Microsoft

Microsoft 365
Microsoft MoIndesign:
Offentlig sektor

Innehåll

1 Om Microsoft Molndesign för Offentlig Sektor – MSMD

Microsoft Molndesign för Offentlig Sektor (MSMD) är en sammanställning av verktyg, mallar, policyer, rapporter och utbildningar som gör det enklare för den offentliga sektorn i Sverige att använda sig av molntjänster i Microsoft 365. Designen är särskilt anpassad för organisationer som behöver uppfylla de regleringar, krav och lagar som gäller för offentlig sektor i Sverige. MSMD erbjuder en molnmiljö för IT-tjänster med mycket hög säkerhet och innehåller samtidigt ett antal verktyg som gör det enklare att följa regleringar och lagar som exempelvis dataskyddsförordningen (GDPR) och offentlighets- och sekretesslagen (OSL).

Microsoft Molndesign för Offentlig Sektor består av olika komponenter beroende på vilken typ av data som hanteras i Microsoft 365:

Nivå 1: Persondata	Komponent
1	**Microsoft Secure Score & Security Compliance Toolkit,** stödjer konfiguration, mätning och uppföljning för att säkerställa att det finns tillräckliga skyddsnivåer för personuppgifter i Microsoft 365.
2	**Compliance Manager,** förenklar arbetet med regelefterlevnad genom att översätta krav till konkreta åtgärder samt mäter graden av efterlevnad.
3	**E-Discovery & Data Subject Request,** gör det möjligt att hantera och svara på förfrågningar om åtkomst, rättelse, radering och export av personuppgifter i Microsoft 365.
4	**Microsoft Information Protection,** gör det möjligt för organisationer att klassa och kontrollera tillgång till information i Microsoft 365. Till exempel enligt principerna för KLASSA från Sveriges Kommuner och Regioner (SKR).
5	**Mall för Data Protection Impact Assessment (DPIA),** underlättar arbetet med att göra en DPIA om behov finns.
6	**Utbildning** i MSMD hos Microsofts partner.
Nivå 2: Sekretess	**Komponent**
7	**Office 365 Customer Lockbox,** inför extra steg för godkännande innan Microsoft kan ta del av kunddata, något som möjliggör sekretessprövning vid supportärenden.
8	**Double Key Encryption (eller motsvarande)** som krypterar tillgång till data för Microsoft via organisationens egen krypteringsnyckel.
Nivå 3: Hemlig	**Komponent**
9	**Microsoft 365 Hybrid med Exchange och SharePoint lokalt installerad,** gör det möjligt att lagra viss data lokalt och annan data i Microsoft 365.

Tabell 1 – Microsoft Molndesign för Offentlig Sektors olika komponenter

2 Lagstiftning att ta hänsyn till vid användning av molntjänster

För offentlig sektor i Sverige finns ett antal lagar och regleringar som berör hantering av information vid olika säkerhetsnivåer. Microsoft Molndesign för Offentlig Sektor underlättar regelefterlevnad av de tre vanligaste lagarna som är nödvändiga att beakta inom offentlig sektor; GDPR, OSL samt säkerhetsskyddslagen. Vilken lag som är tillämplig beror naturligtvis på vilken typ av information som ska lagras och bearbetas. Det kan även finnas annan lagstiftning som kan vara relevant att ta i beaktande.

Utöver de lagar som gäller alla organisationer inom offentlig sektor finns också särskilda lagar för hälso- och sjukvården. Några av dessa är:

- Apoteksdatalagen. Gäller när ett svenskt apotek använder en molntjänst för att behandla hälsoinformation om användare av läkemedel och farmaceutiska tjänster och/eller personer som har behörighet att skriva ut läkemedel.
- Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14). Gäller för vårdgivare och fastslår vissa detaljerade krav, till exempel att vårdgivare ska använda stark autentisering, ha en informationssäkerhetspolicy samt dokumentera och rapportera hur de uppfyller säkerhetspolicyn.
- Socialstyrelsens föreskrifter och allmänna råd (SOSFS 2011:9) om ledningssystem för systematiskt kvalitetsarbete. Innehåller allmänna råd om ledningssystem för systematiskt kvalitetsarbete samt föreskrifter såsom att vårdgivare endast får behandla hälsoinformation när det är nödvändigt för vårdens kvalitet.
- Patientdatalagen. Reglerar bland annat sammanhållen journalföring, spärrning av uppgifter och åtkomsthistorik.

Regleringar inom hälso- och sjukvården implementeras ofta genom dedikerade vårdsystem eller via processer i verksamheten. Det kan till exempel handla om hur tekniken i ett journalsystem som loggar hantering av journaler fungerar. Det kan också handla om hur processer ska utformas för att inhämta patientsamtycke på ett korrekt sätt.

