DATA & MORE SUPPORT

Appregistrering og tilladelser

Data & More Compliance Solution (DMCS) opretter forbindelse til Microsoft 365 via en appregistrering i Deres Entra ID-tenant. De kan vælge mellem fire måder at oprette forbindelse på. De adskiller sig i, hvad Data & More har tilladelse til at gøre, fra skrivebeskyttet scanning til forebyggelse af datatab i realtid. Denne artikel forklarer hver mulighed og samtlige tilladelser, den anmoder om.

01
Demo
Skrivebeskyttet scanning af mail og filer. Velegnet til en prøveperiode.

02
Produktion
Fuld scanning samt politikhandlinger på mail, filer og Teams.

03
Produktion + DLP
Alt i Produktion samt forebyggelse af datatab i realtid og Copilot.

04
Tilføj appregistrering
De opretter og administrerer Deres egen appregistrering.

- **Demo**: skrivebeskyttet scanning af mail og filer. Velegnet til en prøveperiode.
- **Produktion**: fuld scanning samt politikhandlinger på mail, filer og Teams.
- **Produktion + DLP**: alt i Produktion samt forebyggelse af datatab i realtid og Copilot.
- **Tilføj appregistrering**: De opretter og administrerer Deres egen appregistrering.

Sådan fungerer samtykke

Gå til **Indstillinger → Appregistrering** i Data & More. De fire knapper øverst svarer til de fire muligheder: **Demo**, **Produktion**, **Produktion + DLP** og **Tilføj appregistrering**. De første tre benytter en appregistrering, som Data & More vedligeholder: vælg knappen for at få et samtykklink, hvorefter en Microsoft 365-administrator godkender tilladelserne for hele organisationen. Hvis De ikke selv er administrator, giver samme skærmbillede Dem mulighed for at sende en invitations-e-mail til en administrator.

Alle tilladelser i de første tre muligheder er **applikationstilladelser**. Data & More fungerer som en tjeneste og ikke som en tillogget bruger, så scanningen fortsætter, når medarbejdere er fraværende, og ingen personlige adgangskoder er involveret. De kan til enhver tid se og tilbagekalde de tildelte tilladelser i Entra Administration under **Virksomhedsprogrammer**.

Skrivetilladelser medfører ikke automatisk sletning. Sletninger gennemgår et godkendelsestrin med menneskelig kontrol i Data & More, inden noget fjernes.

Hvem skal godkende

- **Global administrator** eller **Privilegeret rolleadministrator**: godkender apptilladelserne (alle muligheder).
- **Exchange-administrator** (eller global administrator): det engangs-trin "Giv Exchange-adgang" i Produktion + DLP.
- **Teams-administrator** (eller global administrator): det engangs-trin "Installer Teams-bot" i Produktion + DLP.

Hvad hver mulighed kan

Funktionalitet	Demo	Produktion	Produktion + DLP	Tilføj appregistrering
Scan Outlook-mail	Ja	Ja	Ja	De vælger
Scan OneDrive- og SharePoint-filer	Ja	Ja	Ja	De vælger

Scan Teams-kanaler og -chats	Nej	**Ja**	**Ja**	De vælger
Genkend kendte personer fra Outlook-kontakter	Nej	**Ja**	**Ja**	De vælger
Læs Deres følsomhedsmærkater (Purview)	**Ja**	**Ja**	**Ja**	De vælger
Send rapporter og notifikationer via e-mail	**Ja**	**Ja**	**Ja**	De vælger
Politikhandlinger: flyt til vault, slet, gendan, tag, anvend mærkater	Nej	**Ja**	**Ja**	De vælger
Forebyggelse af datatab i realtid på e-mail, filer og Teams	Nej	Nej	**Ja**	De vælger
Copilot-forespørgsler og -svar	Nej	Nej	**Ja**	De vælger
Advarsler i Teams fra Data & More-botten	Nej	Nej	**Ja**	De vælger
Hvem vedligeholder appregistreringen	Data & More	Data & More	Data & More	De
Adgang til Deres data	Kun læsning	Læsning og skrivning	Læsning og skrivning	Som De tildeler

De kan opgradere til en større mulighed senere. Vælg den større muligheds knap under Indstillinger og godkend igen; de ekstra tilladelser føjes til den eksisterende app.

