M365 i skolen – personvern og infosikkerhet

brr.no/wordpressbrr/nasjonal-dpia-for-microsoft-365

Bjørn Roger Rasmussen 08.03.2025

(Sist oppdatert 05.09.2025 @ 17:19 av Bjørn Roger Rasmussen.)

I starten av 2025 valgte jeg å engasjere meg innenfor KS-prosjektet **«Nasjonal DPIA for Microsoft 365»**. Som det står å lese på KS sin nettside: «*KS starter arbeidet med å gjennomføre en nasjonal vurdering av personvernkonsekvenser (DPIA) for Microsoft 365 etter modell fra DPIAen for bruk av Google Workspace for Education i skolen.*» Min plass var i en liten arbeidsgruppe som jobbet med **tenant-problematikken**. Dette var på mange måter et forprosjekt forut for selve DPIA-biten.

Microsoft 365 og Teams, hvor Teams er navet i løsningen.

Selv er jeg ikke spesifikt interessert i skole, men jeg satset på at DPIA-en kunne gi store overføringsverdier til andre deler av den kommunale virksomheten. Jeg engasjerte meg opprinnelig i prosjektet fordi det omhandler reelle problemstillinger som er relevante for Kinn kommune, min arbeidsplass.

Det ~~blir~~ kunne blitt interessant å få være med i dette arbeidet innenfor personvern knyttet opp mot den amerikanske «big tech»-leverandøren Microsoft, i grensegangen mot skole og kommune!

Snipp, snapp, snute – etter ca. 5 måneder som prosjektmedarbeider var jeg ute. Jeg har blitt «fristilt» fra prosjektet, mot min vilje (sommeren 2025). Min framdrift, kompetanse og innsats i prosjektet ble tydeligvis ikke verdsatt.

Jeg har endelig gjennomført **endring av tittel** på innlegget! Gammel tittel: «**Nasjonal DPIA for Microsoft 365**«. Ny tittel, som er mye mer dekkende for dagens situasjon og skriverier: «**M365 i skolen – personvern og informasjonssikkerhet**«. (Informasjonssikkerhet forkortet til infosikkerhet for å unngå for lang tittel, jf. SEO-anbefalinger.) Imidlertid består det gamle filnavnet på innlegget (nasjonal-dpia-for-microsoft-365).

Direkte lenke til dette innlegget: https://www.brr.no/wordpressbrr/nasjonal-dpia-for-microsoft-365/

Innledning

Jeg har valgt å **skrive litt** om det jeg har lært om **tenant-inndelinger og utfordringer** (tenant-problematikk) **knyttet til Microsoft 365 i skole**– og kommunesektoren, inkludert et generelt fokus på **personvern og informasjonssikkerhet**. Dette arbeidet er gjort på **eget initiativ og i personlig regi**, og er ikke en del av det offisielle nasjonale KS-prosjektet, da jeg ikke lenger er tilknyttet dette. Noen av tekstene jeg bidro med i fellesprosjektet har jeg delvis, i noe modifisert form, tatt med her i innlegget.

Microsoft 365/Office 365-logoer benyttet av Microsoft i senere år. Nå er det vel mest bruk av M365 Copilot-logoen.

Etter å ha vært dypt fordypet i prosjektets problemstillinger, kjente jeg et behov for å 'skrive meg tom' for å rydde i tankene. Mitt mål er ikke å konkurrere med det nasjonale prosjektet, men å bidra konstruktivt til å belyse sentrale problemstillinger sett fra mitt personlige perspektiv.

Innholdet er altså i stor grad utarbeidet uavhengig fra det nasjonale prosjektet, og jeg har i **noen tilfeller benyttet kunstig intelligens (KI/AI) – nærmere bestemt Microsoft 365 Copilot** (https://copilot.microsoft.cloud/) – som støtte i skriveprosessen. All tekst er naturligvis manuelt og menneskelig kvalitetssikret før publisering.

