

Analys av Microsoft 365 Apps for Enterprise

1	Översikt över Microsoft 365 Apps for Enterprise	2
1.1	Bakgrund och syfte	2
1.1.1	Funktionalitet och avgränsningar i utredningen av M365Apps	2
2	Implementering av M365Apps	2
2.1	Omfattning av implementering av M365Apps	2
2.2	Synkronisering av Skatteverkets AD med Entra ID	2
2.2.1	Tillkommande attribut.....	2
2.3	Vilken övrig information skickas till Microsoft vid nyttjande av M365Apps enligt Scope (diagnostikdata och tjänstdata)? 3	
2.3.1	Obligatoriska diagnostikdata	4
2.3.2	Obligatoriska tjänstdata.....	5
3	Rättsliga överväganden	6
3.1	Allmänna handlingar	6
3.2	Sekretess	6
3.2.1	Överföring av attribut till Entra ID.....	6
3.2.2	Överföring av nödvändig diagnostik- och tjänstdata.....	7
3.3	Dataskydd (GDPR)	7
3.3.1	Personuppgiftsansvar	7
4	Sammanfattning	8

1 Översikt över Microsoft 365 Apps for Enterprise

1.1 Bakgrund och syfte

Skatteverket har valt att starta en utredning med ambitionen att klargöra förutsättningarna för att anskaffa och använda Entra ID, Microsoft 365 Apps for Enterprise (M365Apps) samt Microsoft Teams.

Utredningen innefattar bl.a. att genomföra en noggrann analys av M365Apps för att bedöma dess potentiella roll som ersättare, helt eller delvis, för nuvarande Office.

Ambitionen med detta dokument är att, med utgångspunkt i angiven avgränsning i avsnitt 1.1.1, beskriva den omfattning av M365Apps som Skatteverket bedömer relevant för myndighetens verksamhet.

1.1.1 Funktionalitet och avgränsningar i utredningen av M365Apps

I denna utredning har Skatteverket valt applikationerna Word, Excel, PowerPoint, Outlook och OneNote, installerat på Skatteverkets PC-klientplattform. Skatteverket kan i framtiden välja om applikationerna ska vara tillgängliga på andra plattformar (Web, Mac och mobila enheter) än PC-klientplattform.

M365Apps skiljer sig mot traditionella Office då det tillhandahålls som en prenumerationstjänst. Det innebär att tjänsten och dess innehåll resp. utformning är dynamisk och uppdateras kontinuerligt. Nya funktioner tillkommer löpande och hanteras via olika uppdateringskanaler. Skatteverket väljer hur uppdateringar ska hanteras och i vilken ordning de ska tillgängliggöras i organisationen. M365Apps använder Entra ID för licensiering av användarna. En fungerande internetuppkoppling är nödvändig för att användarna ska kunna licensieras.

2 Implementering av M365Apps

2.1 Omfattning av implementering av M365Apps

Vid en implementering M365Apps så skulle för licensiering och underhåll av installationerna Entra ID användas. Grundläggande attribut som används för att i detta scenario lista användarna beskrivs i: Bilaga 1 Entra ID. Utöver dessa tillkommer nedan angivna attribut.

2.2 Synkronisering av Skatteverkets AD med Entra ID

Microsoft Entra ID är Microsofts molnbaserade identitets- och åtkomsthanteringstjänst. Entra ID krävs för att ge medarbetare åtkomst till Microsoft 365. För att kunna licensiera och underhålla M365Apps krävs att Skatteverkets lokala AD är till viss del synkroniserad med Entra ID.

2.2.1 Tillkommande attribut

Vid aktivering och efterföljande uppdateringar av M365Apps-licensen skickas grundläggande information om PC-klienten. Attributen listas nedan.

Beskrivning	Attribut
OrgId genereras när en användare loggar in med M365Apps. Attributet används för att autentisera användaren med Office Licensing Service. Användaren loggar in i prenumerationstjänsten för att verifiera licensen.	OrgId user identity
Serienummer för M365Apps produktnyckel för datorn. Används för att skapa en unik identifierare per installation av programmen.	Machine Key
Enhetsnamn för datorn som sätts i Windows. Detta behövs för att identifiera vilken dator som har aktiverad licens.	Machine Name
Användarklientens hårdvaruid som genereras i Windows	Machine ID

2.3 Vilken övrig information skickas till Microsoft vid nyttjande av M365Apps enligt Scope (diagnostikdata och tjänstdata)?

Diagnostiska data används för att hålla M365Apps säkert och uppdaterat. Datan används också för att identifiera, diagnostisera och åtgärda problem samt för produktförbättringar. Diagnostiska data är tillgängliga per klient.