2.1 Personuppgifter - GDPR

All data som innehåller personuppgifter berörs av dataskyddsförordningen (GDPR) och omfattar hela EU. I GDPR finns ett antal grundläggande principer som utgör kärnan av förordningen.

Principerna innebär bland annat att man som personuppgiftsansvarig ska:

- Ha stöd i dataskyddsförordningen för att få behandla personuppgifter
- Säkerställa att endast personuppgifter för specifika, särskilt angivna och berättigade ändamål samlas in
- Begränsa antalet personuppgifter som samlas in till vad som är nödvändigt för ändamålen
- Se till att personuppgifterna är riktiga
- Radera personuppgifter när de inte längre behövs
- Skydda personuppgifter, så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs
- Kunna visa att och hur man lever upp till dataskyddsförordningen.

Vilka säkerhetsåtgärder måste vidtas enligt GDPR?

GDPR innehåller inga uttryckliga krav på specifika säkerhetsåtgärder som en organisation måste vidta. GDPR ställer dock krav på lämpliga säkerhetsåtgärder som ger en lämplig säkerhetsnivå, tex kryptering eller pseudonymisering. Vilka säkerhetsåtgärder och vilken säkerhetsnivå som är lämpliga beror på ett antal faktorer. Det handlar bland annat om vilka uppgifter som behandlas, i vilken omfattning de behandlas, på vilket sätt de behandlas och vilka risker för den registrerades fri- och rättigheter som uppstår vid behandlingen. Dessutom ska man vid bedömningen av säkerhetsåtgärdernas lämplighet ta hänsyn till kostnaderna för åtgärderna och den senaste utvecklingen inom teknik- och säkerhetsområdet. Generellt kan man säga att ju högre riskerna är, desto högre nivå på säkerhet krävs för att minska de identifierade riskerna i så hög grad som möjligt.

(Källa: Integritetsskyddsmyndigheten web, dataskyddsförordningens grundläggande principer, februari 2021)

Data och personuppgifter i Microsoft 365 utgörs av olika kategorier

I en molntjänst skapas och lagras olika typer av data, varför Microsoft delar in data i fyra olika kategorier; kunddata, tjänstegenererande data, diagnostikdata och supportdata. Kategorierna gör det enklare att vid behov vidta skyddsåtgärder som är anpassade mot en specifik kategori.

Som ett exempel så kan man dela in riskanalyser i tre delar där den första hanterar personuppgifter i kunddata, den andra hanterar de personuppgifter som behövs för att tjänsterna skall kunna levereras, dvs tjänstegenererade data och diagnostikdata, samt den tredje kring supportdata vid supportärenden.

De fyra kategorierna innehåller följande data:

- **Kunddata:** Detta är alla data, inklusive text-, ljud-, video- eller bildfiler och programvara, som kunder tillhandahåller till Microsoft eller som tillhandahålls på kundernas vägnar genom deras användning av Microsofts onlinetjänster. Det omfattar data som kunder laddar upp för lagring eller bearbetning, samt anpassningar. Exempel på Kunddata är e-postinnehåll i Exchange Online, och dokument eller filer som lagras i SharePoint Online eller OneDrive för företag.
- **Tjänstgenererade data:** Detta är data som genereras eller härleds av Microsoft genom drift av tjänsten, till exempel användnings- eller prestandadata. De flesta av dessa data innehåller pseudonyma identifierare som genereras av Microsoft.
- **Diagnostikdata:** Dessa data samlas in eller erhålls av Microsoft från programvara som installeras lokalt av kunden i samband med Online-tjänsten och kan även kallas telemetri. Dessa data identifieras vanligen med attribut för den lokalt installerade programvaran eller den maskin som kör den programvaran.
- **Supportdata:** Detta är data som tillhandahålls Microsoft av eller på uppdrag av kunden för att erhålla teknisk support för Online Services.

Genom att förstå vilka typer av data som finns i Microsoft molntjänster blir det enklare att använda komponenterna i MSMD och tillämpa dem på olika kategorier av data.

Hur gör Microsoft Molndesign för Offentlig Sektor det enklare att upprätthålla GDPR?

- **Microsoft Secure Score & Security Compliance Toolkit,** stödjer konfiguration, mätning och uppföljning för att säkerställa att det finns tillräckliga skyddsnivåer för personuppgifter i Microsoft 365.
- **Compliance Manager** förenklar arbetet med efterlevnad genom att översätta regelkrav till konkreta åtgärder och ge ett mätbart mått på efterlevnad som går att dokumentera och utvärdera.
- **E-Discovery & Data Subject Request** gör det möjligt att svara på förfrågningar om åtkomst, rättelse, radering och export av personuppgifter i Microsoft 365.
- **Microsoft Information Protection** gör det möjligt för organisationer att klassa och kontrollera tillgång av information i Microsoft 365
- **Mall för Data Protection Impact Assessment (DPIA)** underlättar arbetet med att göra en DPIA om det bedöms nödvändigt.

