Skatteverket

Inledande utredning avseende Microsoft 365

Diarienummer: **8-2800157** | 2024-02-26

Skatteverket

Sammanfattning

En tvärfunktionell arbetsgrupp med medarbetare från Skatteverket och Kronofogdemyndigheten har, utifrån behovet av att ersätta Skype, utrett möjligheten för myndigheterna att övergå till att använda vissa produkter från Microsoft. Dessa produkter är identitets- och åtkomsthanteringstjänsten Entra ID, kontorsprogramsviten 365 Apps for Enterprise (M365Apps) och chatt- och mötesverktyget Teams.

Utredningen omfattar frågor som rör dataskydd, sekretess, it-säkerhet, informationssäkerhet, it-arkitektur, upphandling, verksamhetsutveckling samt arkivvård och annan hantering av allmänna handlingar. En viktig förutsättning som bildar fond till utredningen är att en övergång till att använda de ifrågavarande produkterna skulle innebära att delar av myndigheternas informationshantering utkontrakteras till Microsoft.

En utgångspunkt för utredningen är ett tänkt scenario där implementeringen av produkterna begränsas till en miniminivå, bl.a. beträffande vilka uppgifter som översänds till Microsoft och vilken funktionalitet som är aktiverad. Därigenom har analysen kunnat inrikta sig på produkterna i ett grundutförande. Resultatet av denna inledande utredning utgör således basen för kommande undersökningar av om ytterligare funktioner kan läggas till.

Arbetsgruppens preliminära bedömning är att det inte föreligger några rättsliga, säkerhetsmässiga eller funktionella hinder mot att Skatteverket och Kronofogdemyndigheten använder Entra ID, M365Apps eller Teams. Det måste dock understrykas att den analys som ligger till grund för bedömningen är genomförd utifrån den begränsning avseende implementering som har definierats för utredningen. Bedömningen kan inte tas till intäkt för att införa tjänster eller funktioner som faller utanför utredningens avgränsning.

Det har inte givits möjlighet att inom ramen för denna grundläggande utredning tillräckligt belysa samtliga relevanta aspekter av en övergång till de aktuella produkterna. Det återstår därför vissa frågor, om bl.a. arkivvård, dataskydd och it- och informationssäkerhet, som måste tas om hand i det fortsatta arbetet. Vidare är tjänsterna av en sådan karaktär att deras funktionalitet förändras över tid, varför de efter ett eventuellt införande måste bli föremål för aktiv förvaltning och kontinuerlig bevakning.

Innehåll

1 Inledning

Skatteverket fattade den 27 november 2023 beslut om att utreda och klarlägga förutsättningarna för att införliva Microsoft 365 och Microsoft Teams i myndighetens programportfölj, om att tillsätta en arbetsgrupp för att under 2024 genomföra beslutade utredning och om att inleda testverksamhet avseende implementation och konfiguration av Microsoft 365 samt Microsoft Teams.[1]

Den utredning som låg till grund för beslutet dokumenteras genom denna promemoria. Utredningen har genomförts av en tvärfunktionell arbetsgrupp med kompetenser inom arkivvård, it-säkerhet, it-arkitektur, informationssäkerhet, dataskydd, sekretess, verksamhetsutveckling, Microsofts molntjänster och licensiering. Utredningen omfattar produkterna Microsoft Entra ID (AzureAD), Microsoft 365 Apps for Enterprise (M365Apps) och Microsoft Teams.

Arbetsgruppen har genomfört möten med andra myndigheter, banker och organisationer. Vissa av dessa har beslutat att gå vidare med nyttjande av Microsoft 365 men samtliga har begräsningar i hur tjänsterna får användas och vilken data som får hanteras i leverantörens tjänster.

I promemorian redovisas resonemang och bedömningar som är gemensamma för samtliga produkter som omfattas av utredningen. Frågor som är specifika för en viss produkt behandlas i respektive bilaga. Bilagorna bygger på varandra i följande ordning:

- Bilaga 1 Entra ID
- Bilaga 2 M365Apps
- Bilaga 3 Teams

1.1 Varför ny bedömning

Skatteverket och Kronofogdemyndigheten utredde under 2021 förutsättningarna att ersätta Skype med Teams som huvudsaklig video- och samarbetsplattform. Med anledning av slutsatserna i utredningen fattade myndigheterna den 3 maj 2021 beslut om att inte ersätta Skype med Teams.[2]

Föreliggande utredning skiljer sig från den som genomfördes under 2021 i följande avseenden.

- En av premisserna för slutsatserna i den tidigare utredningen var att Teams skulle ersätta Skype i dess helhet. Den utredning som nu har genomförts har haft som utgångspunkt att det även kan bli aktuellt att endast partiellt ersätta Skype med Teams.
- Utredningen omfattar inte endast Microsoft Teams, utan även andra delar av Microsoft 365.
- Utredningen 2021 omfattade framförallt de rättsliga förutsättningarna för att nyttja Microsoft Teams. I den förnyade utredningen har även andra aspekter tagits i beaktande, som beredskap och resiliens, verksamhetsnytta, Skatteverkets möjlighet att leverera en

[1] Dnr 8-2649343.
[2] Dnr 3(14)3(14)8-958696.

it-arbetsplats till andra myndigheter och den omständigheten att de alternativ till Microsoft 365 som är tillgängliga har visat sig svåra att realisera.