Mulighed 1: Demo (kun læsning)

Det mindste sæt. Data & More læser postkasser og filer for at vise Dem, hvor personlige og følsomme data befinder sig, men kan ikke ændre noget i Deres tenant. Brug det til en prøveperiode eller en indledende vurdering.

- **Dækker:** Outlook, OneDrive og SharePoint-filer.
- ***Ændrer data:*** nej, kun rapporter.
- **Godkendelse:** Global administrator, ét klik.

Tilladelse	Adgang	Hvad Data & More bruger den til
`User.Read.All`	Læsning	Læser listen over brugere og deres grundlæggende profil (navn, e-mail, afdeling, leder), så systemet ved, hvis postkasser og OneDrives der skal scannes, og hvem der ejer de fundne data.
`Directory.Read.All`	Læsning	Læser grupper og gruppemedlemskab, organisationens navn og verificerede domæner samt tildelte tilladelser. Bruges til gruppebaseret afgrænsning og knappen **Kontroller tilladelser**.
`Mail.Read`	Læsning	Læser e-mails og vedhæftede filer, så de kan scannes for personlige og følsomme data.
`Files.Read.All`	Læsning	Læser filer i OneDrive og SharePoint samt oplysninger om, hvem de er delt med, så de kan scannes.
`InformationProtectionPolicy.Read.All`	Læsning	Læser Deres Microsoft Purview-følsomhedsmærkater, så fund kan sammenlignes med, hvordan data er mærket.
`Mail.Send`	Afsendelse	Sender Data & More-rapporter og -notifikationer fra en postkasse, De vælger. Den læser eller ændrer ikke eksisterende mail.

Mulighed 2: Produktion (læsning og skrivning)

Til daglig brug. Data & More scanner hele Microsoft 365, herunder Teams, og udfører de politikker, De har konfigureret: flytning af følsom mail og filer til en vault, sletning af data efter udløbet opbevaringsperiode, gendannelse, tagging og anvendelse af følsomhedsmærkater. Alle tilladelser er påkrævet.

- **Dækker:** Outlook, OneDrive, SharePoint og Teams.
- **Ændrer data:** kun når en politík, De har konfigureret, angiver det.
- **Godkendelse:** Global administrator, ét klik.

Microsoft Graph

Tilladelse	Adgang	Hvad Data & More bruger den til
`User.Read.All`	Læsning	Brugere og grundlæggende profil, licenser og fotos: hvis data der skal scannes, og hvem der ejer dem.
`Directory.Read.All`	Læsning	Grupper og medlemskab, Teams og deres kanaler, organisationsoplysninger samt tilladelseskontrollen.
`Mail.ReadWrite`	Læsning og skrivning	Scanner e-mails og vedhæftede filer. Politikker kan flytte mail til mappen `GDPRvault`, flytte den tilbage, slette eller gendanne den samt tilføje Outlook-kategorier.
`MailboxSettings.ReadWrite`	Læsning og skrivning	Opretter de Outlook-kategorier, der bruges til tagging, og skelner delte postkasser fra personlige.
`Mail.Send`	Afsendelse	Sender rapporter og notifikationer fra en postkasse, De vælger.
`Contacts.Read`	Læsning	Læser Outlook-kontakter, så eksterne personer, som Deres medarbejdere samarbejder med, genkendes som kendte personer.
`Files.ReadWrite.All`	Læsning og skrivning	Scanner OneDrive-, SharePoint- og Teams-filer. Politikker kan flytte filer til en vault-mappe, slette eller gendanne dem samt anvende en følsomhedsmærkat.
`Sites.ReadWrite.All`	Læsning og skrivning	Finder SharePoint-sites og dokumentbiblioteker, skriver Data & More-metadata ind i bibliotekskolonner og gendanner filer fra papirkurven.
`Sites.FullControl.All`	Administration	Føjer Data & More-metadatakolonner til dokumentbiblioteker, når en politík kræver det.
`Team.ReadBasic.All`	Læsning	Læser grundlæggende oplysninger om Teams.
`ChannelMessage.Read.All`	Læsning	Læser opslag og svar i Teams-kanaler, så de kan scannes.
`Chat.Read.All`	Læsning	Læser 1:1- og gruppechats i Teams, så de kan scannes.
`InformationProtectionPolicy.Read.All`	Læsning	Læser Deres følsomhedsmærkater, så politikker kan anvende dem, og fund kan sammenlignes med dem.