For å være helt åpen og transparent om min (begrensede) bruk av KI; Generativ kunstig intelligens (stor språkmodell) i form av Microsoft 365 Copilot har blitt brukt til:

- **Språklig forbedring og språkvask** (i liten grad direkte generering av innhold)
- **Innhenting av bakgrunnsinformasjon** i idéfasen (idédugnad og utvikling)

Språket kan til tider bære preg av **KI-generering** («KI-språk»), men hovedfokuset har vært på å formidle innholdet tydelig og faglig korrekt uten å henge seg opp i språklige spissfindigheter.

I og med at jeg «innrømmer» en viss KI-bruk spurte jeg KI til råds: Microsoft 365 Copilot KI sine «tanker» rundt bruken av Microsoft 365 (M365) innenfor norsk skole (PDF-fil). Fornuftig og bra svart så langt jeg kan vurdere det.

> ## Hvem er jeg?
>
> - Navn: Bjørn Roger Rasmussen
> - Født: 1971
> - Utdannelse: 6-årlig høgskoleutdannelse på hovedfagsnivå (mastergrad-nivå) innenfor informasjonssystemer, inkludert pedagogikk / pedagogisk utdannelse for å eventuelt kunne jobbe som lektor (lærer) i den videregående skolen
> - Nåværende jobb: IKT-rådgiver og personvernrådgiver i Kinn kommune (Måløy, Vestland fylke)
> - Erfaring: Lang og bred erfaring innen IKT i kommunal sektor – over 25 år (per 2025)
> - Mer informasjon: Om bloggen (og meg) + min CV

Innlegget hadde **opprinnelig tittelen «Nasjonal DPIA for Microsoft 365»**, ettersom planen var å dele **lærdommer og erfaringer fra deltakelsen i prosjektet**. Etter at jeg nå er **satt på sidelinjen** i det nasjonale prosjektarbeidet, har jeg **endret tittelen til en mer generell variant: «M365 i skolen – personvern og informasjonssikkerhet»**. En alternativ (men altfor lang) tittel kunne vært: «Mine tanker og vurderinger rundt oppsett av Microsoft 365-tenanter – og litt generelt om personvern og informasjonssikkerhet – i kommunal sektor, med særlig fokus på skole». Siden jeg ikke lenger deltar i prosjektet, vil innlegget ikke ha hovedfokus på DPIA-delen i KS/SkoleSec-arbeidet.»

> Kort om innholdet: Jeg deler noen generelle betraktninger om informasjonssikkerhet og personvern, samt refleksjoner rundt behandlingsprotokoller, risikovurderinger (ROS) og personvernkonsekvensvurderinger (DPIA) – sett fra mitt personlige ståsted. Til slutt presenterer jeg noen antakelser om den videre utviklingen av det nasjonale DPIA-prosjektet til KS, som jeg ikke lenger deltar i.
>
> Kort oppsummert: Tanker og refleksjoner om personvern, informasjonssikkerhet og tenant-problematikk ved bruk av Microsoft 365 i skole og kommunal sektor.

Vinklingen har jeg prøvd å holde på et **ikke-teknisk nivå**. Det er mer en teoretisk drøftelse av ulike alternative valg som eventuelt kan foretas av beslutningstakere.

Introduksjon til tematikken

– Personvern og informasjonssikkerhet i møte med Microsoft 365 i skolen (og kommunal sektor)

Dette innlegget inneholder refleksjoner og vurderinger knyttet til **bruk av Microsoft 365 i skolesektoren**, med særlig fokus på **personvern** (GDPR), **informasjonssikkerhet**, **tenant-oppsett, behandlingsprotokoller, ROS-vurderinger** og **DPIA**. Målet er å gi en praktisk og forståelig fremstilling av sentrale problemstillinger som kommuner og skoler står overfor når digitale verktøy skal tas i bruk på en trygg og ansvarlig måte. Innlegget kombinerer generell informasjon med egne erfaringer fra arbeid med disse temaene i kommunal sektor.