I det följande redogörs för förutsättningar som har förändrats jämfört med senaste bedömningen 2021 som ligger till grund för varför Skatteverket har valt att genomföra en ny bedömning.

1.2 Adekvansbeslut

EU kommissionen beslutade den 10 juli 2023 genom en genomförandeakt att anta ramen för dataskydd mellan EU och USA (adekvansbeslut)[3]. Beslutet om adekvat skyddsnivå gäller endast vid överföring av personuppgifter till mottagare som deltar i ramen för dataskydd mellan EU och USA genom bl.a. självcertifiering.

Adekvansbeslutet, i sig själv, innebär endast att det inte är oförenligt med EU:s dataskyddsförordning (GDPR) att överföra uppgifter till USA.

Personuppgifter kan, efter en bedömning enligt samtliga relevanta regler i GDPR och med stöd av beslutet om adekvat skyddsnivå, överföras till certifierade mottagare i USA utan att några ytterligare skyddsåtgärder behöver vidtas.

Adekvansbeslutet får även betydelse för de överföringar som sker med stöd av standardavtalsklausuler.

1.3 Sekretessbrytande bestämmelse

Den 1 juli 2023 tillkom en ny sekretessbrytande bestämmelse som kan möjliggöra vissa typer av utkontrakteringar som inbegriper sekretessbelagda uppgifter. Bestämmelsen finns i 10 kap. 2a § offentlighets- och sekretesslagen (OSL). Förutsättningarna för att tillämpa den sekretessbrytande bestämmelsen är att den sekretessbelagda uppgiften får lämnas till en enskild leverantör eller en annan myndighet som har i uppdrag att endast teknisk bearbetning eller teknisk lagring uppgiften. För att sekretessen ska brytas i den beskrivna situationen krävs dessutom att det med hänsyn till omständigheterna inte är olämpligt att uppgiften lämnas ut.

Den nya sekretessbrytande bestämmelsen avser endast utkontraktering avseende tjänster som kan beskrivas som teknisk bearbetning eller teknisk lagring. Begreppen finns inte definierade i författningstext men ska förstås på det sättet att leverantörens befattning med uppgiften ska vara av teknisk natur.

Olämplighetsbedömningen som ska ske enligt den sekretessbrytande regeln bör omfatta samtliga relevanta omständigheter avseende t.ex. uppgiftens art, uppgifternas känslighet och hur uppgifterna skyddas hos mottagaren mot ytterligare spridning. Uppgifter som kan ha betydelse vid olämplighetsbedömningen kan vara hänförliga till den utlämnande myndigheten, till den mottagande aktören eller till de specifika uppgifter som avses lämnas ut. Även det allmänna säkerhetsläget, såväl nationellt som internationellt kan få betydelse för olämplighetsbedömningen.

Den nya sekretessbrytande bestämmelsen i 10 kap. 2 a § OSL, tillsammans med den författningsreglerade tystnadsplikten som regleras i lagen (2020:914) om tystnadsplikt vid

[3] EU-US Data Privacy Framework

utkontraktering av teknisk bearbetning eller lagring av uppgifter, utgör viktiga förutsättningar för att svenska myndigheter ska kunna överväga utkontraktering även av uppgifter som är sekretessbelagda.

1.4 Förändrat arbetssätt

Behovet av digitala arbetsverktyg är väsentligt mycket större idag än under 2021.

Kronofogden och i viss utsträckning Skatteverket har börjat tillämpa fri arbetsort vid rekrytering. Det innebär att myndigheternas medarbetare har möjlighet till distansarbete. Det medför ett behov av bra digitala verktyg dels för att kunna göra sitt arbete på bästa sätt, dels för att ha en chans till ett socialt arbetsliv.

1.5 Skatteverkets utökade roll i det civila försvaret

Skatteverket får en större roll i det civila försvaret. Ett område som är viktigt är därför Skatteverkets förmåga att ständigt ha tillgång till verksamhetskritiska system, inklusive kommunikationssystem. Entra ID är en förutsättning för att använda andra tjänster i Microsoft 365.

1.6 Skatteverkets uppdrag att leverera it-drift

Sedan tidigare levererar Skatteverket it till Kronofogdemyndigheten och Valmyndigheten. Sedan våren 2023 har Skatteverket fått uppdraget att leverera it-tjänster till den nystartade myndigheten Utbetalningsmyndigheten.[4]

Det är sannolikt att Skatteverket kommer att leverera it-tjänster till fler myndigheter under kommande år. Dessa tjänster kan komma att inkludera förvaltning av molntjänster.

1.7 Anpassningar hos Microsoft

Nedan beskrivs nytillkomna och uppdaterade komponenter hos Microsoft som är relevanta för utredningen.

Microsoft EU Data Boundary
Microsoft EU Data Boundary är en geografisk avgränsning som kunder kan välja för att begränsa behandling av data till att ske inom EU.

