Skatteverket

Promemoria

Datum
2024-02-26

Dnr
8-2800157

It-avdelningen

Analys av Microsoft Entra ID

1 Översikt över Microsoft Entra ID

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 samt Microsoft Teams.

Utredningen innefattar bl.a. att genomföra en noggrann analys av Entra ID för att bedöma dess potentiella roll som komplement till nuvarande Active Directory (AD).

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

1.1.1 Övergripande funktionalitet

Microsoft Entra ID (Entra ID), tidigare kallat Azure AD, är en molnbaserad plattformstjänst för identitets- och åtkomsthantering som tillhandahålls av Microsoft. Tjänsten används för att upprätthålla styrd åtkomst till bl.a. program och appar inom Microsofts molnerbjudande, t.ex. behörigheter inom MS 365 inklusive Teams, funktioner för multifaktorsidentifiering, identitetsskydd och lösenordsåterställning.

Skatteverket använder Microsofts katalogtjänst Active directory (AD) i sin it-miljö. I AD skapas identiteter för åtkomst till informationssystem som myndigheten använder. Där registreras behörigheter, bl.a. aktualiteten, och rättigheter samt enheter i en Windows-domän och Skatteverket kan genom tjänsten effektuera styrning och kontroll av användarnas behörigheter. Entra ID fyller motsvarande funktion inom Microsofts molnbaserade tjänsteutbud. En användare som förväntas använda Microsofts produkter och tjänster måste registreras i Entra ID. Behandlingen i Entra ID har efter registreringen som ändamål att genomföra behörighetsstyrning och avgränsa användaren så att vederbörande endast kan använda produkter och tjänster som personen har behörighet till. När medarbetare inom Skatteverket behöver förändra sina behörigheter och rättigheter i den molnbaserade it-miljön så styrs det genom behörighetsadministration och verkställs i Entra ID. Behörighetsadministrationen ombesörjs av Skatteverket.

Omfattningen av funktioner och nyttan med Entra ID sammanfaller med i vilket utsträckning som Skatteverket väljer att använda olika program och funktioner inom MS 365 inklusive Teams.

1.2 Funktionalitet inom utredningen

Tillämpning av Entra ID erbjuder verkställighet av en central behörighetsadministration inom Microsofts molnbaserade utbud av tjänster inklusive MS 365. Skatteverket kan genom myndighetens behörighetsadministration åsätta behörigheter och rättigheter till anställda och konsulter utifrån förväntat behov av applikation och resurser inom den molnbaserade tjänstemiljön.

En effekt av att Skatteverket ansluter till Entra ID är att all användning av domänen @skatteverket.se kommer att falla under myndighetens kontroll och kunna begränsas till myndighetens verksamhet vid användning av domänen i Microsofts molntjänster. Ett exempel

på detta är att om medarbetare försöker skapa ett Xbox-konto med sin jobbadress kommer hen att nekas.

För Skatteverkets anställda innebär en användning av Entra ID en Single Sign On (SSO) via behörighetskorten till MS 365 inklusive Teams.

2 Implementering av Entra ID

2.1 Omfattning av implementeringen av Entra ID

Entra ID är som anges ovan en plattformstjänst som ger stöd för användning av andra servicetjänster, t.ex. MS 365 inklusive Teams, som Microsoft tillhandahåller i molnmiljö. Omfattningen av implementeringen, eller användningen av Entra ID, är starkt beroende av hur omfattande användningen av Microsofts samlade molnutbud avses att bli för Skatteverket. I detta dokument är utgångspunkten att Skatteverkets användning av Entra ID är så begränsad att den egentligen inte möjliggör någon användning av Microsofts tjänster. Tanken har istället varit att endast tillåta de attribut i behandlingen som krävs i Entra ID, för att ge förutsättningar för en så enkel och renodlad bedömning som möjligt av plattformstjänsten. Bedömningen kan då ske ur ett rättsligt och säkerhetsmässigt perspektiv med den absolut grundläggande informationen som måste överföras från Skatteverkets AD till Entra ID.

I kommande bedömningar av Office 365 Apps for Enterprise och av Teams, eller av andra tjänster inom Microsoft molntjänster, kommer den grundläggande bedömningen av Entra ID att kompletteras med ytterligare nödvändiga attribut från Skatteverkets AD som måste överföras till Entra ID. I det läget ska varje nytt tillkommande attribut bedömas var för sig samt sett till helheten i den överförda informationsmängden.

2.2 Synkronisering av Skatteverkets AD med Entra ID

Utvalda användare och användarattribut synkroniseras löpande från Skatteverkets OnPrem AD till Skatteverkets Entra ID. Detta görs antingen med Microsoft Entra Connect Sync (tidigare Azure AD Connect) eller Microsoft Entra Cloud Sync. Skillnaden är att i den förra körs tjänsten OnPrem och i den senare körs tjänsten i Skatteverkets Microsoft molnmiljö. Båda verktygen låter myndighetens administratörer konfigurera vilka användarkonton samt vilka av dessas attribut som ska synkroniseras. Nedan anges de attribut som är föremål för synkronisering enligt den omfattning av implementeringen som omfattas av detta dokument.

