Microsoft 365 Copilot from an administrator perspective

Kent Agerlund & Morten Nilsen
Security principals @ twoday in Denmark, Finland & Norway

twoday

Morten Bøtkjær Nilsen

Principal consultant
morten.b.nilsen@twoday.com

- Worked with IT since 2008
- Primarily focused on AI, security, compliance and device management within Microsoft products
- Scandinavia with a focus on Denmark, Finland & Norway

Kent Agerlund

Principal consultant
kent.agerlund@twoday.com

- Consultant since 1991
- Primarily focused on AI, modern work including device management, security and compliance solutions within Microsoft products.
- Scandinavia with a focus on Denmark, Finland & Norway

twoday

You get a Copilot! You get a Copilot!

Microsoft 365 Chat

- Included in the Microsoft 365 license
- Provides access to Chat based on GPT-4o
- Access to the use of agents (usage-ba
- Data is protected via Enterprise Data Protection (EDP)

Microsoft 365 Copilot

- Includes all Chat features
- Personal assistant in Microsoft 365 applications
- Requires a separate license per user

● Included ▲ Included — Metered

		Microsoft 365 Copilot Chat Free + Consumption	Microsoft 365 Copilot $30 pupm
Chat	Copilot Chat – Web grounded (powered by GPT-4o)	●	●
	Copilot Chat – Work grounded (work data in your tenant's Microsoft Graph and 3rd party data via Graph connectors)		●
	Copilot Pages	●	●
	File upload[1]	●	●
	Code Interpreter[1]	●	●
	Image generation[1]	●	●
Agents[2]	Create agents using Copilot Studio[3], including SharePoint agents	●	●
	Discover and pin agents	●	●
	Use agents grounded in Web data	●	●
	Use agents grounded in work data (work data in your tenant's Microsoft Graph and 3rd party data via Graph connectors)	▲	●
	Use agents that act independently using autonomous actions	▲	▲
Personal assistant	Copilot reasons over personal work data (e.g. Outlook, OneDrive, meeting transcripts)		●
	Copilot in Teams		●
	Copilot in Outlook		●
	Copilot in Word		●
	Copilot in Excel		●
	Copilot in PowerPoint		●
	Copilot Actions		In preview
	Pre-built M365 agents (Interpreter, Facilitator, Project Manager, Employee Self-Service)		In preview
Copilot Control System	Enterprise Data Protection (EDP)	●	●
	IT management controls	●	●
	Agent management	●	●
	SharePoint Advanced Management		●
	Copilot Analytics to measure usage and adoption[4]		●
	Pre-built reports and advanced analytics to measure ROI		●

1. Limits apply. 2. Applies to employee-facing agents only. 3. Learn more about the full capabilities of Copilot Studio: aka.ms/CopilotStudioCapabilities 4. Basic reporting in Microsoft Admin Center available for Copilot Chat.

The technical challenges

What is your own perception of reality?