End-to-end kryptering för Teams
Microsoft Teams har nu möjligheten att använda End-To-End-kryptering (E2EE) i kommunikation för att man ska kunna säkerställa att endast kommunikationsdeltagarna kan dekryptera och läsa meddelandena.

Microsoft Sovereignity
Microsoft Sovereignity är ett ramverk som kan användas för att styra var data behandlas enligt specifika regler gällande åtkomst, aktivitet och användning.

[4] 15 och 15 b §§ förordningen (2017:154) med instruktion för Skatteverket och 7 § förordningen (2007:977) med instruktion för Valmyndigheten.

Microsoft Purview
Microsoft Purview är en integrerad plattform för styrning, efterlevnad och riskhantering av data, utformad för att hjälpa organisationer att uppfylla juridiska och regulatoriska krav.

2 Rättsliga bedömningar

I samband med utkontraktering av informationsbehandling ställs den utkontrakterande myndigheten inför olika typer av rättsliga frågeställningar och utmaningar. I förgrunden hamnar frågor om tillämpningen av offentlighets- och sekretesslagen (2009:400), OSL, och om dataskydd för berörda informationsmängder. Även frågor om tillämpligheten av tryckfrihetsförordningens, TF, regler om allmänna handlingar samt om arkivlagstiftningen för handlingar som berörs av utkontrakteringen behöver adresseras. Givetvis uppkommer rättsliga frågeställningar också ur andra rättsområden i en upphandling, men den aktuella utredningen har avgränsats till de nämnda rättsområdena.

Skatteverket beslutade i maj 2021 att inte ersätta applikationen Skype med molntjänsten Teams. Skatteverkets gjorde då bedömning att det inte fanns rättsliga förutsättningar för att använda Teams på ett sådant sätt att myndighetens behov uppfylldes. Arbetsgruppens initiala uppgift har varit att undersöka om det skett förändringar som innebär att det idag finns rättsliga förutsättningar för att gå vidare med en fördjupad bedömning av de aktuella tjänsterna.

I den förnyade prövningen som nu är för handen har arbetsgruppen delat upp bedömningen utifrån tjänst, Entra ID, Microsoft 365 Apps och Teams.

2.1 Allmänna handlingar

Myndigheter som överväger att utkontraktera informationshantering behöver utreda och klargöra konsekvenserna av utkontrakteringen avseende tillämpningen av tryckfrihetsförordningen och arkivlagen. Övervägandena behöver bl.a. klargöra när och i vilken omfattning informationshanteringen inom utkontrakteringen kommer att generera allmänna handlingar och hur dessa handlingar ska omhändertas eller gallras. Övervägandena behöver också omfatta myndighetens förmåga att leva upp till kraven i tryckfrihetsförordningen i samband med begäran om utlämnande av allmän handling.

Det följande är avgränsat till frågor om allmänna handlingar som har relevans för samtliga applikationer som omfattas av utredningen. Frågor som specifikt rör en viss applikation behandlas i respektive bilaga.

2.1.1 Tjänst- och diagnostikdata

Enligt 2 kap. 3 § TF avses med handling en framställning i skrift eller bild samt en upptagning som endast med tekniska hjälpmedel kan läsas eller avlyssnas eller uppfattas på annat sätt. ”Upptagningar” innefattar bland annat upptagningar för automatiserad behandling, det vill säga elektroniska handlingar.[5] Av 2 kap. 4 § TF framgår att en handling är allmän om den förvaras hos en myndighet och enligt 9 eller 10 § är att anse som inkommen till eller upprättad hos en myndighet. Enligt 2 kap. 6 § första stycket TF anses en upptagning som avses i 3 § förvarad hos en myndighet, om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel

[5] Jfr 2 kap. 1 § Riksarkivets föreskrifter (RA-FS 2009:1) och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling).

som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas eller avlyssnas eller uppfattas på annat sätt. Av förarbetena till bestämmelsen framgår att detta tillgänglighetsrekvisit inte ska förstås så att en myndighet måste ha omedelbar tillgång till en upptagning för att denna ska kunna anses vara förvarad hos myndigheten. Även en upptagning som lagras hos en utomstående för en myndighets räkning och som på begäran översänds till myndigheten kan vara förvarad hos myndigheten.[6]

I samband med nyttjandet av de produkter som är föremål för utredningen, inhämtar Microsoft tjänst- och diagnostikdata från Skatteverket. De elektroniska handlingar som tillkommer som en följd av detta överförande av information från Skatteverket till Microsoft torde vara tillgängliga för Skatteveverket på det sätt som anges i 2 kap. 6 § första stycket TF, oberoende av om Skatteverket har omedelbar tillgång till dem eller kan ta del av dem först efter att ha begärt det hos Microsoft. Handlingarna är därmed att anse som förvarade hos Skatteverket. I den utsträckning handlingarna även är att anse som inkomna till eller upprättade hos Skatteverket, och således rekvisiten i 2 kap. 4 § TF är uppfyllda, är de allmänna handlingar hos Skatteverket.