Innleggets stikkordsmessige innhold:

- **Innledning**, og min **tilnærming** kontra KS sin.
- Kort om **Microsoft 365-løsningen og lisensiering**.
- Litt om (antatt) **IKT-status i skolene**.
- Forklaring av tenant, tenant-inndeling og **tenant-problematikken**.
- Generelt om **informasjonssikkerhet og personvern** (GDPR).
- **Mer om tenant-problemstillingen**, sett i lys av personvern og informasjonssikkerhet.
- **Fordeler og ulemper** med å samle alt i en **felles tenant**.
- Noen aktuelle **sikringstiltak**.
- Hva som (sannsynligvis) **inngår og ikke inngår i det nasjonale DPIA-prosjektet**, etter den kjennskap jeg fikk til saken.
- Teoretisk tilnærming til **behandlingsprotokoller**, **risikovurdering (ROS)**, **personvernkonsekvensvurdering (DPIA)**, hvor tidligere foretatt tenant-valg vil påvirke analysene.
- **Anbefalinger til skoleeier** på tenant- og personvernområdet
- Litt om **min ufrivillige uttreden fra det nasjonale KS DPIA-prosjektet**.
- **Avsluttende kommentarer** og noen utvalgte **lenker**.

Utgangspunktet er delvis den lærdommen jeg tilegnet meg gjennom det nasjonale prosjektet, supplert med erfaringer og kunnskap fra min daglige jobb, der jeg også har ansvar som personvernrådgiver.

Hovedfokuset i innlegget er tenant-problematikken, som fungerer som en rød tråd. Selv om enkelte digresjoner forekommer, er alt relatert til personvern og informasjonssikkerhet for skole og kommune som benytter M365.

Microsoft 365

Hva slags produkt er det snakk om:

Hva er Microsoft 365 (M365)?

Microsoft 365 er en abonnementstjeneste fra Microsoft som gir tilgang til en samling digitale produktivitetsverktøy og tjenester — både som skybaserte løsninger og som apper for lokal installasjon.

Pakken inkluderer blant annet:

- Office-apper/applikasjoner som Word, Excel, PowerPoint og Outlook.
- Skylagring via OneDrive og SharePoint for sikker lagring og deling av filer — både individuelt og i samarbeid med andre.
- Og i større og større grad: Kunstig intelligens (KI) i form av Microsoft 365 Copilot integreres stadig mer som et intelligent tillegg i applikasjonene.
- Samarbeidsverktøy som Teams for chat, videomøter og samhandling.
- Sikkerhet og administrasjon for både privatpersoner, organisasjoner og virksomheter (bedrifter).

Tjenestene oppdateres fortløpende (automatisk), og funksjonaliteten er tilgjengelige på/via ulike enheter. Microsoft 365 tilbyr digitale verktøy som kan brukes både privat, innenfor skole og i arbeidssammenheng.

Microsoft 365 (M365) er tilgjengelig (helt eller delvis) på flere ulike operativsystemer og plattformer: Windows, macOS, iOS, ChromeOS og Android. I tillegg kan tjenestene benyttes via nettleser (web) på enhver enhet med internettforbindelse.

Skytjenestene leveres via Microsoft sin Azure-plattform, som står for den tekniske infrastrukturen bak identitetshåndtering, datalagring, sikkerhet og integrasjon.

I kommunal- og fylkeskommunal sektor — både i administrasjon, tjenesteyting og spesielt innen skole (grunnskole og videregående) — er Microsoft 365 i utstrakt bruk. I skolen benyttes tjenestene med en (forhåpentligvis) pedagogisk og personvernvennlig tilnærming.

Microsoft 365 er en omfattende og vid plattform som ofte fungerer som et av de sentrale IKT-hovedsystemene i skolen. Løsningen tilbyr tjenester for kommunikasjon, samarbeid, dokumenthåndtering og læringsstøtte. Bruken innebærer **behandling av store mengder data, inkludert personopplysninger** om elever og ansatte, noe som stiller **høye krav til informasjonssikkerhet og personvern**. Tjenester og data – også innenfor M365-sfæren – håndteres i stadig større grad i **skyen** fremfor lokalt.