twoday

Securing and governing Microsoft 365 Copilot

Baseline

Microsoft 365 Copilot
+ Office 365 E3

Multi-factor authentication

Audit logging

Core

Microsoft 365 Copilot
+ Microsoft 365 E3
+ SharePoint Advanced Management

Conditional Access

Manual sensitivity labels

Data loss prevention policies

Advanced SharePoint sitewide access controls and reporting

Unified endpoint management

Best-in-class

Microsoft 365 Copilot
+ Microsoft 365 E5
+ SharePoint Advanced Management

Conditional Access based on identity risk

Automatically apply sensitivity labels

Automatically remove inactive content

Prevent data leak on endpoint devices

Detect non-compliant usage

twoday

But first you need to pass this guy

Datatilsynet

Mitä

Hiekkalaatikko-sivu / Valmiit projektit ja raportit

NTNU, loppuraportti: Copilot yksityisyyslasit päässä

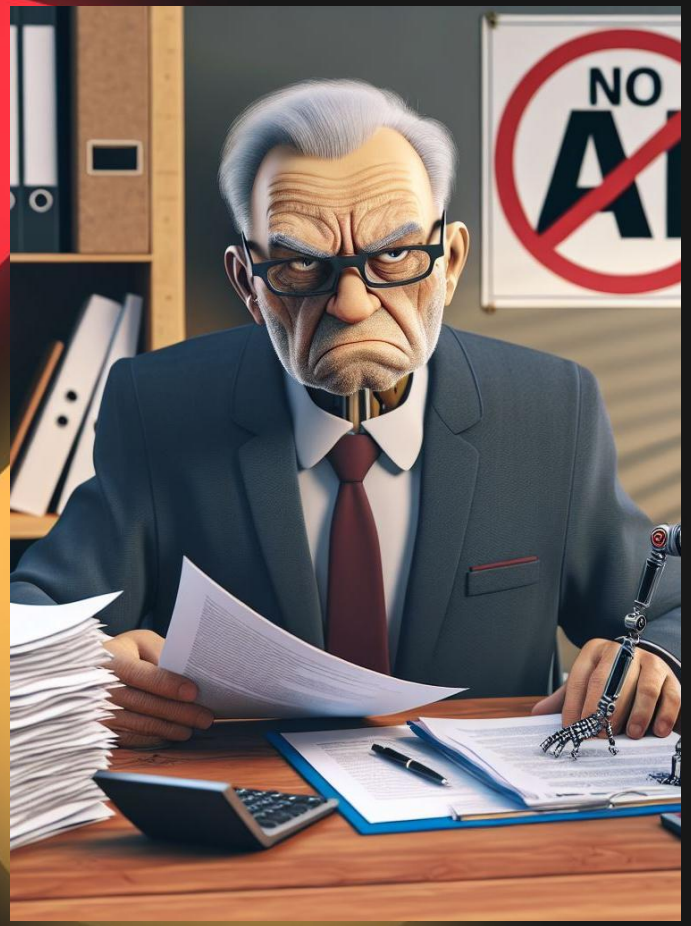
Generatiivinen tekoäly (AI) ei ole enää vain hauska työkalu, vaan sitä ollaan nyt integroimassa jo käyttämiimme digitaalisiin ratkaisuihin. Microsoft lanseerasi Copilot for Office -ohjelmistopakettinsa marraskuussa 2023, joka voi yksinkertaistaa jokapäiväistä työtä huomattavasti. Jotkut ovat käyttäneet sitä kokonaan tai osittain. Monet istuvat aidalla. Koska mitä todella tapahtuu, kun otat Microsoft 365 Copilotin käyttöön?

Sisältö

1. Yhteenveto
2. Tietoa hankkeesta
3. Rajaaminen

Yhteenveto

Norjan tietosuojaviranomainen ja NTNU ovat tarkastelleet sovellettavia tietosuojavaatimuksia ja sitä, mitä arvioita NTNU:n tulisi tehdä ennen Microsoftin tekoälyavustajan käyttöä. Samanaikaisesti NTNU toteutti pilottiprojektin, jossa selvitettiin, ovatko he valmiita ottamaan käyttöön M365



Source: NTNU, loppuraportti: Copilot yksityisyyslasit päässä | Norjantietosuojaviranomainen

twoday

Baseline

Required licenses:
Office 365 E3 or higher

Follow the recommended **baseline activities** to proceed with Microsoft 365 Copilot deployment.

Product	Deployment outcomes	Get started activities
Microsoft 365 Copilot	Evaluate data governance maturity and data security controls	• Complete Microsoft 365 Copilot Optimization Assessment • Based on the outcomes of the assessment determine your path forward
	Deploy Microsoft 365 Copilot	• Follow the Microsoft 365 Microsoft Copilot setup guide to proceed with the deployment steps • If there are any concerns about your data security, enable Restricted SharePoint Search • If enabled, update Restricted SharePoint Search allow list: configure up to 100 sites to be on the allow list of sites. Start with sites containing highly used unrestricted content. • Also check Updated Windows and Microsoft 365 Copilot Chat experience | Microsoft Learn
Copilot with commercial data protection	Enable commercial data protection in Copilot for all users in your organization	• Log into Copilot on copilot.microsoft.com and flip the Work/Web toggle to Web. See if commercial data protection is enabled (look for green Protected pill by the user profile) • Review the Copilot with commercial data protection documentation to ensure that commercial data protection is available for your users

PowerShell Copy

```powershell
# Get the package full name of the Copilot app
$packageFullName = Get-AppxPackage -Name "Microsoft.Copilot" | Select-Object -ExpandProperty PackageF
# Remove the Copilot app
Remove-AppxPackage -Package $packageFullName
```

