Offentliga verksamheter som gjort förflyttningen vittnar om att det saknas lämpliga helhetslösningar som lever upp till funktionella krav och att man i stället behöver titta på hybridlösningar.

En digital samarbetsplattform som eventuellt bygger på flera olika system medför en ”rörig” digital verktygslåda. Tydligare uttryckt innebär det fler verktyg som ska komplettera ett fullständigt system. En konsekvens som kan bidra till sämre användarvänlighet och minskad nytta och på så vis minska den digitala mognaden.

När vår organisations digitala mognad ökar, så ökar också behovet av tillgänglighet på vilken klient som helst (dator, mobil, platta etc). Funktionerna i det tilltänkta systemet ska vara enkla och enhetliga för att möta upp medarbetares och verksamheternas behov. Det bör därför ställas höga krav på användarvänlighet med sömlösa funktioner om plattformen bygger på fler samarbetslösningar. Utrymmet för störningar och otillgänglighet i en sådan tjänst är litet vilket ställer ökade krav på kontinuitetsplaner.

Slutligen saknas erfarenhet från IT-branschen vad avser omställning och implementering för ett sådant arbete. Det saknas även erfarenhet av att ställa om vilket kommer att medföra nya kompetensbehov inom den egna organisationen; från IT ändå ut till användare och verksamheten. Kostnader kommer även att öka kring omställning och utbildning.

eSam skriver i sin rapport avseende arbetet Digital plattform för offentlig sektor:
Konsekvensanalysen visar att det finns stora utmaningar inför ett fortsatt arbete. Det krävs både tid och resurser och även ett förändrat synsätt som tar höjd för behovet av ett helhetsperspektiv för hela offentlig sektor”

Uppgjord av		Nr		
Emil Lindqvist				
Godkänd av		Datum	Rev	Referens
Niklas Narvell/Pia Thunström		2022-11-07		

Innehåll

Uppgjord av		Nr		
Emil Lindqvist				
Godkänd av		Datum	Rev	Referens
Niklas Narvell/Pia Thunström		2022-11-07		

Bakgrund

Eskilstuna kommun behöver utreda vilken samarbetsplattform som kan medverka till kommunens önskan om ökat samarbete via digitala plattformar som kan stödja; chatt, videokonferens och dokumentdelning. I dagsläget är det MS Teams som gäller för de dokument och den dokumentation som är av säkerhetsklass 0 och 1.

Beslut om att använda MS Teams sträcker sig till 2022-12-31 samt licensiering t o m 2023-03-31.

Kommunfullmäktige har i oktober 2021 fattat ett beslut om att i första hand använda inomeuropeiska molntjänster. Detta kan påverka de möjligheter som finns för att hitta lämplig plattform eller separata alternativ

Syfte

Utredningen har som syfte att stödja framtida beslutsfattningar om lösningar som i sig själva eller tillsammans med andra lösningar kan utgöra en digital sammarbetsplattform för Eskilstuna kommun och de krav som ställs på våra verksamheter.

Med begreppet digital sammarbetsplattform avses ett eller flera verktyg där följande funktioner ska/bör finnas med:

- Videokonferens
- Chat
- Dokumenthantering/lagring
- Event/stormöten

Metod och nulägesanalys

En nulägesanalys och kartläggning av grundläggande funktionalitet i nuvarande samarbetsplattform i Microsoft Teams har tagits fram genom intervjuer av nyckelroller inom den egna organisationen, andra offentliga aktörer, samt analys av arbetet digital samarbetsplattform för offentlig sektor, dSam.

- IT-arkitekter inom kommunen (3).
- Intervju med leverantörsrepresentant
- Intervju med projektledare dSam

För att nå en slutsats har vi identifierat vilka funktioner som nyttjas i dag (Microsoft Teams) och som behöver ersättas vid förändring.

Uppgjord av		Nr		
Emil Lindqvist				
Godkänd av		Datum	Rev	Referens
Niklas Narvell/Pia Thunström		2022-11-07		

(Utöver skallkraven finns också andra funktioner som till exempel Kanban-tavla, ett sätt att planera och visualisera arbetsflöden, digital whiteboard och kalendersynk som förloras vid en eventuell förändring).

Lösningsalternativ

I utredningen har vi valt att titta närmre på system som i sig själva eller med hjälp av andra kan utgöra grunden för en framtida digital plattform. Systemen i utredningen valdes på grund av att de testats eller redan används av andra aktörer inom offentlig verksamhet och kan utvärderas efter reella erfarenheter.