När Microsofts applikationer installeras på en användarklient så kan den skicka diagnostikdata till Microsoft. Skatteverket kan konfigurera applikationerna så att olika mängder diagnostikdata skickas till leverantören. Nedan redovisas tre konfigurationsalternativ som kan väljas av Skatteverket.

Det föreligger tre nivåer för överföring av diagnostiska data för programvaran som Skatteverket kan välja mellan:

1. Obligatoriskt: Den minimala mängd data som är nödvändig för att bidra till att säkerställa att applikationerna är säkra, aktuella och fungerar som förväntat på den enhet där det är installerat.
2. Valfritt: Ytterligare data som hjälper Microsoft att genomföra produktförbättringar samt tillhandahålla mer omfattande information för att underlätta upptäckt, diagnos och åtgärdande av problem hos användaren.
3. Inget: Ingen diagnostisk data avseende applikationen som körs på användarens klient samlas in och överförs till Microsoft.

Obligatorisk diagnostikdata krävs för att produkterna ska kunna hållas uppdaterade. Av den anledningen bedömer utredningen att myndigheten behöver välja alternativet Obligatoriskt, d.v.s. att Skatteverket endast medger minsta nödvändiga mängd diagnostikdata med anledning av användning av applikationer skickas till Microsoft.

Nedan beskrivs de två olika typerna av data som skickas till Microsoft när M365Apps används på en klientdator med inställningen "Obligatoriskt". Skatteverket har intentionen att använda mjukvarukonfigurationer för att begränsa insamling av obligatoriska data så långt som möjligt.

Data i den obligatoriska kategorin är sådana data som är nödvändiga för att hålla M365Apps uppdaterad, säker och fungera som förväntat. Detta hjälper även Microsoft att upptäcka betydande funktionsfel.

2.3.1 Obligatoriska diagnostikdata

Obligatorisk diagnostikdata är minsta mängden data som krävs för att hålla M365Apps uppdaterat samt säkerställa att implementationen fungerar som avsett på användarklienten.

Obligatorisk diagnostiskdata i M365Apps är organiserad i följande datakategorier:

Datakategori	Beskrivning	Exempel
Enhetsanslutning och konfiguration	Den här typen av Obligatoriska diagnostikdata innefattar information om enheten, dess konfiguration och anslutningsmöjligheter.	<ul style="list-style-type: none">Information om drivrutinen för en användares bildskärmskort som har orsakat flera M365Apps-programkrascher nyligen, så att M365Apps eventuellt slutar använda bildskärmskortet (och använder programvarurendering i stället) tills drivrutinen uppdateras.Diagnostiskinformation om användarens Internetanslutning för att förstå hur den kan påverka anslutningen till M365Apps-tjänster.
Prestanda för produkter och tjänster	Den här typen av Obligatoriska diagnostikdata innehåller information om enhetens eller tjänstens hälsa och prestanda.	<ul style="list-style-type: none">Händelser som genereras vid ett okontrollerat avslut av programmet.Den händelse som indikerar ett kraschat programtillägg och varför det kraschade.Inhämtning av vilken funktion som används om t.ex. PowerPoint avslutas okontrollerat, t.ex. bildspel, dokument öppet, spara, redigera, samredigering eller avstängning.
Produkt- och tjänstanvändning	Den här typen av Obligatoriska diagnostikdata innefattar information om användningen av enheten, operativsystemet, program och tjänster.	<ul style="list-style-type: none">Händelser som genereras för att fastställa om en fil har öppnats eller sparats.Resultatet av att lägga till ett konto i Outlook.

Datakategori	Beskrivning	Exempel
Programvaruinstallation och inventering	Den här typen av Obligatoriska diagnostikdata innefattar information om programvaruinstallation och uppdatering av enheten.	<ul style="list-style-type: none"> En händelse som används för att se till att nya användare kan starta och köra OneNote första gången. Information om funktionen för start av anpassade tilläggfunktioner i Excel som räknar startförsök, körningar, lyckade avslutningar, infrastrukturfel och användarkodfel.

2.3.2 Obligatoriska tjänstdata

Obligatoriska tjänstdata samlas in och skickas till Microsoft för att M365Apps-funktioner skall fungera t. ex. licensierings- och uppdateringstjänsten. Dessa tjänster är nödvändiga för att använda M365Apps.