2.2 Särskilt känsliga personuppgifter – Offentlighet- och sekretesslagen (OSL)

Offentlighet- och sekretesslagen (OSL) reglerar bland annat hur särskilt känsliga uppgifter som omfattas av sekretess ska skyddas. Det kan vara uppgifter om sjukdomar, hälsa, skyddade identiteter eller liknande. Lagen innehåller regler kopplat till allmänna handlingar, sekretesshandlingar och reglerar under vilka förutsättningar sekretess får brytas.

I Sverige har det under många år saknats en gemensam tolkning av hur sekretessklassad information ska hanteras vid outsourcing och användandet av molntjänster. Regeringen har därför tillsatt en utredning som bland annat ska ge förslag på tydligare rättsliga förutsättningar vid användandet av molntjänster. Utredningen har i ett delbetänkande föreslagit att en ny sekretessbrytande bestämmelse ska införas i OSL från januari 2022 som skulle ge ett tydligare lagstöd vid outsourcing av sekretessklassad information (SOU 2021:1).

Hur gör Microsoft Molndesign för Offentlig Sektor det enklare att upprätthålla OSL?

Förutom alla delar som omfattas av GDPR så ingår:

- **Office 365 Customer Lockbox** (extra kostnader kan tillkomma) som inför ett extra steg för sekretessprövning innan någon kan ges tillgång till kunddata vid support.
- **Double Key Encryption** (eller motsvarande) som hindrar tillgång till kunddata för alla som inte har tillgång till krypteringsnycklarna, inklusive Microsoft.

2.3 Säkerhetsskyddsklassificerade data – Säkerhetsskyddslagen

Information som är av betydelse för Sveriges säkerhet kan beröras av säkerhetsskyddslagen. Säkerhetskänslig verksamhet avser något som har betydelse för Sveriges säkerhet eller gäller information som Sverige har förbundit sig att skydda genom internationella åtaganden. Denna typ av information kan klassificeras enligt fyra olika nivåer; begränsat hemlig, konfidentiell, hemlig och kvalificerat hemlig. Eftersom det finns specifika krav kopplade till både fysisk säkerhet och svensk säkerhetsklassad personal kan det vara svårt att lagra säkerhetsklassad information i publika molntjänster.

Ett alternativ är att hantera säkerhetsklassad information lokalt och övrig information via en molntjänst. Man skapar då hybrida kopplingar mellan Exchange och SharePoint i molnet och i den lokala infrastrukturen. Verktygen Microsoft Information Protection och Data Loss Prevention (DLP) kan användas för att märka upp säkerhetsklassad information och förhindra att den lagras i molnet.

Som en guide för klassning av säkerhetsklassad information finns SÄPO:s vägledning i säkerhetsskydd.

Säkerhets-skyddsklass	Den skada som ett röjande av uppgifterna kan medföra medföra	Värdeord till stöd för bedömningen om en viss typ av skada föreligger
Kvalificerat hemlig	Ett röjande kan medföra en synnerligen allvarlig skada.	Synnerligen allvarliga negativa konsekvenser av stor omfattning, under lång tid, som utgör ett direkt hot mot den nationella förmågan. Konsekvenserna är inte begränsade till enstaka funktioner. Mycket svårt att återställa.
Hemlig	Ett röjande kan medföra en allvarlig skada.	Allvarliga/betydande negativa konsekvenser, av stor omfattning eller av väsentlig art, som innebär ett direkt hot mot den nationella förmågan, om än mot avgränsade funtioner. Svårt att återställa.
Konfidentiell	Ett röjande kan medföra inte obetydlig skada.	Påtagliga negativa konsekvenser för den nationella förmågan, om än i begränsad omfattning, som äventyrar, vållar skada, hindrar, underlättar för en antagonist eller innebär större avbrott.
Begränsat hemlig	Ett röjande kan medföra en endast ringa skada.	Ringa negativa konsekvenser som är begränsade till att påverka, försvåra eller störa den nationella förmågan i mindre omfattning.

Tabell 2 – Klassning av säkerhetsklassad information (källa: SÄPO, Vägledning i säkerhetsskydd, Informationssäkerhet, juni 2019)

Hur hjälper Microsoft Molndesign för Offentlig Sektor att upprätthålla säkerhetsskyddslagen?

Förutom komponenter som finns beskrivna i avsnitten avseende GDPR och OSL så erbjuder Microsoft:

- **Hybrid koppling mellan Microsoft 365, Exchange och en lokal SharePoint** vilket gör att information som klassats högre än vad som tillåts lagras i Microsofts moln kan sparas lokalt.
- **Ytterligare funktioner som Microsoft Information Protection, Cloud App Security och Data Loss Prevention** hjälper till att upprätthålla beslutade regler kring hur data får lagras.

2.4 Sammanställning

Nedan är en sammanställning av de olika delarna i MSMD och hur de adresserar olika lagstiftningar.