	Chat	Video	Stormöten	Lagring	Kalender	Ord/Kalkyl	Kostnad i SEK / år
MS Teams	x	x	x	x	x	X	15 634 200*
Nextcloud	x	x		x	x	X	23 940 000
Webex	x	x					15 960 000
Jitsi Meet		x					Uppgift saknas
Rocket Chat	x						Uppgift saknas
Screen 9			x				Uppgift saknas

**Teams ingår i Microsoft licensen och är inget tillägg. Därför förändras ej kostnaden om man fortsätter att nyttja Microsofts för övrigt, t ex Office-paketet.*

Till ovanstående prisbilder tillkommer utbildningsinsatser i den totala kostnaden oavsett produkt. Schablonuträkning: 2 timmar per anställd = 600 x 13 300 = 7 980 000

Kostnadsförslag

MS Teams	**Nextcloud**	**Webex**
Licenser, antal och kostnad	Licenser och kostnad	Licenser och kostnad
E3 – 2300 st – 4050 kr / år	13 300 st – 1800 kr / år	13 300 st – 1200 kr / år
F3 – 6100 st – 660 kr / år		
A3 – 4900 st – 460 kr / år		
Totalt 15 634 200 SEK / år	**Totalt** 23 940 000 SEK / år	**Totalt** 15 960 000 SEK / år
Jitsi meet	**Rocket chat**	**Screen 9**
Licenser och kostnad	Licenser och kostnad	Licenser och kostnad
Uppgifter saknas*	Uppgifter saknas*	Uppgifter saknas*

** I kalkylerna finns det lösningar som saknar uppgifter om kostnad vilket beror på att vi inte kunnat erhålla kostnadsförslag från licenspartner eller att verksamheter som fått offert valt att inte offentliggöra den.*

Uppgjord av		Nr		
Emil Lindqvist				
Godkänd av		Datum	Rev	Referens
Niklas Narvell/Pia Thunström		2022-11-07		

Lösningsförslag

Alternativ 1 – Nextcloud, helhetslösning

Referens: Utredning av digital samarbetsplattform dSam. https://esamverkan.se

Nextcloud är en lösning med öppen källkod från ett tyskt företag (Nextcloud GmbH) som står bakom och erbjuder support och underhåll. Ett antal svenska partners finns på marknaden. Nextcloud erbjuder inte själva molntjänster utan förlitar sig på partners. Det finns svenska och europeiska leverantörer som erbjuder lösningen som molntjänst och lösningen finns även för egen IT-drift.

Nextcloud Hub erbjuder funktionalitet som liknar det Microsoft 365, Google Workspace.

Lösningen är anpassningsbar och det går att välja att tillgängliggöra en bred flora av funktionalitet med hjälp av de 100-tal appar som finns tillgängliga. Vanligast förekommande appar är beständig chatt med stöd för gruppchatt och personlig chatt, mötes och videokonferenstjänst, e-post, kalender, fil- och dokumenthantering, dokumentredigerare för webb som ger stöd för samtidig redigering, ”tasks”/kanban, kalender och Whiteboard.

Erfarenheter

Enligt intervju med projektledare för dSam (Se bilaga) har man enligt erfarenheter från Skatteverket gjort bedömning att Nextcloud inte lever upp till de krav man ställer på plattformen som helhetslösning. Nextcloud erbjuder funktioner som videomöten och chat så tycker man att det är otillräckligt. Det gäller specifikt funktioner så som videomöten och gruppchat. Utifrån de erfarenheterna har man från Skatteverket tagit beslut att gå vidare med en hybridlösning, se lösningsalternativ 2 nedan.

Alternativ 2 – Nextcloud, hybridlösning

Referens: Utredning av digital samarbetsplattform dSam. https://esamverkan.se

Hybridlösning med Nextcloud som grundplattform och komplimenterande samarbetslösningar till de funktioner som ej lever upp till verksamhetens krav. Enligt intervju med projektledare för dSam (Se bilaga) finns det brister inom de tjänster Nextcloud erbjuder och som i stället ersätts av andra lösningar som komplement.

Chat – Rocket chat

Referens: Utredning av digital samarbetsplattform dSam. https://esamverkan.se

Rocket.Chat är en programvara med öppen källkod för fasta chattrum med stöd för

Uppgjord av		Nr		
Emil Lindqvist				
Godkänd av		Datum	Rev	Referens
Niklas Narvell/Pia Thunström		2022-11-07		

gruppchatt, personlig chatt och videomöten. Rocket.Chat (samtal) använder Jitsi (koppling till mobil) eller BigBlueButton (virtuella klassrum/grupper för möten, dokument och chatt) som lösning för videomöten. Det finns stöd för att hantera filer kopplade till chattarna. Rocket.Chat har öppna programmeringsgränssnitt (API:er) för utökad funktionalitet och integration med andra system. Exempelvis går det att koppla ihop Rocket.Chat med andra lösningar via Matterbridge (sätt att synka flera system med varandra samtidigt).