Tjänst	Beskrivning
Autentisering	Autentisering är en tjänst som tillhandahåller validering av användar-ID för olika plattformar. Det krävs för att möjliggöra inloggning, aktivera en licens och för att skapa en enhetlig användarupplevelse mellan sessioner och olika enheter.
Klicka-och-kör	Klicka-och-kör är den installationsteknik som används för att installera och uppdatera M365Apps i Windows. Den söker efter nya versioner av M365Apps, och när en ny version är tillgänglig, laddar ned och installerar den. Klicka-och-kör upptäcker behovet av, utföra nedladdning av och installera uppdateringar, inklusive säkerhetsuppdateringar.
Medgivandetjänst	Medgivandetjänsten ger en konsekvent och omfattande upplevelse för att hantera inställningar för användarsekretess som är associerade med deras konton. Tjänsten används för att avgöra vilka sekretessmeddelanden som ska visas för användaren när ett program startas. Den spårar också de svar som användaren har gett till eventuella tidigare sekretessmeddelanden.
Förbättrade konfigurationstjänsten (ECS)	ECS ger Microsoft möjligheten att konfigurera om installationer utan behovet att om distribuera M365Apps igen. Det används för att gradvis kontrollera distribution av funktioner och uppdateringar medan effekten av distributionen övervakas från diagnostiska data som samlas in. Det används även för att hantera säkerhet och prestandaproblem med en funktion eller en uppdatering. Dessutom stöder ECS konfigurationsändringar relaterade till diagnostiska data för att säkerställa att rätt händelser samlas in.
Licensiering	Licensiering är en molnbaserad tjänst som stödjer in aktivering för nya installationer och hanterar licensen på en användares olika enheter efter att M365Apps har aktiverats. Det registrerar var och en av dina enheter och aktiverar M365Apps, kontrollerar status för din prenumeration och hanterar dina produktnycklar.

Tjänst	Beskrivning
Tjänstkonfiguration	Tjänstkonfiguration möjliggör förmågan att göra uppdateringar på M365Apps konfigurationsinställningar för att aktivera eller inaktivera klientfunktioner. Den kallas varje gång ett program startas och ger information om andra M365Apps-konfigurationer och tjänster. Tjänstkonfiguration styr också vilka tjänster som har utsetts som viktiga tjänster.
Telemetri	Telemetritjänsten används för att samla in diagnostikdata från M365Apps. Den möjliggör insamling av diagnostikdata som genereras av M365Apps, både obligatoriska och valfria diagnostikdata. Det ansvarar också för insamlingen av vissa nödvändiga servicedata för M365Apps.

3 Rättsliga överväganden

Inledningsvis bör det tydliggöras att M365Apps, vid eventuell implementation, skulle installeras lokalt i Skatteverkets it-miljö vilket medför att inga dokument eller filer av det kommer att sparas i Microsofts molnmiljö. Det innebär att den information som Skatteverket lämnar till Microsoft kan begränsas till vissa attribut från Skatteverkets AD samt nödvändig diagnostik- och tjänstdata.

3.1 Allmänna handlingar

Eftersom den verksamhetsinformation som hanteras i Word och de övriga applikationerna kommer att lagras i Skatteverkets it-miljö, och informationshanteringen alltså inte utkontrakteras till Microsoft, påverkas inte informationens karaktär av allmänna handlingar eller ej av att Skatteverket övergår till att använda M365Apps.

Beträffande den tjänst- och diagnostikdata m.fl. handlingar som översänds till och bearbetas av Microsoft i samband med Skatteverkets nyttjande av tjänsterna aktualiseras däremot frågor om i vilken utsträckning de handlingarna är allmänna, om arkivansvar m.m. Dessa frågor behandlas dock i huvuddokumentet.

3.2 Sekretess

3.2.1 Överföring av attribut till Entra ID

En grundförutsättning för att använda M365Apps är att Skatteverket använder Microsofts plattformstjänst för identitets- och åtkomsthantering, Entra ID. För att använda Entra ID måste vissa attribut från Skatteverkets AD överföras till Entra ID, vilket redogjorts för i Bilaga 1 Entra ID. För att använda M365Apps behöver minimum ytterligare fyra attribut¹ överföras till Microsoft.

Skatteverket gör bedömningen att de tillkommande uppgifterna inte omfattas av någon sekretessbestämmelse till skydd för enskild.

Ur myndighetens perspektiv kan uppgifterna i Skatteverkets AD omfattas av sekretess enligt 18 kap. 8 § p. 3 OSL. Skatteverket har gjort bedömningen att enskilda uppgifter samt uppgiftsmängden som hel- eller delmängd i myndighetens AD kan utgöra en sådan upplysning

¹ OrgId user identity, Machine Key, Machine Name samt Machine ID.

om säkerhets- eller bevakningsåtgärd som avses i bestämmelsen och som avser myndighetens system för automatiserad behandling av information. Skatteverket gör härvid bedömningen att de aktuella uppgifterna är sekretessreglerade enligt nämnd bestämmelse.

Mot bakgrund av uppgifternas karaktär och Microsofts möjlighet att skydda uppgifterna gör Skatteverket den sammantagna bedömningen att uppgifterna som överförs till Entra ID, var för sig såväl som tillsammans, inte omfattas av sekretess.