Inom ramen för detta arbete har det inte funnits utrymme att genomföra någon fullständig analys av vilka typer av handlingar som förekommer i samband med överförandet av data till Microsoft och huruvida dessa handlingar är att anse som allmänna, utan frågan måste bli föremål för fortsatt utredning. Följande kan emellertid sägas. Microsofts insamlande av tjänst- och diagnostikdata sker genom att händelser m.m. loggas av Microsoft. De loggar som genereras är sådana fortlöpande förda förteckningar som avses i 2 kap. 10 § andra stycket 1 TF, som om de förs hos en myndighet är att anse som upprättade hos myndigheten när de har färdigställts för anteckning eller införing.[7] Microsoft samlar in data inom ramen för en leverans av vissa tjänster till Skatteverket, och insamlandet är en förutsättning för att tjänsterna ska kunna tillhandahållas. Detta talar för att loggarna bör kunna betraktas som handlingar som Microsoft framställer för Skatteverkets räkning.[8] Loggarna är i sådana fall att anse som upprättade hos Skatteverket, och därmed som allmänna handlingar hos Skatteverket.

Enligt 2 kap. 9 § tredje stycket TF ska en åtgärd som någon vidtar endast som ett led i en teknisk bearbetning eller teknisk lagring av en handling som en myndighet har tillhandahållit inte anses leda till att handlingen har kommit in till den myndigheten. Denna undantagsbestämmelse möjliggör att en myndighet utkontrakterar sin informationshantering till annan myndighet eller enskild, utan att handlingar blir att anse som allmänna hos myndigheten enbart av det skälet att myndigheten får tillgång till handlingarna hos uppdragstagaren på det sätt som avses i paragrafens första stycke. Någon motsvarande undantagsbestämmelse, om att en handling inte ska anses *upprättad*, enligt något av de villkor för upprättande som anges i 2 kap. 10 § TF, när den tillhandahålls för teknisk hantering hos en utomstående, har inte införts i TF. Uppenbarligen har lagstiftarens utgångspunkt varit att en handling som en myndighet tillhandahåller enbart i syfte att den ska tekniskt bearbetas eller tekniskt lagras hos någon inte blir att anse som expedierad av myndigheten genom tillhandahållandet. ”I fall av nu angivet

[6] Prop. 1975/76:160, s. 88–89.

[7] Se t.ex. rättsfallet RÅ 1998 ref. 44.

[8] Jfr rättsfallet RÅ 1984 2:49, i vilket en handling som framställts av ett företag på uppdrag av en kommun ansågs som förvarad och upprättad hos den uppdragsgivande kommunen, trots att handlingen aldrig hade befunnit sig i kommunens lokaler.

slag är det naturliga att se saken så att upptagningen aldrig har befunnit sig utanför myndigheten."[9]

För den fortsatta utredningen av om allmänna handlingar kommer in till eller upprättas hos Skatteverket som en följd av att Microsoft samlar in tjänst- och diagnostikdata, är det alltså av avgörande betydelse vilken befattning Microsoft tar med de uppgifter som översänds. En av de frågor som måste besvaras är om Microsofts insamlande av data enbart innebär att företaget tekniskt bearbetar eller tekniskt lagrar handlingar på Skatteverkets uppdrag eller om Microsoft även använder handlingarnas informationsinnehåll för ändamål i sin egen verksamhet. Om Microsoft vidtar andra åtgärder med handlingarna än att tekniskt bearbeta eller tekniskt lagra dem för Skatteverkets räkning, torde översändandet av data till Microsoft innebära att handlingar expedieras och därmed blir att anse som upprättade hos Skatteverket.[10]

Skatteverket får gallra de allmänna handlingar som upprättas i samband med översändandet av tjänst- och diagnostikdata endast i enlighet med föreskrifter eller beslut av Riksarkivet, vilket följer av 14 § arkivförordningen (1991:446). Enligt 3 kap. 2 § Riksarkivets föreskrifter (RA-FS 2021:7) och allmänna råd om gallring av handlingar inom stödverksamheter får handlingar rörande drift och förvaltning av informationssystem gallras när de inte behövs för verksamheten. De loggar och eventuella andra handlingar med tjänst- och diagnostikdata som här är aktuella torde vara sådana handlingar som omfattas av medgivandet om gallring. Skatteverket får därmed gallra dem vid den tidpunkt som verket bedömer lämplig. Vilka handlingar som gallras och efter vilka frister gallringen sker ska enligt 4 kap. 1 § RA-FS 2021:7 dokumenteras av Skatteverket. Dokumentationen görs lämpligen i Skatteverkets arkivförteckning.[11]

2.1.2 Teknisk bearbetning och teknisk lagring

En övergång till M365Apps, Microsoft Teams och Entra ID kommer att medföra att Skatteverket utkontrakterar delar av sin informationshantering till Microsoft, och därvid tillhandahåller Microsoft elektroniska handlingar. Detta berörs i avsnittet om tjänst- och diagnostikdata ovan och i avsnittet om allmänna handlingar i bilaga 3 Teams.