Lisenser og abonnement

A-lisenser (abonnementer) er rettet mot – og tilpasset – skole og utdanning (inkluderer noen pedagogiske verktøyer), mens E-lisenser er rettet mot administrativ eller kommersiell bruk i virksomheter. A3/E3 har mindre med sikkerhetsfunksjonalitet «innebygget» enn A5/E5.

Mer om lisensnivåer for spesielt interesserte:

4.1.2 Lisensiering og sikkerhetsfunksjonalitet i Microsoft 365

Lisensieringsnivået i Microsoft 365 har betydning for hvilke sikkerhetsfunksjoner og muligheter som er tilgjengelige for å sikre oppsettet – spesielt når det gjelder datasegregering og kontrollert samhandling. Nedenfor følger en oversikt over relevante lisensnivåer M365 (A/E)[15], og eventuelle behov for tilleggsmoduler:

- **Høyeste lisensnivå – A5/E5:** *Information Barriers v2* er inkludert som standard. Dette gir avansert støtte for segmentering av brukere og kontrollert kommunikasjon, og er godt egnet for miljøer med behov for strenge skiller mellom brukergrupper. For enkelte organisasjoner kan det være aktuelt å oppgradere til dette nivået ut fra andre hensyn og vurderinger (ønsket funksjonalitet) enn «bare» ut fra det som har med tenant-problematikken og sikkerheten å gjøre.
- **Middels lisensnivå – A3/E3:** *Information Barriers* er ikke inkludert som standard, men kan aktiveres ved å kjøpe tillegget *Microsoft 365 E5 Compliance* (også kjent som *Microsoft Purview Compliance*). Dette gir tilgang til *Information Barriers v2*. Selv uten tilleggsprodukter kan en slik installasjon i en viss grad beskyttes via enklere former for adresseboksegrering, tilgangsstyring, segmentering av brukere og begrensninger i hvem man kan kommunisere med via Teams og e-post, men funksjonaliteten er ikke så sostifikert som for høyere lisensnivåer og/eller via tilleggsprodukter.
- **Lavt lisensnivå – A1/E1:** Disse lisensene kan også suppleres med *Microsoft 365 E5 Compliance*-tillegg, for å få tilgang på *Information Barriers*. For en god del brukere vil denne pakken være for begrenset til å dekke behovene i skole- og arbeidshverdagen. M365-pakken gir f.eks. ikke tilgang på skrivebords-utgavene av Office-appene (kun tilgang på web-/mobilversjoner).
- **Lavest lisensnivå – F1/F3:** F-lisenser er også et valg, som er lisenser som passer til «Frontline Worker»-ansatte (frontlinje-ansatte). Typisk i bruk innenfor f.eks. helse/pleie- og omsorg, på vaktrom eller andre steder hvor de ansatte ikke jobber ved en datamaskin hele dagen. Lisensnivået er neppe særlig relevant eller aktuelt for skole.

Desto høyere lisensnivå, jo større og mer funksjonalitet er inkludert som standard. Høyere lisensnivåer gir også tilgang på større lagringskvoter i forbindelse med skylagringen.

[15] Microsoft 365-lisenser med prefiks A (f.eks. A1, A3, A5) er rettet mot utdanningssektoren og skoler, mens lisenser med prefiks E (f.eks. E1, E3, E5 + F1/F3) er beregnet for kommersiell bruk i virksomheter og offentlige organisasjoner. Funksjonaliteten er i stor grad lik, men det kan være forskjeller i tilgjengelighet, pris og lisensvilkår, særlig når det gjelder tilleggstjenester som Microsoft Purview Compliance. Generelt gir et høyere lisensnivå mer funksjonalitet – men også en høyere månedlig abonnements-/lisenskostnad.