3.2.2 Överföring av nödvändig diagnostik- och tjänstdata

Microsoft samlar in omfattande diagnostik- och tjänstdata från användarens programvara. De data som samlas in kan genom attributen som behandlas i Entra ID knytas till en viss enskild användare, dvs i första hand en anställd på Skatteverket.

Vid en översiktlig genomgång av de uppgifter som samlas in kan Skatteverket konstatera att de enskilda dataposterna² inte omfattas av någon sekretessbestämmelse till skydd för enskild.

När omfattande mängder data samlas in innebär det en risk för s.k. kartläggning, vilket i sin tur kan leda till att den sammantagna informationen ger (uppgifter om) kunskap om nya förhållanden. Dessa nya förhållanden kan omfattas av sekretess. Skatteverket gör bedömningen att den sammantagna mängden uppgifter samt eventuellt tillkommande förhållanden inte innebär att de ger sådan information som omfattas av sekretess till skydd för enskild.

3.3 Dataskydd (GDPR)

De tillkommande attribut som överförs till Entra ID vid användandet av M365Apps föranleder ingen annan dataskyddsbedömning än den som gjorts vid införandet av Entra ID³.

Den diagnostik- och tjänstdata som samlas in av Microsoft innehåller personuppgifter enligt definitionen i artikel 4 GDPR. Behandling av personuppgifter föranleder alltid en riskbedömning och i vissa fall en konsekvensbedömning enligt art. 35 GDPR. Såväl de tillkommande attributen som diagnostik- och tjänstedata ska ingå i en kommande riskbedömning och eventuell konsekvensbedömning.

Utöver en riskbedömning behöver Skatteverket ta ställning till flera rättsliga frågor i samband anskaffandet av Microsofts tjänster. Arbetsgruppen har gjort bedömningen att överföring av personuppgifter till USA och risken att amerikanska myndigheter kan bereda sig tillgång till uppgifter inte i sig är ett hinder mot att anskaffa de aktuella tjänsterna.⁴

3.3.1 Personuppgiftsansvar

Skatteverket är personuppgiftsansvarig för behandlingen av anställdas personuppgifter. Syftet med att anskaffa de aktuella tjänsterna är att tillhandahålla arbetsverktyg. De anställda behöver tjänsterna för att utföra sina arbetsuppgifter. Det är således nödvändigt för Skatteverket att

² <https://learn.microsoft.com/sv-se/deployoffice/privacy/essential-services> samt <https://learn.microsoft.com/en-us/deployoffice/privacy/required-diagnostic-data>.

³ Se Bilaga 1 Entra ID

⁴ Se Bilaga 1 Entra ID samt huvuddokumentet

behandla personuppgifterna för att uppfylla anställningsavtalet. Därmed föreligger det en rättslig grund för behandlingen enligt artikel 6.1 b GDPR.⁵

Enligt art. 28.3 GDPR får ett personuppgiftsbiträde endast behandla personuppgifterna i enlighet med den personuppgiftsansvariges instruktioner.

Det framgår av det standardiserade personuppgiftsbiträdesavtalet⁶ att Microsoft endast ska behandla personuppgifter för att tillhandahålla Skatteverket tjänsterna enligt myndighetens dokumenterade instruktioner. Därutöver anges att personuppgifter även får behandlas för *verksamhetsutövning* i samband med att myndigheten tillhandahåller tjänsterna.⁷ Det framgår även av avtalet att kunden godkänner den behandlingen. Det förefaller således som att behandlingen för *verksamhetsutövning* går utöver instruktionen vilket indikerar att Microsoft gör bedömningen att de i den delen inte anser att de agerar som ett biträde.

Enligt avtalet innebär *verksamhetsutövning* bl.a. att personuppgifter behandlas för fakturering, ersättning till Microsofts personal samt för intern rapportering och företagsmodellering, till exempel prognostisering, intäkter, kapacitetsplanering och produktstrategi.

Skatteverket behöver i det fortsatta arbetet säkerställa att inga personuppgifter behandlas för ändamål som är oförenliga med det ursprungliga ändamålet, d.v.s. att tillhandahålla arbetsredskap till de anställda. I det arbetet ingår även att utifrån de faktiska omständigheterna klargöra rollerna för respektive behandling.

4 Sammanfattning

Arbetsgruppen har inte identifierat något rättsligt, säkerhetsmässigt eller funktionellt hinder mot att Skatteverket använder M365Apps. Det måste dock understrykas att detta är en preliminär bedömning som är gjord med utgångspunkt i den avgränsning avseende implementering som har definierats för utredningen.

⁵ Bedömning vid personuppgiftsbehandling (grundläggande bedömning), dnr. 8-2389033

⁶ Dataskyddstillägg för Microsofts produkter och tjänster, 2 januari 2024

⁷ Ibid., s. 5, "business operations"