Under förutsättning att Microsoft endast tekniskt lagrar eller tekniskt bearbetar Skatteverkets handlingar för verkets räkning, blir handlingarna inte att anse som inkomna till Skatteverket enbart genom den omständigheten att de är tillgängliga för verket genom Microsofts applikationer. Under samma förutsättning blir handlingarna inte heller att anse som expedierade och därmed upprättade hos Skatteverket enbart genom att verket tillhandahåller Microsoft dem. På så vis undanhålls en situation där handlingar hos Skatteverket som inte är avsedda att vara allmänna blir att anse som allmänna genom utkontrakteringen. Framförallt beträffande chattar i Teams framstår det som angeläget att undvika att lagring i Microsofts moln medför att stora mängder rent intern verksamhetsinformation blir allmänna handlingar.

Om Skatteverket ska använda de ifrågavarande produkterna, och därmed ge Microsoft i uppdrag att hantera handlingar för verkets räkning, är det alltså av vikt att Skatteverket

---

[9] Prop. 1975/76:160, s. 137.

[10] Jfr rättsfallet HFD 2011 ref. 52.

[11] Skatteverket har fattat beslut (8-2336225) om hur Riksarkivets gallringsföreskrifter RA-FS 2021:3, RA-FS 2021:6 och RA-FS 2021:7 ska tillämpas för loggar. Beträffande säkerhetsloggar har gallringsfristerna bestämts med beaktande av Säkerhetspolisens föreskrifter om säkerhetsskydd.

försäkrar sig om att Microsoft inte tar annan befattning med handlingarna än den tekniska bearbetning eller den tekniska lagring som ingår i uppdraget. Detta skulle kunna uttryckas som att Skatteverket har en ”undersökningsplikt” avseende vilka åtgärder som Microsoft kan komma att vidta med handlingarna. Hur avtalet med Microsoft är utformat blir här centralt, eftersom det måste framgå att Microsoft endast får tekniskt bearbeta eller teknisk lagra handlingarna för Skatteverkets räkning. Vidare är det självfallet så att, om det kommer till Skatteverkets kännedom att Microsoft vidtar åtgärder med handlingarna som inte ryms inom uppdraget, måste verket genast tillse att Microsofts tillgång till handlingarna upphör.

2.1.3 Frågor om handlingsoffentlighet och arkivvård

I 2 kap. 1 § TF stadgas att var och en ska ha rätt att ta del av allmänna handlingar. Enligt 15 § första stycket ska den som begär ut en allmän handling som får lämnas ut genast eller så snart det är möjligt och utan avgift få ta del av handlingen på stället på ett sådant sätt att den kan läsas eller avlyssnas eller uppfattas på annat sätt. I 17 § första stycket föreskrivs att en begäran att få ta del av en allmän handling görs hos den myndighet som förvarar handlingen. Av paragrafens andra stycke framgår att huvudregeln är att den myndighet som anges i första stycket också ska pröva begäran. Det finns ingen möjlighet för en myndighet att överlåta ansvaret för sina allmänna handlingar åt en annan myndighet eller enskild.[12] Också i det fall en myndighet har uppdragit åt annan att lagra en allmän handling för myndighetens räkning, ska begäran om utfående av handlingen göras hos myndigheten, vilken även ska pröva begäran och svara för att handlingen tillhandahålles i tid.

Att en myndighet utkontrakterar hela eller delar av sin informationshantering får naturligtvis inte innebära försämrade möjligheter att ta del av allmänna handlingar hos myndigheten. Vad gäller allmänna handlingar som förekommer i Word och andra kontorsprogram eller i chattar, torde en övergång till M365Apps och Microsoft Teams inte medföra någon förändring av Skatteverkets förutsättningar att hantera en begäran om att få ta del av allmän handling jämfört med i dag. Läget kan emellertid inte betraktas som lika klart i fråga om de loggar och eventuella andra allmänna handlingar som kan tillkomma i samband med översändandet till Microsoft av tjänst- och diagnostikdata. Den fortsatta utredningen måste därför innefatta en analys av om Microsofts hantering av dessa data kan innebära utmaningar för Skatteverkets möjligheter att efterleva bestämmelserna om handlingsoffentlighet i 2 kap. TF.

Av 3 § första stycket arkivlagen (1990:782) följer att de allmänna handlingar som inkommer och upprättas i samband med att Skatteverket använder de applikationer som behandlas i utredningen bildar arkiv hos Skatteverket. Enligt 4 § ska varje myndighet svara för vården av sitt arkiv, om inte en arkivmyndighet med stöd av 9 § har övertagit detta ansvar. Av 6 § 3 och 5 arkivlagen framgår att det i arkivvården bl.a. ingår att myndigheten dels ska skydda arkivet mot förstörelse, skada, tillgrepp och obehörig åtkomst, dels ska verkställa föreskriven gallring i arkivet.

Med stöd av 11 § arkivförordningen (1991:446) har Riksarkivet meddelat föreskrifter om statliga myndigheters arkivvård. Bl.a. föreskrivs i 1 kap. 3 § Riksarkivets föreskrifter (RA-FS 1991:1) och allmänna råd om arkiv hos statliga myndigheter att, om en myndighet överlåter framställning, teknisk bearbetning eller teknisk lagring av handlingar till en annan myndighet

[12] Myndigheter ska under vissa omständigheter överlämna eller återlämna allmänna handlingar enligt bestämmelser i 9, 11 och 12 §§ arkivlagen (1990:782). En myndighet får även återlämna en handling som den har fått som lån. I dessa fall upphör dock de handlingar som återlämnas eller överlämnas att vara myndighetens handlingar.

eller till en enskild, ska denna genom en skriftlig överenskommelse åläggas skyldighet att följa tillämpliga föreskrifter inom arkivområdet.