MSMD	GDPR	OSL	Säkerhets-skyddslagen
1. Microsoft Secure Score & Security Compliance Toolkit	X	X	X
2. Compliance Manager	X	X	X
3. E-Discovery & Data Subject Request	X	X	N/A
4. Microsoft Information Protection	X	X	X
5. DPIA mall	X	X	N/A
6. Utbildning i MSMD	X	X	X
7. Office 365 Customer Lockbox	N/A	X	N/A
8. Double Key Encryption	N/A	X	N/A
9. Microsoft 365 Hybrid med Exchange och SharePoint lokalt installerad	N/A	N/A	X

Tabell 3 – Sammanställning av olika delar i MSMD

3 Komponenter som ingår i MSMD

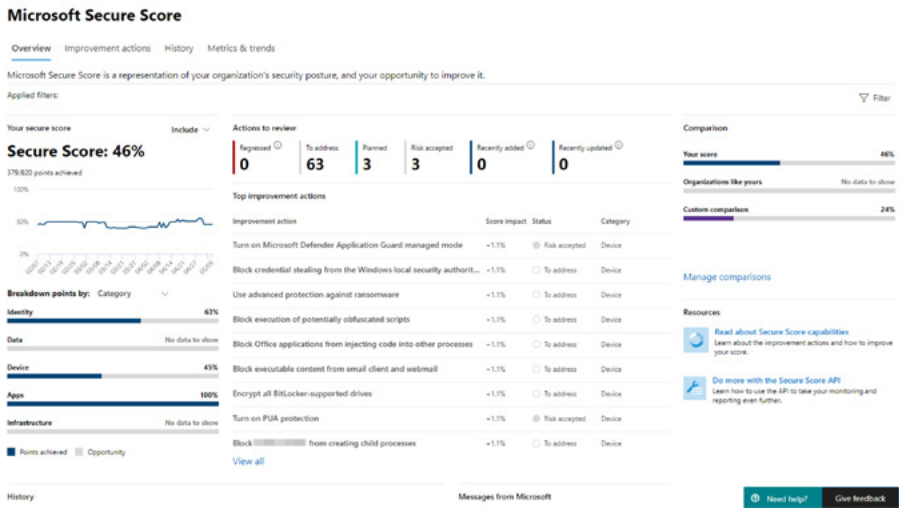
Nedan beskrivs kortfattat de komponenter som ingår i MSMD.

3.1 Microsoft Secure Score & Security Compliance Toolkit

En hög grundläggande IT-säkerhet krävs för att det ska vara möjligt att uppfylla regulatoriska krav. Secure Score ingår i MSMD och mäter verksamhetens säkerhetsnivå och ger vägledning kring åtgärder som kan göras för att höja säkerheten. Security Compliance Toolkit underlättar arbetet med klienternas säkerhet.

Microsoft Secure Score

Secure Score är ett verktyg som genom mätningar, rekommendationer och vägledning kan höja de delar av organisationens säkerhetsnivå som är kopplade till Microsoft 365 . Secure Score utvärderar säkerhetsstatus för identiteter, enheter, information, appar och infrastruktur och visar resultatet med hjälp av poäng. Rekommendationer ges sedan för vilka säkerhetshot som bör prioriteras och hur de kan åtgärdas.



Figur 1 – Microsoft Secure Score

Poängen i Secure Score påverkas av:

- Hur rekommenderade säkerhetsåtgärder är konfigurerade
- Hur säkerhetsrelaterade uppgifter utförs
- Huruvida förbättringsåtgärder vidtagits med hjälp av alternativa lösningar som exempelvis tredjepartsapplikationer

Vissa förbättringsåtgärder ger poäng när de är fullständigt konfigurerade för samtliga användare och andra ger delpoäng om de konfigurerats för vissa enheter eller användare. Om man inte kan eller vill genomföra en föreslagen förbättringsåtgärd kan man istället välja att acceptera risken.

Säkerhet bör alltid balanseras mot användbarhet och alla rekommendationer kanske inte fungerar i alla miljöer.

Security Compliance Toolkit

Security Compliance Toolkit (SCT) är verktyg som ger administratörer med ansvar för IT-säkerhet möjlighet att hämta, analysera, testa, redigera och lagra rekommenderade konfigurationsbaslinjer som erbjuds från Microsoft.

SCT gör det enklare för IT-administratörer att hantera organisationens grundprincipobjekt (GPO) och befintliga GPO-objekt kan jämföras mot Microsofts rekommenderade baslinjer. De kan sedan redigeras, sparas i arkiv och tillämpas brett via Active Directory eller individuellt via lokala principer.