*Note: Eligible customers can request technical and deployment assistance from Microsoft FastTrack

twoday

Baseline

Required licenses:

Office 365 E3, Microsoft 365 Business Standard/Premium, or higher; and SPP-SharePoint Advanced Management

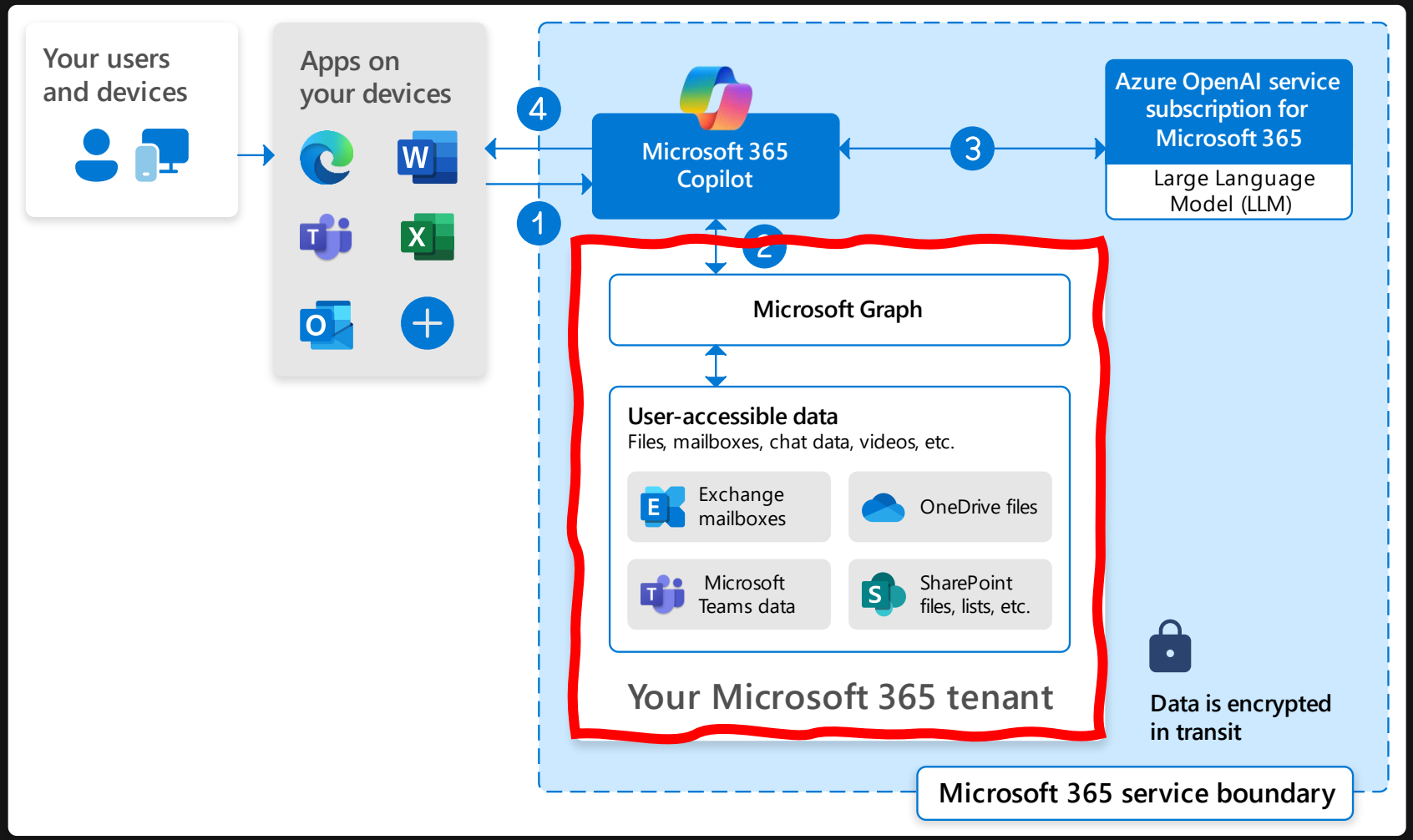
Product	Deployment outcomes	Core activities
Microsoft 365 Copilot	If enabled, update Restricted SharePoint Search allow list	Configure up to 100 sites to be on the allow list of sites. Extend to sites containing highly used, low risk content
Microsoft SharePoint*	Evaluate sharing controls that govern who can share and how broadly	At the tenant level: • Update sharing link defaults from organization-wide sharing to specific people links. • Consider hiding "Everyone Except External Users" in the People Picker control to reduce risks around accidental misuse. Consider educating site admins on the site-level controls they can use to restrict sharing: • Set the default sharing link type on specific sites • Set sharing link expiration on anyone links • Set site owner sharing approval on sensitive sites • Ask OneDrive for Business (ODB) owners to run sharing reports in their ODB and correct as needed • Ask site owners to manually review SharePoint site permissions and correct as needed
Microsoft SharePoint Advanced Management	Clean up unused sites	• Implement Inactive Site Policy in Simulation mode • Then Activate to take actions like: Site Owner attestation, make read-only, move to Microsoft 365 Archive