Beskrivning	**AD-attribut**
Förnamn	givenName
Efternamn	surname
Modernt användarnamn	userPrincipalName
Är kontot aktiverat	enabled
Lösenord senast satt	pwdLastSet
Ankarobjekt	sourceAnchor
Land	countryCode
Visningsnamn	DisplayName

Skatteverket

It-avdelningen

Beskrivning	AD-attribut
E-postadress	mail

Synkronisering av ovan angivna attribut kommer att avse majoriteten av alla anställda och konsulter inom Skatteverket som förväntas använda program eller tjänster inom MS 365 inklusive Teams. Synkroniseringen sker för resp. användare efter ett aktivt val att så ska ske på användarnivå. Synkroniseringen mellan Skatteverkets AD och Entra ID kommer att ske regelbundet för att tillhandahålla en uppdaterad och korrekt identitets- och åtkomsthantering.

3 Allmänna handlingar

Den informationsmängd som ska överföras från Skatteverket till Microsoft vid skapandet av identitets- och åtkomsthanteringstjänsten och i samband med det fortsatta nyttjandet av tjänsten är uppgifter om personalens namn, e-postadress och landsbeteckning. Det får förutsättas att dessa uppgifter finns i befintliga allmänna handlingar (upptagningar för automatiserad behandling) i Skatteverkets personalsystem och att det som kommer att ske är att Skatteverket gör sammanställningar av de ifrågavarande uppgifterna ur handlingarna, fixerar sammanställningarna i listor och översänder listorna till Microsoft. Sammanställningarna är möjliga att göra tillgängliga med rutinbetonade åtgärder, varför de är att anse som förvarade och därmed allmänna handlingar hos Skatteverket redan innan de faktiskt har tillgängliggjorts (2 kap. 6 § TF), och de fixerade sammanställningarna är att betrakta som kopior eller dubbletter av dessa allmänna handlingar.

Översändandet till Microsoft av en lista med en eller flera fixerade sammanställningar innebär således inte att någon ny handling expedieras och därigenom blir upprättad hos Skatteverket. Sammanfattningsvis tillkommer inte några allmänna handlingar genom användandet av Entra ID.

4 Sekretess

Skatteverkets AD tillhör den personaladministrativa verksamheten hos myndigheten. Sekretess till skydd för enskild i personaladministrativ verksamhet regleras i 39 kap. offentlighets- och sekretesslagen (OSL). Inom den personaladministrativa sekretessen gäller ett skydd för enskilds personliga förhållanden i samband med bl.a. personalsocial verksamhet, om enskildas hälsotillstånd och i vissa typer av anställningsrelaterade ärenden. Sekretess kan också gälla inom personaladministrativ verksamhet för vissa angivna uppgifter, bl.a. enskilds bostadsadress, privata telefonnummer och fotografier som utgör underlag för tjänstekort.

De uppgifter som Skatteverket överför för användandet av Entra ID enligt bedömningen i detta dokument specificeras i avsnitt 2.2. De uppgifterna omfattas inte av sekretessbestämmelserna i 39 kap. OSL 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 vissa uppgiftsposter samt uppgiftsmängden som helhet i myndighetens AD kan utgöra en sådan upplysning om

säkerhets- eller bevakningsåtgärd som avses i bestämmelsen och som avser myndighetens system för automatiserad behandling av information.

I samband med sekretessprövningen enligt 18 kap. 8 § OSL har en utredning[1] företagits för att identifiera vilka attribut ur Skatteverkets AD som obligatoriskt måste överföras till Entra ID. Uppgifterna som Skatteverket måste överföra till Entra ID är personalens namn, e-postadresser och landsbeteckning. Dessa informationsposter utgör en mycket begränsad del av den informationsmängd som finns i Skatteverkets AD. Med hänsyn till att det endast är ett fåtal uppgifter som behöver överföras till Entra ID och till att de överförda uppgifternas karaktär är av mindre känslig art är det Skatteverkets bedömning att skaderekvisitet i 18 kap. 8 § OSL inte uppfylls.

Attributen som överförs till Microsoft omfattas inte av absolut sekretess vilket innebär att det ska ske en skadebedömning när uppgifterna lämnas till en tjänsteleverantör. Vid skadebedömningen är det avgörande att utlämnandet sker till en känd kontraktsparter, Microsoft. Skatteverket kan därmed skapa sig en bild av hur uppgifterna kommer hanteras och vilken risk för ytterligare spridning som föreligger. Mot bakgrund av den bilden och de enskilda uppgifternas känslighetsgrad har myndigheten gjort bedömningen att det inte föreligger sekretess gentemot Microsoft.