Följande baslinjer finns att tillgå:

- Windows 10 security baselines
- Windows Server security baselines
- Microsoft Office security baseline
- Microsoft Edge security baseline

3.2. Compliance Manager

För organisationer som behöver uppfylla krav från flera olika regleringar kan det kännas överväldigande att veta var man ska börja arbetet. Compliance Manager är en komponent i MSMD som förenklar arbetet med efterlevnad genom att översätta regelkrav till konkreta åtgärder. Detta arbetssätt ger ett kvantifierbart mått på efterlevnad.

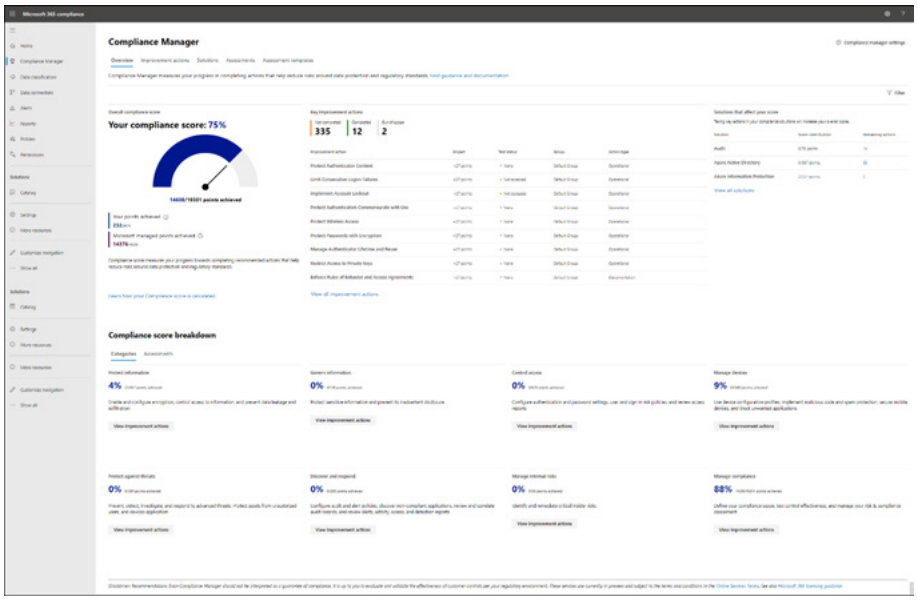
Globalt kan det förekomma så många som 220 uppdateringar och justeringar i olika regleringar varje dag. Med Compliance Manager blir det enklare för organisationen att hålla sig uppdaterad om nya eller förändrade krav.

Compliance Manager har bland annat följande funktioner:

- Inbyggda utvärderingar för branschstandarder och föreskrifter samt anpassade utvärderingar för att uppfylla en organisations unika efterlevnadsbehov.
- Arbetsflödesfunktioner som hjälper organisationen att genomföra riskbedömningar.
- Detaljerad steg-för-steg-vägledning med förslag till förbättringsåtgärder som gör det enkelt att följa de standarder och regler som är mest relevanta för en specifik organisation.
- Riskbaserad efterlevnadspoäng som kartlägger befintlig status för efterlevnad.

Att uppfylla regleringar som GDPR handlar om ett delat ansvar. Compliance Manager hjälper till att tydliggöra vad som är Microsofts ansvar, vad som är organisationens ansvar och vad som är ett delat ansvar. Verktyget hjälper också till att dokumentera:

1. Åtgärder relaterade till Microsofts molntjänster, som Microsoft ansvarar för att implementera
2. Organisationens åtgärder, som implementeras och hanteras av organisationen
3. Delade åtgärder, som organisationen och Microsoft har ett delar ansvar för att implementera



Figur 2 – Compliance manager - Microsoft 365

Genom att använda Compliance Manager får man en bild av hur befintlig regelefterlevnad motsvarar krav från GDPR och annan reglering.

3.3 E-Discovery & Data Subject Request

GDPR ger individer rätt att hantera egna personuppgifter som har samlats in av en organisation. Det handlar till exempel om rätten att begära kopior av uppgifterna, korrigeringar, begränsa behandling, radera eller ta emot data i elektroniskt format så att den kan flyttas till en annan personuppgiftsansvarig.

En formell begäran från en registrerad person till en personuppgiftsansvarig om att vidta åtgärder för deras personuppgifter kallas på engelska för en Data Subject Request eller DSR. I Microsoft 365 finns inbyggda verktyg för att uppfylla en DSR enligt GDPR.

Det första steget i att besvara en DSR är att identifiera de personuppgifter som är föremål för förfrågan. Detta görs genom sökning av efterfrågade personuppgifter med hjälp av eDiscovery-verktyget i Microsoft 365.

Efterlevnadscentrets funktion för innehållssök kan användas för att söka efter information som lagrats som e-post, dokument eller igenom konversationer i Teams eller på Skype.