SharePoint

Disse tre tildeles via SharePoint API i stedet for Microsoft Graph. De bruges til at læse site-grupper og site-ejere, så fund på et site sendes til de ansvarlige personer.

Tilladelse	Adgang	Hvad Data & More bruger den til
`Sites.Read.All`	Læsning	Læser SharePoint-sitegrupper og deres medlemmer.

`Sites.FullControl.All`	Administration	Læser et sites ejergruppe.
`User.Read.All`	Læsning	Oversætter SharePoint-brugere til personer i Deres mappe.

Scanning af Exchange Online-arkivet

Online-arkivet læses via Exchange Web Services (EWS), som ikke er dækket af nogen af pakkerne. Hvis De ønsker at scanne det, skal De også tildele **Office 365 Exchange Online**-applikationstilladelsen `full_access_as_app`.

Mulighed 3: Produktion + DLP (læsning og skrivning)

Alt i Produktion samt forebyggelse af datatab i realtid. Microsoft 365 notificerer Data & More i det øjeblik, en e-mail sendes, en fil deles eller en Teams-besked postes. Data & More kontrollerer den op imod Deres DLP-politikker og kan advare, tilbageholde eller blokere den inden for få sekunder. Det dækker også Microsoft 365 Copilot og kan advare brugere via en Teams-bot.

- **Dækker:** Produktion samt forebyggelse af datatab i realtid og Copilot.
- **Ændrer data:** blokerer, tilbageholder eller begrænser deling, når en DLP-politík matcher.
- **Godkendelse:** Global administrator samt op til tre engangs-trin.

Ud over alle Produktionstilladelser

Tilladelse	API	Adgang	Hvad Data & More bruger den til
`AiEnterpriseInteraction.Read.All`	Microsoft Graph	Læsning	Læser Microsoft 365 Copilot-forespørgsler og -svar, så de kan kontrolleres for følsomme data. Hver bruger skal have en Microsoft 365 Copilot-licens.
`AuditLogsQuery.Read.All`	Microsoft Graph	Læsning	Søger i revisionsloggen efter Copilot Chat- og agentaktivitet, som Copilot-eksporten ikke inkluderer.
`AppCatalog.Read.All`	Microsoft Graph	Læsning	Finder Data & More DLP-botten i Deres Teams-appkatalog.
`TeamsAppInstallation.ReadWriteForUser.All`	Microsoft Graph	Installation	Installerer Data & More DLP-botten for brugere inden for scope, så den kan sende dem advarsler i en 1:1-chat.
`TeamsAppInstallation.ReadWriteForTeam.All`	Microsoft Graph	Installation	Installerer botten i Teams, hvor kanaladvarsler er nødvendige.
`Exchange.ManageAsApp`	Office 365 Exchange Online	Administration	Opretter og vedligeholder de mailflowregler, der tilbageholder udgående e-mail til eksterne modtagere, indtil den er kontrolleret. Data & More administrerer kun sine egne regler.

Engangs-konfigurationstrin

Visse handlinger kan ikke tildeles som applikationstilladelser. De gennemføres én gang fra DLP-siden, mens De er logget ind som administrator.

Trin	Hvem logger ind	Hvad det tildeler
Giv Exchange-adgang	Exchange-administrator eller global administrator	Logger ind med den delegerede `Exchange.Manage`-tilladelse og registrerer Data & More i Exchange Online med to Exchange-roller: **Transport Rules** (administrer egne mailflowregler) og **View-Only Configuration** (læs Deres accepterede domæner, så intern mail ikke tilbageholdes).

Installer Teams-bot	Teams-administrator eller global administrator	Bruger den delegerede `AppCatalog.ReadWrite.All`-tilladelse én gang til at publicere Data & More DLP-botten i organisationens Teams-appkatalog.
Tillad sletning af Teams-beskeder (valgfrit)	Global administrator eller hver beskedforfatter	Microsoft tillader kun, at en Teams-besked slettes på vegne af dens forfatter. Godkendelse af den delegerede `ChannelMessage.ReadWrite`- og `Chat.ReadWrite`-tilladelse for organisationen giver DLP mulighed for at fjerne en blokeret besked uden at spørge hver forfatter.

Copilot DLP er udelukkende advarselsbaseret: Data & More kan notificere om en risikabel Copilot-samtale, men ændrer den ikke.