M365 lisensnivåer, hentet fra de forkastede skriveriene foretatt av meg innenfor det nasjonale DPIA-prosjektet.

De gammeldagse, evigvarende lisensene er tilnærmet historie. I dag **bygger Microsoft 365 på en abonnementsmodell**, der tjenester og programvare leveres som en del av et månedlig eller årlig abonnement. Dette gir økt fleksibilitet, kontinuerlige oppdateringer og enklere budsjettering for virksomheter og organisasjoner. I stedet for å kjøpe en lisens én gang og måtte oppgradere manuelt ved behov, får man nå tilgang til de nyeste funksjonene og sikkerhetstiltakene automatisk, så lenge abonnementet er aktivt.

Litt Microsoft-kritikk: Muligens minner vår **Microsoft-avhengighet** mest om et **ufrivillig tvangsekteskap**. Vi har gjort oss helt avhengige av Windows og Microsoft 365 (Microsoft sitt økosystem), og det finnes få gode og reelle alternativer som dekker fullt ut funksjonaliteten som ligger i Microsoft-produktene. (F. eks. å gå over til Google Workspace vil ikke gjøre tingenes tilstand noe særlig mye bedre!) Microsoft vet også å utnytte deres (nesten) monopolstilling, gjennom at prisene på abonnementer og lisenser hele tiden er sterkt økende langt utover normal prisstigning.

Status i skolen

Den harde sannhet i deler av skoleverket ut fra det vi kan lese via media og nettet:

Barnas personvern innenfor skole er til tider under stort press på grunn av den utstrakte digitaliseringen og den digitale transformasjonen innenfor kommunal sektor. Ukritisk innføring av nye digitale læringsverktøy går / kan gå på bekostning av personvernet til elevene. Det er ofte **mangel på grundige vurderinger og mangelfull kompetanse** til å gjøre gode vurderinger av personvernet og personvernkonsekvensene, noe som kan føre til ukritisk og ikke-ønsket **innsamling av personopplysninger for kommersielle formål og reklame**.

De harde realitetene i enkelte tilfeller: Skolene tar i bruk **flotte gratis-apper** (programmer), der skoleelever i praksis **betaler for bruken med sine personopplysninger** som valuta eller betalingsmiddel.

Målet bør være å sikre barns læring uten å kompromittere deres personvern. Barnas personvern bør og må ikke gå på billigsalg i iveren etter å innføre digitale verktøy i skolen, pga. dårlig gjennomtenkte innføringer av digital teknologi. Barn og elevers personopplysninger skal ikke være en handelsvare.