	Identify sites with potentially overshared content, then take action to control access to that content	• Run Data Access Governance (DAG) reports • Apply Restricted Access Control on sites based on DAG reports • Initiate Site Access Reviews for sites with potentially overshared content
	Take proactive measures on business-critical sites	• Apply Restricted Access Control policy to proactively protect against oversharing • Apply a BlockDownloadPolicy on sensitive sites or for Teams Meeting Recordings
Microsoft Purview	Gain visibility into how users are interacting with data in the organization and with Microsoft 365 Copilot	• Confirm that Microsoft Purview Audit is enabled, if not enable it
	Enable citations and protections for sensitive data access by Microsoft 365 Copilot	Manually Label emails and documents with out-of-the-box sensitivity labels using one-click or previously created policies
	Protect sensitive information from being shared beyond its intended audience and reduce the risk of oversharing	Create and deploy Data Loss Prevention (DLP) policies for SharePoint, Exchange, and OneDrive for Business
	Retain the data you need to keep and remove data that no longer has business value to reduce data surface for oversharing	Create and Configure retention policies to archive or delete content exceeding data retention guidelines or maximum retention date
	Gain additional understanding of content used and shared in Copilot interactions	Use Microsoft Purview eDiscovery Content search to find email in search for in email, documents, and instant messaging conversations