Mulighed 4: Tilføj appregistrering (Deres egen app)

Nogle organisationer foretrækker at oprette appregistreringen i deres egen tenant, så de ejer legitimationsoplysningerne og selv bestemmer, hvilke tilladelser der tildeles. Data & More bruger derefter den pågældende app i stedet for sin egen. Tildel kun det, de kilder og funktioner, De planlægger at bruge, kræver; tabellen sidst i dette afsnit angiver minimumet for hver enkelt.

1. Registrer appen

1. Log ind på **portal.azure.com** som global administrator.
2. Søg efter **App registrations** og vælg **New registration**.
3. Indtast et navn (f.eks. *Data & More DMCS*) og vælg **Accounts in this organizational directory only**.
4. Under **Redirect URI** vælger De **Web** og indtaster `https://signup.dataandmore.com/api/authorized`.
5. Vælg **Register**.
6. Åbn **Authentication** og tilføj to yderligere **Web**-omdirigerings-URI'er: `https://signup.dataandmore.com/api/authorize_redirect` og Deres Data & More-serveradresse efterfulgt af `/api/auth/ad/login/authorized`. Hvis Deres server er `https://gdpr.dataandmore.com`, er det `https://gdpr.dataandmore.com/api/auth/ad/login/authorized`. Vælg **Save**.

Tilføj altid begge `signup.dataandmore.com`-adresser, uanset hvilken pakke De bruger. De er nødvendige for samtykke- og login-trinene.

2. Tilføj API-tilladelser

1. Åbn **API permissions** og vælg **Add a permission → Microsoft Graph → Application permissions**. Tilføj Graph-tilladelserne for Deres pakke (Demo, Produktion eller Produktion + DLP ovenfor), eller det minimumssæt for de funktioner, De ønsker, fra tabellen nedenfor.
2. **SharePoint** (Produktion og Produktion + DLP): vælg **Add a permission** igen, åbn **APIs my organization uses**, søg efter **SharePoint**, og tilføj de tre SharePoint-applikationstilladelser.
3. **Exchange** (Produktion + DLP eller Online-arkiv): vælg **Add a permission → APIs my organization uses**, søg efter **Office 365 Exchange Online**, og tilføj `Exchange.ManageAsApp` (DLP) og/eller `full_access_as_app` (Online-arkiv).
4. Vælg **Grant admin consent** og bekræft. Alle tilladelser bør nu vise statussen grøn **Granted**.

3. Opret legitimationsoplysninger

1. På appens **Overview**-side noterer De **Application (client) ID** og **Directory (tenant) ID**.
2. Åbn **Certificates & secrets → New client secret**, tilføj en beskrivelse og en udløbsdato, og vælg **Add**.
3. Kopiér hemmeligheds-**værdien** med det samme. Den vises kun én gang, og De skal bruge værdien og ikke hemmeligheds-ID'et. Alternativt kan De uploade et certifikat; et certifikat er påkrævet for at læse SharePoint-sitegrupper og -ejere.

4. Tilslut den til Data & More

1. Åbn **Indstillinger → Appregistrering → Tilføj appregistrering** i Data & More, og indtast tenant-ID, klient-ID samt hemmeligheds-værdien eller certifikatet. Hvis De ikke selv kan gøre dette, skal De sende de tre værdier til **support@dataandmore.com** via en sikker kanal.
2. Vælg **Kontroller tilladelser**. Data & More viser, hvilke tilladelser der er fundet, markerer eventuelle manglende tilladelser og angiver, hvornår hemmeligheden eller certifikatet udløber.