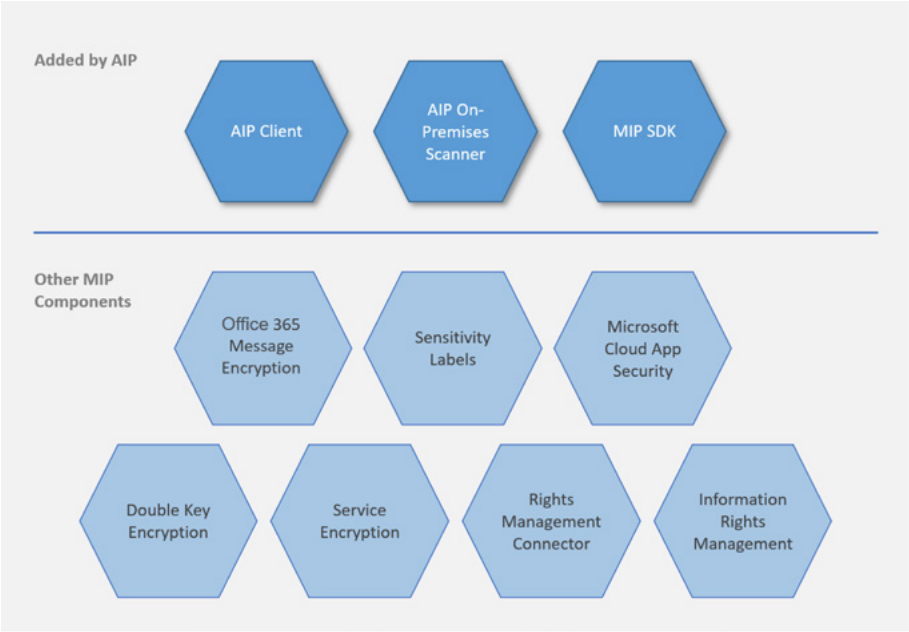
Vid sökningen visas antalet platser och ett uppskattat antal sökresultat i sökstatistiken. Verktyget kan snabbt presenetera statistik, till exempel över vilka platser som har flest objekt som matchar aktuell sökfrågan. Resultaten kan förhandsgranskas eller exporteras till en lokal dator för vidare behandling i tredjepartsverktyg.

3.4. Microsoft Information Protection

Ett ofta använt verktyg för styrning och klassificering inom offentlig sektor är KLASSA från Sveriges kommuner och regioner (SKR). Det är ett självskattningsverktyg som hjälper till att klassificera verksamhetssystem och datalagring.

Microsoft Information Protection (MIP) har flera tekniska lösningar för att upprätthålla ett effektivt klassificeringssystem. Azure Information Protection är den mest kända. Den bygger på klassificering av information via etiketter, samt skydd och kryptering via Azure Rights Management.

Med den som bas för rättighetshantering är det möjligt för organisationer att styra tillgång och åtkomst av information i Microsoft 365.



Figur 3 – Microsoft Information Protection består av ett antal olika tekniska lösningar där Azure Information Protection (AIP) är en viktigt del.

Delarna i Microsoft Information Protection hjälper till att uppfylla regleringar där data kan behöva hanteras olika beroende på vilken klass den tillhör, till exempel regler för var den får lagras.

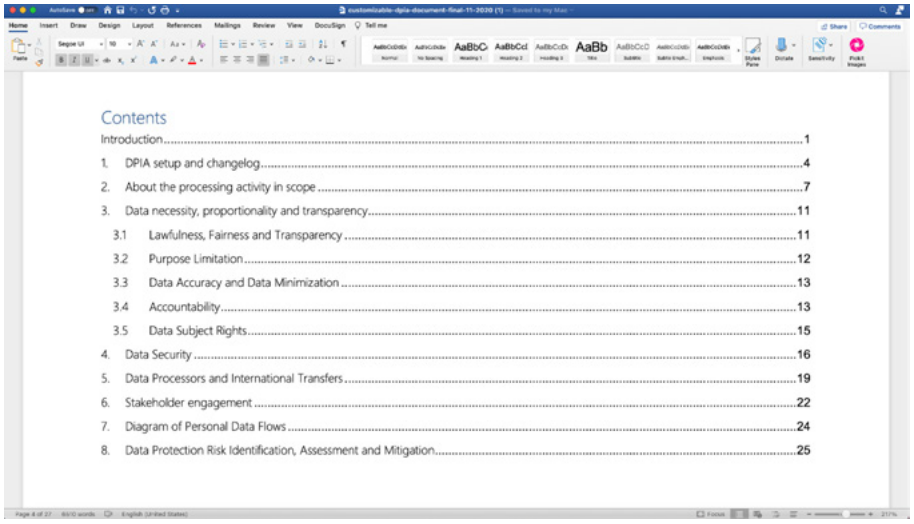
MIP ger också möjligheter att:

- Spåra och kontrollera vem som har tillgång till känslig information och hur den används.
- Identifiera riskbeteenden hos användare och spärra information som används felaktigt.
- Kräva multifaktorsinloggning för att öppna skyddade dokument.
- Använda klassificeringen i de regelverk som byggs upp i Microsoft 365, exempelvis DLP för att säkerställa att information hanteras korrekt.