5 Dataskydd (GDPR)

Som framgår ovan krävs det att uppgifter överförs från Skatteverkets AD till Entra ID om myndigheten ska använda MS 365 inklusive Teams som arbetsredskap. Överföring av uppgifter kommer att ske inledningsvis när Skatteverket ansluter sig till MS 365 och därefter kontinuerligt för uppdatering efter förändringar i personalkollektivet. Vilka uppgifter som kommer att överföras till Entra ID beror på omfattningen av Skatteverkets upphandling samt vilka funktioner inom MS 365 myndigheten ska använda. Överföringen kommer att innefatta behandling av personuppgifter.

I detta avsnitt kommer endast frågan om tredjelandsöverföring till USA i samband med behandling av personuppgifter i Microsofts tjänster, inkl. Entra ID att beröras. Andra frågor med betydelse för dataskyddet, såsom rättslig grund och skyddsåtgärder, kommer att beskrivas och bedömas inom ramen för en fortsatt utredning, riskbedömning och eventuell konsekvensbedömning.

5.1 Tredjelandsöverföring generellt till USA

Huvudregeln är enligt art. 44 GDPR att personuppgifter inte får överföras till tredje land.

Personuppgifter får dock överföras till ett tredjeland om kommissionen har beslutat att tredjelandet säkerställer en adekvat skyddsnivå. När kommissionen bedömer om en adekvat skyddsnivå föreligger ska den särskilt bl.a. beakta rättsstatsprincipen, respekten för de mänskliga rättigheterna och de grundläggande friheterna, relevant lagstiftning, både allmän lagstiftning och sektorslagstiftning, inklusive avseende allmän säkerhet, försvar, nationell säkerhet och straffrätt och offentliga myndigheters tillgång till personuppgifter.

[1] Utredningen finns i dokumentet Utredning av SAM och SID synkronisering till Entra ID.

Med utgångspunkt i det ogiltigförklarade genomförandebeslutet om skölden för skydd av privatlivet (Privacy shield) har EU-kommissionen och den amerikanska administrationen förhandlat om nya förutsättningar för att uppnå en adekvat skyddsnivå för behandling av personuppgifter enligt amerikansk rättsordning. Den 10 juli 2023 fattade EU-kommissionen beslut om en genomförande akt[2] avseende beslut om adekvat skyddsnivå för överföring av personuppgifter till organisationer i USA som förbundit sig att följa regelverket inom ramen för dataskydd mellan EU och USA.

Kommissionens beslut enligt art 45.3 GDPR, att det föreligger en adekvat skyddsnivå har till stor del sin grund i de förändringar som USA:s regering vidtagit på området för nationell säkerhet (inklusive rättelsemekanismen).

EDPB framhåller att de förändringar som gjorts på området för nationell säkerhet i USA gäller all överföring och att kommissionens bedömning därmed även får betydelse för vilka ytterligare säkerhetsåtgärder som behöver vidtas vid överföringar enligt art. 46 GDPR.

Oaktat kommissionens adekvansbeslut ska den personuppgiftsansvarige, innan behandlingen sker, göra en allmän riskbedömning avseende behandlingen, inklusive tredjelandsöverföringen.

5.2 Överföring av personuppgifter till USA vid användning av Entra ID

Det framgår av Microsofts standardiserade personuppgiftsbiträdesavtal att vissa personuppgifter överförs eller kan komma att överföras till USA i samband med användning av MS 365. I avtalet[3] anges att överföringen till USA sker med stöd av standardavtalsklausuler[4] i enlighet med art. 46.2 c GDPR. Enligt uppgift avser Microsoft inte att ändra skrivningen i sitt biträdesavtal utan överföringen kommer även framgent grundas på standardavtalsklausulerna.

Mot bakgrund av adekvansbeslutet och uttalandena från EDPB (Europeiska dataskyddsstyrelsen) menar Skatteverket att det är möjligt att överföra de aktuella personuppgifterna till USA med stöd av standardavtalsklausuler enligt art. 46 GDPR. Några nackdelar för den registrerade i samband med en överföring med stöd av standardavtalsklausulerna relativt adekvansbeslutet har inte identifierats.

6 Sammanfattning

Arbetsgruppen har inte identifierat något rättsligt, säkerhetsmässigt eller funktionellt hinder mot att Skatteverket använder Entra ID för identitets- och åtkomsthantering vid användning av Microsofts molnbaserade tjänster. Det måste dock understrykas att detta är en preliminär bedömning som är gjord med utgångspunkt i den avgränsning avseende funktionalitet som har definierats för utredningen.

---

[2] Kommissionens genomförandebeslut i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 om adekvat skydd av personuppgifter enligt ramen för dataskydd mellan EU och Förenta staterna, C(2023)4745. Se även: https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en

[3] I biträdesavtalet beskrivs tillåtna överföringar till USA som sådana då uppgifter behandlas för bl.a. licenshantering och beredning av faktureringsunderlag. Denna typ av behandling benämns i biträdesavtalet som ”business operations”. Utöver överföring för business operations så kan överföring av personuppgifter ske i samband med supportärenden.

[4] https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en