Best in class

Required licenses:
Microsoft 365 E5; and SPP-SharePoint Advanced Management

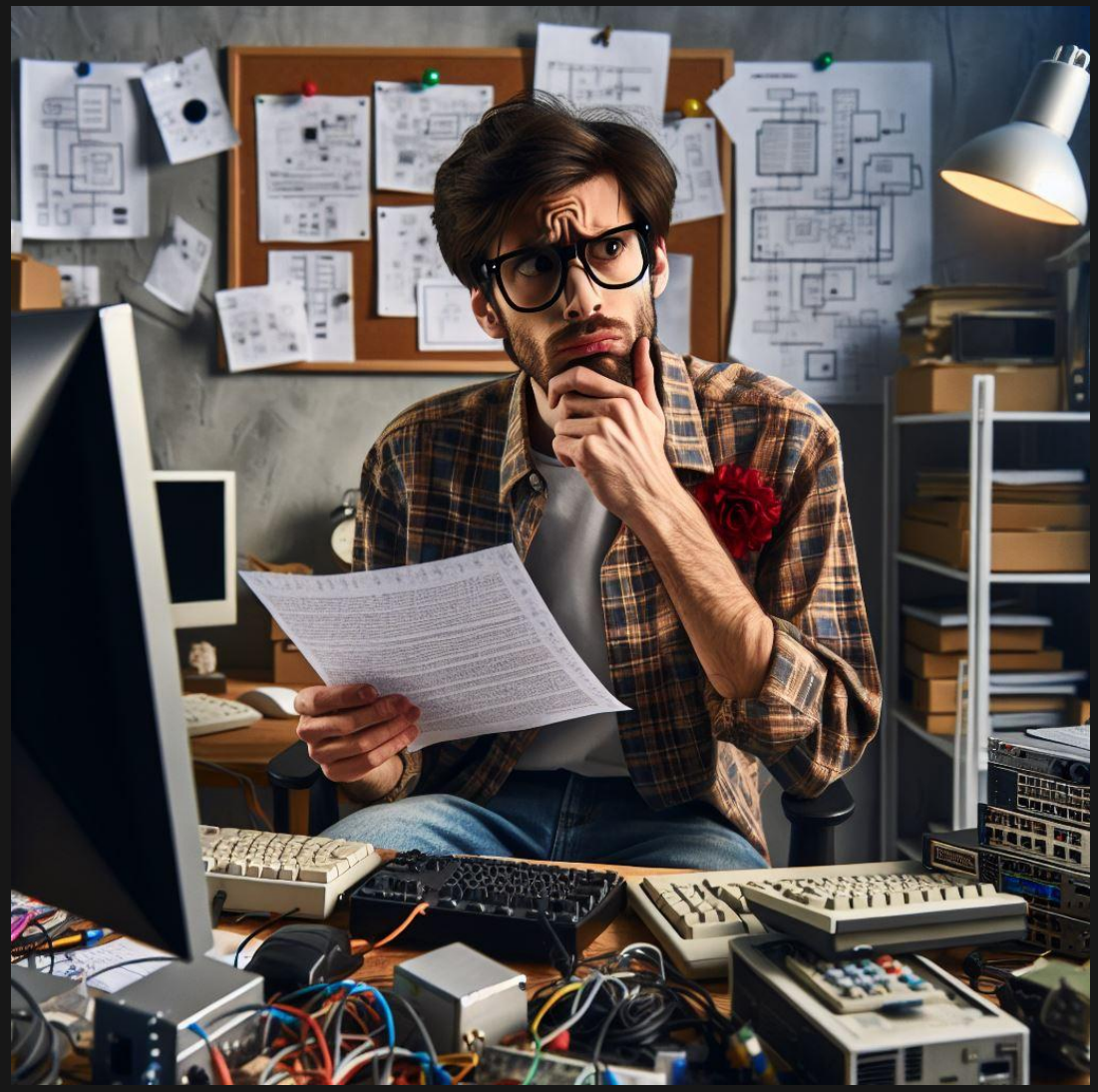
Product	Deployment outcomes	Best-in-Class activities
Microsoft 365 Copilot	If enabled, update Restricted SharePoint Search allow list	• Configure up to 100 sites to be on the allow list of sites. Extend to sites containing restricted content, after validating permissions are set correctly
	Disable Restricted SharePoint Search to allow full Copilot experience	Once all the data security concerns are addressed, disable Restricted SharePoint Search
Microsoft SharePoint Advanced Management	Perform periodic reviews of oversharing reports, initiating Site Access Reviews and restricting access as appropriate	Run DAG reports on a periodic basis. Apply RAC policies and initiate Site Access Reviews for sites that contain potentially overshared content.
	Perform periodic reviews of inactive sites, and take action	Apply inactive sites policy with optional actions configured.
	Perform periodic reviews of Change History reports to discover when oversharing occurs	Run the change history report and investigate changes to sharing in sites.
Microsoft Purview	Apply a baseline protection to documents and containers (Microsoft 365 Groups, Microsoft Teams Sites) without the need for content inspection or manual labeling	• Set a default sensitivity label on SharePoint Online document libraries to protect documents without content inspection • Use Sensitivity labels to protect content in Teams, Groups and SharePoint sites
	Dynamically protect sensitive information from being shared beyond its intended audience and reduce the risk of oversharing on across instant messages and user endpoints.	• Create, deploy, and regularly evaluate Teams DLP Policies • Create, deploy, and regularly evaluate Endpoint DLP Policies • Create Adaptative Protection policies to automatically assign DLP policies based on the users identified risk level
	Automatically protect sensitive data access by Microsoft 365 Copilot for based on recommended conditions.	• Automatically apply sensitivity labels to content in SharePoint, OneDrive, and Exchange • Automatically apply sensitivity labels to content within Office apps
	Automatically retain or dispose of documents based on their content	Automatically apply retention labels to content that match specific conditions
	Detect sensitive data and non-compliant content in Copilot interactions	Create Communication Compliance policies to regularly evaluate interactions with Microsoft 365 Copilot
	Preserve, collect, review, analyze, and export Copilot interactions	Use eDiscovery Premium to search for and optionally delete Copilot interactions

Without governance in line, Copilot won't shine!



twoday

So where do we start?



twoday

Congratulations, you are still breathing !

twoday