Enligt 1 kap. 9 § Riksarkivets föreskrifter (RA-FS 2009:1) och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling) ska en myndighet som upphandlar program eller tjänster för utveckling eller drift av ett system överenskomma med leverantören om tillgång till program och dokumentation i den utsträckning som krävs för tillämpningen av den författningen. Av 1 kap. 10 § framgår att, om en myndighet genom uppdrag överlåter teknisk framställning, bearbetning eller bevarande av elektroniska handlingar till en annan myndighet eller enskild, ska denna genom skriftlig överenskommelse åläggas skyldighet att följa de bestämmelser som är tillämpliga. Av överenskommelsen ska framgå att såväl myndigheten som arkivmyndigheten har rätt att vid behov kontrollera efterlevnaden av bestämmelserna. Enligt de allmänna råden till paragrafen bör det särskilt uppmärksammas att myndigheten inte kan överlåta ansvaret för de elektroniska handlingarnas informationsinnehåll åt någon annan. Råden innehåller även en upplysning om att inte heller prövningen av utlämnandet av de allmänna handlingarna kan överlåtas åt annan.

Om Skatteverket upphandlar de Microsoftprodukter som är föremål för utredningen, kommer Skatteverket att genom uppdrag överlåta bl.a. teknisk framställning och teknisk lagring av elektroniska handlingar till Microsoft. Riksarkivets föreskrifter bör därmed ha betydelse för hur avtalet med Microsoft utformas. Microsoft ska dels åläggas skyldighet att följa tillämpliga arkivförfattningar, dels ge Skatteverket tillgång till de program och den dokumentation som krävs för att verket ska kunna tillämpa Riksarkivets föreskrifter om elektroniska handlingar. Vidare ska det av avtalet framgå att både Skatteverket och Riksarkivet har rätt att vid behov kontrollera hur Microsoft efterlever föreskrifterna.

Ett problem av principiell natur är att tjänst- och diagnostikdata bevaras enligt Microsofts standardinställningar. Det innebär att tidpunkterna för gallring av de allmänna handlingarna i praktiken kommer att bestämmas av Microsoft, inte av Skatteverket. Det är oklart om Skatteverket, efter att ha gjort en egen bedömning av hur länge handlingarna behövs för verksamheten, kan ge Microsoft instruktioner om vilka gallringsfrister som ska gälla för handlingarna eller om att handlingarna ska bevaras. Vidare är det Microsofts rutiner, vilka kan förändras över tid, som styr vilka uppgifter som införs i loggarna över tjänst- och diagnostikdata och hur loggarna ska utformas. I de avseendena kommer alltså Skatteverket att sakna reell möjlighet att utöva sitt arkivansvar enligt 4 § arkivlagen, om Skatteverket övergår till M365Apps, Teams och Entra ID.

2.2 Sekretess

Vid användning av de aktuella tjänsterna kommer uppgifter lämnas ut till Microsoft. Ett utlämnande sker till exempel vid synkronisering av Skatteverkets AD eller när medarbetare kommunicerar via Teams.

Arbetsgruppen har bedömt de attribut som överförs och synkroniseras med Entra ID för respektive tjänst. Vissa uppgifter är sekretessreglerade men arbetsgruppen gör bedömningen att ett utlämnande till Microsoft inte skulle medföra skada eller men för det intresse som sekretessen avser att skydda.

Vid Skatteverkets tidigare bedömning 2021 var utgångspunkten att användning av Teams förutsätter att stora delar av den utlämnade informationen är tillgänglig för Microsoft.

Arbetsgruppen konstaterar att E2EE numera kan användas i en större omfattning, till exempel vid gruppsamtal varför användarnytta kan åstadkommas utan att sekretesskyddade uppgifter eller känsliga personuppgifter röjs för Microsoft. Arbetsgruppen menar att E2EE innebär att Microsoft hindras från att ta del av det uppgiftens informationsbärande innehåll.

2.3 Dataskydd

Vid användningen av de aktuella tjänsterna kommer vissa personuppgifter överföras till USA och myndigheten behöver därmed säkerställa att det finns en rättslig grund för en sådan överföring. Mot bakgrund av det adekvansbeslut som kom sommaren 2023 menar arbetsgruppen att det numera finns rättsliga förutsättningar att föra över personuppgifter till USA. Hur adekvansbeslutet påverkar möjligheterna att föra över personuppgifter berörs närmare i dokumentet som behandlar Entra ID.

Den personuppgiftsbehandling som sker behöver bedömas i en riskanalys men arbetsgruppen gör, mot bakgrund av de tekniska och organisatoriska åtgärderna, bedömningen att användandet av tjänsterna inte innebär en hög risk för enskildas fri- och rättigheter. Den bedömningen förändras inte av att det föreligger en risk för att uppgifter kan komma att olovligen lämnas vidare av Microsoft till amerikanska underrättelsemyndigheter.