Microsoft ser till att plattformen M365 har hög IT-säkerhet, men vilka användare som ska ha tillgång till organisationens data styr organisationen själv över.

3.5. Data Protection Impact Assessments (DPIA)

Enligt GDPR ska registeransvariga göra en konsekvensbedömning av dataskydd (DPIA) för behandling av data som "sannolikt kommer att leda till en hög risk för fysiska personers rättigheter och friheter". Det finns inget i Microsoft 365 som nödvändigtvis kräver att en DPIA skapas av en personuppgiftsansvarig. Huruvida en DPIA krävs handlar snarare om hur en organisation konfigurerar och använder Microsoft 365 samt vilka personuppgifter som kommer att lagras och användas i tjänsten.



Figur 4 – Mall för Data Protection Impact Assessments (DPIA)

Vilken data som kommer att lagras och användas i Microsoft 365 kan dokumenteras i en "Data Protection Impact Assessments" (DPIA). Mer information om detta samt en mall med färdiga exempel som kan spara mycket tid finns här

3.6. Utbildning i MSMD

Genom Microsofts partnernätverk erbjuds introduktion till Microsoft Molndesign, bland annat genom workshops.

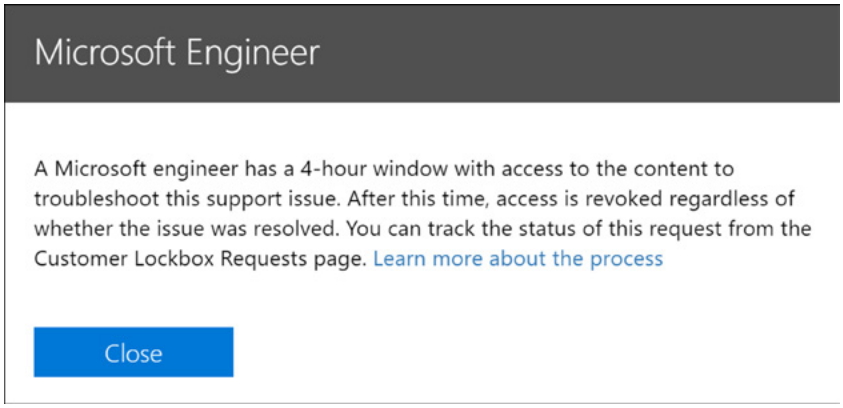
Grunder	Teknik	Praktik
Introduktion MSMD	Microsoft Secure Score	Mäta säkerhet
GDPR	Compliance Manager	Compliance analys
OSL	DPIA mall	Kryptering
Säkerhetsskyddslagen	Double Key Encryption	Sätta upp miljö
Informationssäkerhet	Data Subject Request	Verifiera
Klassificering	Customer Lockbox	

Tabell 4 – Utbildningar i MSMD

3.7. Office 365 Customer Lockbox

Nästan all felsökning i Microsoft 365 är automatiserad och kräver inte tillgång till kunddata. Skulle det ändå behövas tillgång till kunddata, exempelvis vid ett supportärende, måste personal på Microsoft följa en gedigen process för att få godkännande till åtkomst. Med Customer Lockbox för Office 365 får organisationen möjlighet att granska och godkänna, eller avvisa, en begäran från Microsoft om tillgång till kunddata (dvs organisationens data). Processen används i situationer där en Microsoft-tekniker behöver åtkomst till kunddata för att kunna lösa en supportförfrågan.

Customer Lockbox kan användas som ett steg där en extra bedömning görs av huruvida information som kan komma att delas vid en supportförfrågan lyder under sekretess eller ej, och om informationen i så fall kan delas eller inte.



Figur 5 – Office 365 Customer Lockbox

Customer Lockbox-förfrågningar sparas i en granskningslogg. Det ger möjlighet att spåra tillfällen när denna typ av begäran har gjorts, om de accepterats eller nekats samt vilka åtgärder som sedan utförts. Genom sökverktyget för granskningslogg i Security & Compliance Center kan dessa loggar plockas fram vid behov.

3.8. Double Key Encryption

Det finns en mängd alternativ för kryptering i Microsofts molnplattformar. Till exempel kryptering av data under transport, av databaser eller av dokument. Krypteringsnycklar kan också lagras i särskild hårdvara där Microsoft inte kan komma åt nycklarna. De kan också lagras utanför själva molntjänsten, exempelvis genom Double Key Encryption (DKE), baserat på funktioner i och Microsoft 365.

DKE använder två olika krypteringsnycklar för att skydda information med mycket hög sekretess. En nyckel finns hos Microsoft. Den andra finns hos organisationen, som därmed får full kontroll och ägandeskap över den andra nyckeln. På så sätt kan inte Microsoft få åtkomst till känsliga data.