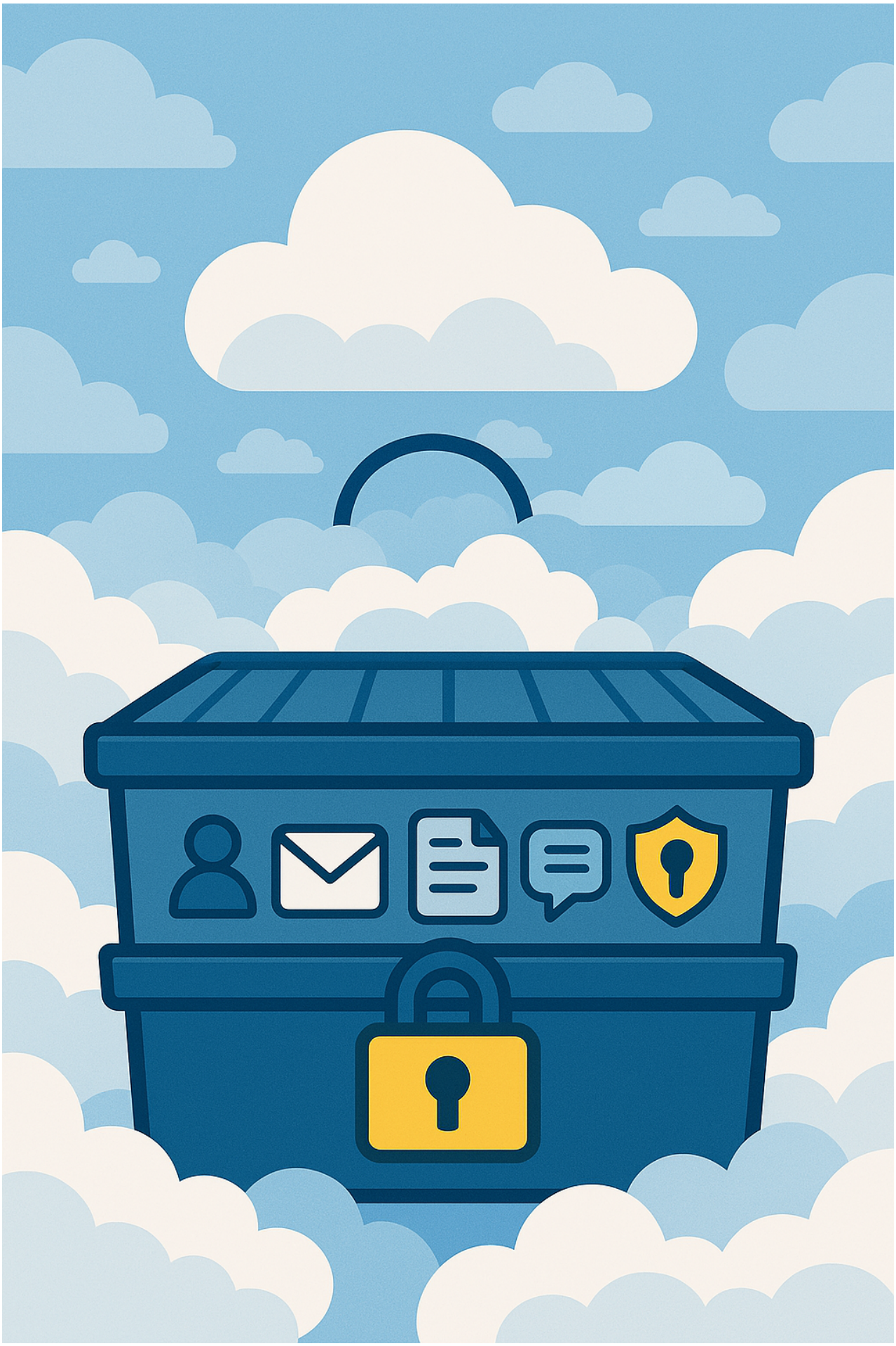
Når det gjelder bruken av M365 i skole har KS foretatt en kartlegging forut for DPIA-prosjektet, hvor noen av funnene var:

- Mange har ikke gjort en DPIA, mens det står litt bedre til med gjennomføringene av ROS. (Men om kvaliteten på ROS-ene er god nok er en annen sak.)
- Lisensnivå M365: E3/A3 er det mest brukte lisensnivået innenfor skole (og kommune). (A3/E3 har mindre med sikkerhetsfunksjonalitet «innebygget» enn A5/E5.)
- Det vanligste: 1 felles tenant for kommunal virksomhet inkludert skole (skoleadministrasjon, lærere og elever).

En tenant – hva er det?

Hva er en tenant:

En tenant i Microsoft 365 (M365) er på en måte som **et eget «område» eller «leietakermiljø» i Microsofts sky**. Det er **en isolert og dedikert instans** (arbeidsområde) som en organisasjon får når den registrerer seg for M365-tjenester. Dette området er adskilt fra andre organisasjoner, og kan ses på som **en «lukket» kontainer for organisasjonens Microsoft 365-tjenester og data** – lagret i skyen, men i en infrastruktur som deles med mange andre organisasjoner. Innholdet i tenanten omfatter blant annet brukere og brukerkontoer, e-post, filer, dokumenter, kommunikasjon, sikkerhetsinnstillinger og administrative data.