2.3.1 Otillåtet utlämnande till amerikanska myndigheter

I den bedömning som gjordes 2021 identifierades risken för ett otillåtet utlämnande av Skatteverkets uppgifter genom att dessa överförs av Microsoft till amerikanska underrättelsemyndigheter eller brottsutredande myndigheter. Enligt de förutsättningar som då var för handen gjorde Skatteverket bedömningen att det inte fanns förutsättningar för användning av Teams i myndighetens verksamhet som huvudsakligt verktyg för video- och samarbeten.

Arbetsgruppen menar att det alltjämt föreligger en risk för att myndighetens uppgifter kan komma att utlämnas till amerikanska myndigheter. Den initiala frågan som behöver besvaras är om den aktuella risken innebär att Microsoft inte kan lämna sådana garantier som krävs enligt art. 28.1 GDPR och att Skatteverket därav är förhindrad att anlita Microsoft.

Enligt art. 28.1 GDPR får myndigheten endast anlita ett personuppgiftsbiträde som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i GDPR och säkerställer att den registrerades rättigheter skyddas. Arbetsgruppen menar att bestämmelsen innebär att personuppgiftsbiträdet ska ge tillräckliga garantier för att en lämplig säkerhetsnivå (artikel 32) uppnås i förhållande till risken. Den aktuella bestämmelsen innebär således inte att biträdet behöver lämna en fullständig garanti för att inga uppgifter kan komma att lämnas ut till amerikanska myndigheter. Bedömningen ska ske utifrån risk i det aktuella fallet.

Därefter behöver myndigheten avgöra om den aktuella risken för ett utlämnande till amerikanska myndigheter innebär att myndigheten inte kan gå vidare med att anskaffa de aktuella tjänsterna. Bedömningen sker normalt inom ramen för en konsekvensbedömning. Vid den bedömningen bör det samtidigt utredas hur den aktuella risken har påverkats av adekvansbeslutet.

En preliminär bedömning ger vid handen att risken för otillåtet utlämnande till amerikanska underrättelsemyndigheter och brottsutredande myndigheter kan omhändertas genom tekniska

och administrativa skyddsåtgärder. Skyddsåtgärderna innebär att inga känsliga personuppgifter, inbegripet uppgifter som skyddas av sekretess tillgängliggörs för Microsoft på ett sådant sätt att de kan bli föremål för ett utlämnande till amerikanska myndigheter. De skyddsåtgärder som arbetsgruppen bedömer som effektiva utgörs dels av kryptering, E2EE, samt avvägd konfiguration av tjänsterna och dels utbildningsinsatser för samt instruktioner till medarbetarna inom Skatteverket.

3 Strategisk kommunikation

Försvarsberedningen har i en serie utredningar under hösten 2023 tydliggjort målet med det civila försvarets förmågor med anledning av det ändrade säkerhetspolitiska läget.

Det civila försvaret ska verka för samhällets samlade mobilisering i händelse av krig. De viktigaste samhällsfunktionerna ska säkerställas, till exempel det finansiella systemets funktionalitet och elektroniska kommunikationer. Tillgång till grunddata och ekonomisk säkerhet bidrar till att säkerställa de viktigaste samhällsfunktionerna

Erfarenheter från Ukraina visar på betydelsen av ett systematiskt informations- och cybersäkerhetsarbete och ett starkt cyberförsvar, liksom på betydelsen av robusthet i elektroniska kommunikationer, god reparationsberedskap och samarbete mellan privata och offentliga aktörer.

En av de förmågor som lyfts särskilt strategisk kommunikation. Utöver en samlad förmåga att motstå ett väpnat angrepp måste regeringen tillsammans med andra offentliga aktörer också ha förmåga att kommunicera effektivt, snabbt och samordnat.

Samarbetet och informationsutbytet med motsvarande funktioner i andra länder och inom EU bör utvecklas i syfte att kunna samordna nationella åtgärder med åtgärder på unionsnivå och internationellt.

Skatteverket har genom sina interna Skype-lösningar vissa utmaningar med kommunikationsförmåga i internationella sammanhang, både som deltagare och som kommunikatör. Myndigheten behöver förstärka sin kommunikations- och samarbetsförmåga utifrån dagens allvarliga säkerhetspolitiska läge.[13]

Skatteverket behöver förbereda en skalbar, internationellt gångbar lösning för att säkerställa kommunikationsförmåga och samarbetsförmåga med internationella samarbetspartners, vid kris, ett höjt beredskapsläge eller väpnat angrepp.

4 Bedömning ur it-säkerhetsperspektiv

I Skatteverkets utredning av Microsoft 365 har arbetsgruppen övervägt förutsättningarna för Entra ID och Microsoft Teams som ersättare för Skype och M365 Apps som uppgradering av Office med utgångspunkt i it-säkerhetsaspekter. Utredningen har granskat behandlingen av attribut samt tjänste- och diagnostikdata. Granskningen har också innefattat komponenter och

[13] DS 2023:34

lösningar inom utredningens avgränsning. Utgångspunkt har varit den information som komponenterna måste hantera framför vilken information som kan tillåtas i vilken lösning.