Videokonferens – Jitsi meet

Referens: Utredning av digital samarbetsplattform dSam. https://esamverkan.se

Jitsi är vanligt förekommande i de analyserade lösningarna, både som paketerad tjänst och som integrerad videomötesfunktion i t.ex. helhetslösningar. Jitsi är baserad på öppen källkod med ett företag baserat i USA (8x8) som erbjuder support, underhåll och molntjänster. Flera bolag erbjuder kommersiell support inklusive Element (krypterade mobila lösningar end to end). Flera europeiska och svenska leverantörer erbjuder Jitsi som tjänst. Lösningen finns även för drift i egen IT-miljö.

Jitsi har funktioner för att hålla små till medelstora videomöten och fungerar i de flesta moderna webbläsare. Exempelvis finns funktionalitet som chatt under mötet, skärmdelning, egen bakgrundsbild eller suddig bakgrund, möjlighet att spela in mötet, dela ljud och videofilmer, streaming och totalsträckskryptering (end to end).

Stormöten – Screen 9

Referens: Utredning av digital samarbetsplattform dSam. https://esamverkan.se

Screen 9 är ett svenskt företag som fokuserar på att leverera en videoplattform med tjänster kring distribution av live och on-demand video. Tjänsten kan köpas på flera sätt. Screen 9 erbjuds som molntjänst, hybrid och drift i eget datacenter.

Konsekvensanalys

- Fördelen med inom-europeiska lösningar är att de är kompatibla med gällande EU-lagstiftning. Eskilstuna kommun slipper lägga ned tid och resurser på att avtalsmässigt skydda informationen från en leverantör där det finns rädslor om olovlig spridning och behandling av informationen. Det kan vara både tidskrävande och dyrt att ständigt konstruera olika skydd för att kunna nyttja tjänsten.
- Även om vi upphandlar en tjänst idag som är inom-europeiskt ägd så är det ingen garanti för att för att det inte kan bli uppköpt av en större global aktör utanför EU. Exempel är Skype och Candy Crush som båda tidigare var svenska företag men numera ingår/ägs av Microsoft.
- Att samarbeta och kommunicera med organisationer utanför kommunen är en viktig del i vår verksamhet. Det är därför viktigt att vi ställer höga krav på en

Uppgjord av		Nr		
Emil Lindqvist				
Godkänd av		Datum	Rev	Referens
Niklas Narvell/Pia Thunström		2022-11-07		

etablerad digital samarbetsplattform så att vi enkelt kan upprätthålla god kommunikation. En förflyttning till en miljö som saknar integrationer med etablerade lösningar kan få negativa konsekvenser gällande vår kommunikation med externa samarbetspartners.

- Att byta ut etablerade lösningar är förenat med kostnader, i vårt fall minst dubbelt så höga. Behovet av Microsofts produkter kvarstår oberoende till digital samarbetsplattform. Andra utmaningar är kompetensförsörjning och förändringsledning. Även implementeringsarbetet kommer att kräva särskild kompetens vilket medför risk för högre resurskostnader.
- På grund av corona-pandemin har det funnits ett stort behov av distansarbete och kravet på en digital arbetsplats ökat. Microsoft Teams har blivit ett erkänt och etablerat verktyg i kommunens digitala verktygslåda. Enkla och användarvänliga funktioner är något som verksamheten efterfrågar och kravet på sömlösa integrationer blir av allt större vikt.
- Att flytta från en etablerad digital samarbetsplattform till en hybridlösning innebär att man behöver lära sig fler system än ett. Implementeringsarbetet kommer kräva stora förändringar för kommunens samtliga verksamheter och resan omfattar både teknik och kultur. Risken för en ”rörig” digital verktygslåda ökar vilket sannolikt medför ett minskat användande.
- Att byta ut en helhetstjänst ökar risken för integrationsproblem och tillgänglighetsstörningar vilket kan få stora konsekvenser för den egna organisationen. Det behövs ställas utökade krav på kontinuitetsplaner då en samarbetsplattform som dagligen används för intern och extern kommunikation blir en viktig verksamhetsfunktion. Utrymmet för störningar eller otillgänglighet i en sådan funktion behöver hållas ner.
- I takt med att vi utökar funktioner i den digitala verktygslådan och allt fler lösningar levereras som tjänst, ökar tillgängligheten på vilken klient som helst. Krav på system som fungerar sömlöst över olika klienter blir av allt större vikt. En digital samarbetsplattform som kombineras av olika tjänster är också beroende av systemintegrationer vilket medför en ökad risk för kompabilitetsproblem.