En tenant-kontainer i skyen. Illustrasjon generert av Microsoft Copilot.

En visuell metafor for M365-tenants: En leilighet i et leilighetskompleks kan ses på som en tenant:

En visuell metafor for M365-tenants: En leilighet i et leilighetskompleks kan ses på som en tenant. Illustrasjon generert av Microsoft Copilot.

Man kan forestille seg et moderne (og STORT!) leilighetskompleks der hver leilighet har sin egen nøkkel, sine egne møbler og sine egne regler, men deler felles infrastruktur som inntak og opplegg for strøm og vann. Akkurat slik fungerer tenants i M365: isolerte enheter med egne data og konfigurasjoner, men bygget på en felles digital plattform.

Generelt om informasjonssikkerhet og personvern

Når vi snakker om oppsett og drift av Microsoft 365 (M365), inkludert valg av tenant-struktur, er det viktig å forstå og ta hensyn til grunnleggende prinsipper for **informasjonssikkerhet og personvern**. Dette danner grunnlaget for trygge løsninger i kommuner og skole, som er i samsvar med gjeldende krav til informasjonssikkerhet og

personvern. Til syvende og sist er det elevene som skal bli tilfredsstillende trygget gjennom veloverveide valg og tiltak. Valgte tenant-oppsett har også i høyeste grad relevans for informasjonssikkerheten og personvernet.

Det kan i noen tilfeller være en utfordring å **balansere høy brukervennlighet med kravene til informasjonssikkerhet og personvern**.

Hva er informasjonssikkerhet?

Informasjonssikkerhet handler om å beskytte informasjon for å sikre:

- **Konfidensialitet:** Informasjon kun tilgjengelig for dem som har rettmessig tilgang og tjenstlig behov for den.
- **Integritet:** Informasjon ikke har blitt endret eller slettet av feil eller av uvedkommende.
- **Tilgjengelighet:** Informasjon tilgjengelig når den trengs, for dem som trenger den (tjenstlig behov).

Disse tre prinsippene kalles ofte **KIT** (Konfidensialitet, Integritet og Tilgjengelighet). Brudd på ett eller flere av disse utgjør et sikkerhetsbrudd.

I tillegg er det andre viktige hensyn:

- **Robusthet**: Evnen til å håndtere og komme seg etter hendelser som angrep eller tekniske feil.
- **Etterlevelse**: All behandling av informasjon må følge lover og regler, som GDPR og andre nasjonale krav.
- **Økonomi**: Det koster å sikre informasjon – men det kan koste enda mer å la være.

Internkontroll i offentlig sektor

Offentlige virksomheter, som kommuner og fylkeskommuner, er **pålagt å ha styring og kontroll med informasjonssikkerheten gjennom internkontroll**, jf. eForvaltningsforskriften § 15. Internkontrollen skal baseres på anerkjente standarder for styringssystem for informasjonssikkerhet.

Den mest brukte standarden er **ISO/IEC 27001**, med veilederen **ISO/IEC 27002**. Den beskriver hvordan man etablerer og vedlikeholder et styringssystem for informasjonssikkerhet, med 93 konkrete tiltak innen blant annet:

- Tilgangsstyring
- Tofaktorautentisering
- Logging og overvåking
- Skysikkerhet
- Beskyttelse mot skadevare

Mange kommuner bruker også **NSMs grunnprinsipper for IKT-sikkerhet**, og flere har tatt i bruk styringssystemet fra **KiNS (Foreningen kommunal informasjonssikkerhet)**, som i hovedsak bygger på de samme prinsippene. Kinn kommune benytter seg av sistnevnte, dvs. KiNS sitt styringssystem (internkontroll) for informasjonssikkerhet og personvern.

Hva betyr GDPR for oss?