Minimumstilladelser pr. funktion

Funktion	Scanning (læsning)	Politikhandlinger (skrivning)
Altid nødvendig	`User.Read.All`, `GroupMember.Read.All`, `Organization.Read.All`, `Application.Read.All`	Ingen
Outlook	`Mail.Read`, `MailboxSettings.Read`	`Mail.ReadWrite`, `MailboxSettings.ReadWrite`
Exchange Online-arkiv	Exchange: `full_access_as_app`	Exchange: `full_access_as_app`
OneDrive	`Files.Read.All`	`Files.ReadWrite.All`, `Sites.ReadWrite.All`, `Sites.Manage.All`
SharePoint	`Sites.Read.All`, `Files.Read.All`; SharePoint: `Sites.Read.All` (certifikat)	`Files.ReadWrite.All`, `Sites.ReadWrite.All`, `Sites.Manage.All`
Teams-kanaler	`Channel.ReadBasic.All`, `ChannelMessage.Read.All`, `Files.Read.All`	`Files.ReadWrite.All`
Teams-chats	`Chat.Read.All`	Ingen
Kendte personer	`Contacts.Read`	Ingen
Følsomhedsmærkater	`InformationProtectionPolicy.Read.All`	`Files.ReadWrite.All` (til anvendelse)
Rapporter via e-mail	Ingen	`Mail.Send`
Copilot	`AiEnterpriseInteraction.Read.All`, `AuditLogsQuery.Read.All`	Ingen
Forebyggelse af datatab i realtid	Scanningtilladelserne for hver kilde, De beskytter	Exchange: `Exchange.ManageAsApp`; Graph: `Mail.ReadWrite`, `Mail.Send`, `Files.ReadWrite.All`, `AppCatalog.Read.All`, `TeamsAppInstallation.ReadWriteSelfForUser.All`, `TeamsAppInstallation.ReadWriteSelfForTeam.All`; samt de engangs-trin under Produktion + DLP

> **Vær opmærksom på:** De er ansvarlige for at forny hemmeligheden eller certifikatet, inden det udløber; visningen **Kontroller tilladelser** viser udløbsdatoen. Hvis en tilladelse mangler, viser den relaterede kilde en adgangsfejl i stedet for at fejle uden besked. Tilføj tilladelsen, giv administratorsamtykke igen, og kør **Kontroller tilladelser**.

Begræns, hvad Data & More kan tilgå

Applikationstilladelser gælder for hele tenanten. Hvis De ønsker at indsnævre dem, tilbyder Microsoft følgende kontrolmuligheder, og Data & More fungerer med dem alle:

- **Afgrænsning i Data & More.** Vælg, hvilke brugere, grupper, sites og Teams hver kilde dækker. Intet uden for afgrænsningen scannes eller ændres.
- **Exchange-applikationsadgangspolitik eller RBAC for applikationer.** Begræns `Mail.Send` og postkasseadgang til en mailaktiveret sikkerhedsgruppe.

- **Revision.** Hvert kald, Data & More foretager, vises i Deres Entra-loginlogge og Microsoft 365-revisionsloggen under appens navn.

Hyppige spørgsmål

Kan Data & More læse mine brugeres adgangskoder?

Nej. Ingen af disse tilladelser giver adgang til adgangskoder eller loginoplysninger. Data & More autentificerer som sin egen app med sin egen hemmelighed eller sit eget certifikat.

Hvorfor har et primært læseprodukt brug for skrivetilladelser?

Skriveadgang bruges kun, når en politík, De har konfigureret, beder Data & More om at handle, f.eks. for at flytte en følsom fil til en vault eller slette e-mail efter udløbet opbevaringsperiode. Sletninger gennemgår desuden et godkendelsestrin med menneskelig kontrol. Hvis De kun ønsker rapporter, skal De vælge Demo eller udelukkende tildele læsetilladelser i Deres egen app.

Kan vi starte med Demo og opgradere senere?

Ja. Vælg **Produktion** eller **Produktion + DLP** under **Indstillinger → Appregistrering** og godkend igen. Eksisterende scanningsresultater bevares.

Hvad sker der, hvis vi fjerner en tilladelse?

De funktioner, der er afhængige af den, ophører, og de berørte kilder viser en adgangsfejl. Alt andet fortsætter med at fungere. Kør **Kontroller tilladelser** for at se, hvad der mangler.

Bruger Data & More delegerede (tillogget bruger) tilladelser?

Ingen af de tre pakker indeholder delegerede tilladelser, ikke engang `User.Read`. Delegerede tilladelser bruges kun til engangs-DLP-trinene, til personlige konti (hvor en bruger tilslutter sin egen postkasse og OneDrive) samt til sletning af Teams-beskeder, som Microsoft kun tillader på vegne af forfatteren.

Jeg har mistet klienthemmeligheden. Kan jeg se den igen?

Nej. Microsoft viser en klienthemmelighedsværdi kun én gang, umiddelbart efter den er oprettet. Opret en ny hemmelighed, opdater den under **Indstillinger → Appregistrering**, og slet den gamle.