De attribut som är nödvändiga att synkronisera mot Microsoft, för att de tjänster som omfattas av utredningens avgränsning ska fungera, utgör vid synkroniseringen låga it-säkerhetsrisker. Samma bedömning görs för den tjänst- och diagnostikdata som överförs till Microsoft.

När information avseende attribut samt tjänst- och diagnostikdata aggregeras kan säkerhetsrisken höjas. Risken är då dock närmast av karaktären informationssäkerhetsrisk.

I det kommande arbetet behöver utredningen, utifrån it-säkerhetsperspektivet, fortsätta att bedöma attribut samt tjänst- och diagnostikdata. Den fortsatta utredningen behöver även omfatta framtida säkerhetsbrister samt motsvarande säkerhetslösningar som skulle begränsa användande av information i tjänsterna utifrån informationsklassning eller styrande lagstiftning.

5 Bedömning ur informationssäkerhetsperspektiv

Rapporten utgår strikt från den avgränsning som fastslagits. Den informationsmängd som skapas och behandlas genom Skatteverkets användning av de aktuella tjänsterna har begränsats till en nödvändig nivå. Det tillkommer att analysera hur tjänsterna kan användas i praktiken och vilka tekniska och administrativa utmaningar som då identifieras.

5.1 Kommande undersökningsbehov

Denna rapport behöver följas av en djupare studie. Riskanalys både från ett informations-, och it-säkerhetsperspektiv behöver utföras. Riskanalysen ska, utifrån identifierade risker, fånga upp om befintliga tekniska säkerhetsåtgärder och befintliga administrativa rutiner/regelverk anses tillräckliga eller om komplettering eller utökning bör ske.

Studien behöver även undersöka hur bibehållen säkerhetsnivå säkerställs vid förändringar av tjänst eller funktion och som därigenom påverkar exempelvis diagnostikdata, attribut och tjänstdata i informationsflödet.

Vidare behöver även säkerhetsbrister/lösningar identifieras som skulle begränsa användande av information i tjänsterna utifrån informationsklassning eller styrande lagstiftning.

6 Förvaltning

Det finns skillnader mellan att hantera och förvalta IT-resurser on-premise och i molnet. I en molntjänst sker förändringar och uppdateringar löpande, ofta månadsvis vilket kräver att man har koll på förändringar som sker med det tjänster man använder och vad förändringar innebär. Detta innebär att förändringar av verktygen verksamheten använder förändras med tid, både gällande funktionalitet och i användargränssnittet.

Det är viktigt att förstå att förvaltningen av molntjänster som Microsoft 365 kräver en kontinuerlig uppmärksamhet på tjänsteförändringar och uppdateringar, vilket innebär proaktiv övervakning samt vid behov, anpassning av verksamhetens IT-rutiner. En sådan dynamisk miljö ställer speciella krav på att kunna agera på förändringar, även icke acceptabla inom kostnader, avtal, juridik och säkerhet.

Livscykelhanteringen i Microsoft 365 innebär att strategiskt styra och hantera IT-resurser från upprättande till avveckling. Detta omfattar att säkerställa att programvarulicenser och användarrättigheter är korrekt tilldelade och uppdaterade, att upprätta och följa säkerhets- och efterlevnadspolicyer, samt att aktivt hantera data genom dess olika faser - från skapande och användning till arkivering eller radering. Effektiv livscykelhantering kräver proaktiv hantering och anpassning till nya funktioner och uppdateringar som Microsoft 365 regelbundet introducerar, för att säkerställa att organisationens IT-infrastruktur är säker, effektiv och i linje med uppsatta mål och krav.

För varje ny funktion eller tillägg till befintlig funktion behöver djupgående analys och värdering av data i form av attribut diagnostikdata och tjänstdata man måste lämna ifrån sig. Den behöver bedömas för sig och tillsammans med redan tidigare genomgången data, och den behöver även bedömas utifrån aggregerad mängd. En detaljerad teknisk utvärdering behöver också genomföras för att identifiera och säkerställa att eventuella konfigurationsändringar, anpassningsbehov eller potentiella kompatibilitetsproblem inte påverkar tidigare bedömning av informationssäkerhet och juridik.

Målet är att på sikt skapa en produktiv sammarbetsplattform som följer gällande dataförordningar.

Exempel på områden som behöver adresseras vid förvaltning är

- tydlighet gällande tillåten och inte tillåten användning av tjänsten och hantering av information,
- komplettering med administrativa regler och rutiner där tekniska säkerhetsåtgärder inte räcker till, och
- kontinuerlig utbildning av användare.

Innan Skatteverket kan börja använda Microsoft 365 behöver en detaljerad teknisk utvärdering genomföras för att identifiera och säkerställa eventuella konfigurationsändringar, anpassningsbehov eller potentiella kompatibilitetsproblem utifrån vårt användningsområde.

Vid förvaltningsetablering av en ny eller utökad molntjänst som Microsoft 365 så behöver Skatteverket ha en förändrings- och exitstrategi. Man behöver också undersöka möjliga alternativa lösningar.

Skatteverket behöver ha en kontinuitetsplan i sådana fall Microsofts tjänster inte är tillgängliga. Ett sådant scenario gör att Skatteverket behöver ha alternativa kommunikationsvägar.