DKE kan vara bra för att hantera extremt känslig data, till exempel information som hanteras av organisationer som bedriver sjukvård eller hanterar stora mängder känsliga personuppgifter.

När en organisation har något av följande krav kan det vara lämpligt att använda DKE för att skydda information:

- Under alla omständigheter ska endast behöriga inom organisationen kunna dekryptera mycket känsligt innehåll
- Microsoft får inte ha någon åtkomst till mycket känsliga data
- När nycklar ska stanna inom en geografisk gräns samt under egen kontroll.

När DKE används kan funktionalitet för vissa tjänster begränsas, som exempelvis funktioner för analys som är beroende av tillgång till information och data. Det bör därför alltid göras en konsekvensanalys innan DKE införs.

Ett alternativ/komplement till DKE är även end-to-end encryption (E2EE) för Teams-möten som gör att samtal krypteras direkt mellan deltagare och gör dem därmed otillgängliga även för Microsoft. Funktionen annonserades som preview i mars 2021.

Dessa typer av krypteringslösningar kan vid behov även användas för att adressera olika typer av frågor kopplade till tredjelandsöverföringar, utländsk lagstiftning, utlämnande av data vid brottsutredningar mm. Lär mer om detta här.

3.9. Microsoft 365 Hybrid med Exchange och SharePoint lokalt installerad

Med en lokalt installerad hybrid miljö (med Exchange och SharePoint) kan data som inte får hanteras i molnet sparas lokalt men ändå hanteras av användare på ett sätt som upplevs smidigt och integrerat.

Med hjälp av klassificering och Data Loss Prevention (DLP) kan man med hjälp av regler förhindra att viss information sparas i molnet. Användare styrs istället till att spara den informationen i en lokal SharePoint-miljö.

Ett typiskt exempel är att tydligt synliggöra klassificering med hjälp av teman på SharePoint. Det gör det enkelt för användare att förstå i vilken lagringsyta de befinner sig samt vilken sorts information som är avsedd att hanteras på den platsen.

4 Fördjupning i MSMD komponenter

Läs mer om komponenterna i MSMD på följande länkar.

4.1. Microsoft Secure Score & Security Compliance Toolkit

Secure Score:
https://docs.microsoft.com/sv-se/microsoft-365/security/mtp/microsoft-secure-score

Security Compliance Toolkit:
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10

4.2. Compliance Manager

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager

4.3. E-Discovery & Data Subject Request

https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-office365

4.4. Microsoft Information Protection

https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection

4.5. DPIA mall

https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dpia-office365

4.6. Office 365 Customer Lockbox

https://docs.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests

4.7. Double Key Encryption

https://docs.microsoft.com/en-us/microsoft-365/compliance/double-key-encryption

4.8. Microsoft 365 Hybrid med Exchange och SharePoint lokalt installerad

https://docs.microsoft.com/en-us/exchange/exchange-hybrid

5. Appendix A: Exempel på tekniska skyddsåtgärder vid olika informationsklasser

Utifrån ett teknisk perspektiv finns olika skyddsåtgärder i Microsoft 365 för olika klasser av information. Nedan är ett exempel som ofta används (källa: Altitude 365)

Klasser:

Servicegenerad Data, Diagnostisk Data & Support Data

- Personuppgifter som behövs för att tjänsten ska fungera

Customer Data

- Personuppgifter som skapas av användare i epost eller filer

OSL

- Sekretessklassad data enligt OSL

Klasser som används av KLASSA ifrån SKR, utvecklad av MSB

- K0 – Öppen, ingen skyddsnivå
- K1 – Grundläggande skyddsnivå
- K2 – Utökad skyddsnivå
- K3 – Hög skyddsnivå

Kryptering/ Skyddsmekanism	Service-generated Data, Diagnostic Data & Support Data	Customer Data	OSL	K0	K1	K2	K3	Säkerhets-skyddslagen
TLS / IPSec between Microsoft servers	X	X		X	X			
Bitlocker/DM-Crypt	X	X		X	X	X	X	
Service encryption MMK	X	X		X	X	X	X	
Service encryption CK (BYOK)	X	X		X	X	X	X	
TLS	X	Epost		X	X			
Enforced TLS		Epost	X	X	X	X	X	X
MTA-STS		Epost	X	X	X	X	X	
MIP MMK						X		
MIP DKE (HYOK 2.0)		X	X			X	X	
OME/AME		X	X	X	X	X		X
DLP	X	X	X	X	X	X	X	X
Auditing	X	X	X	X	X	X	X	
Customer Lockbox	X	X	X	X	X	X	X	
SharePoint Hybrid		Filer	X					X
Exchange Hybrid		Epost	X					X

Tabell 5 – Utbildningar i MSMD

Microsoft

Tack
Merci
Thank you
Gracias