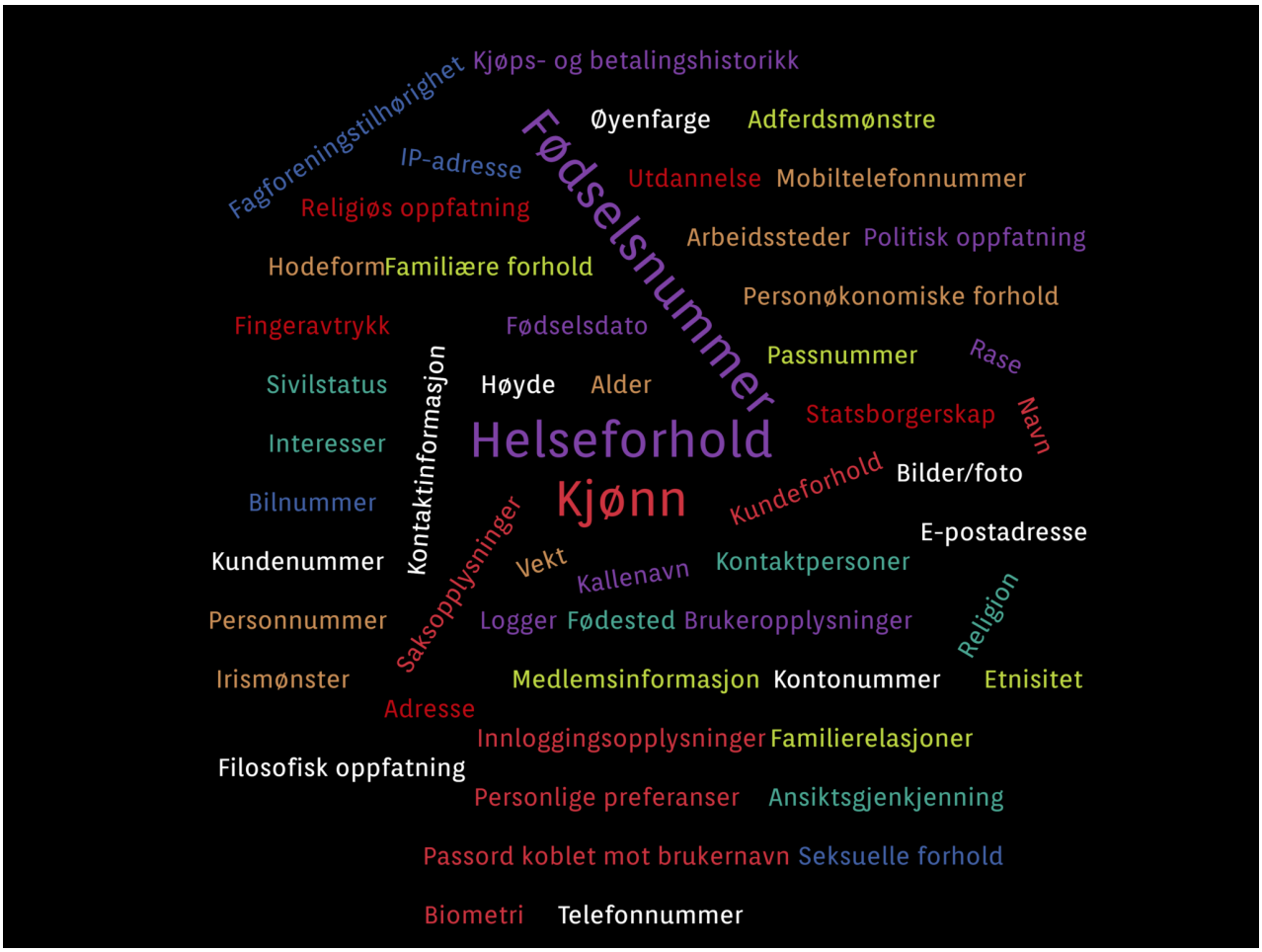
Først det åpenbare om **hva er personvern** (ifølge Datatilsynet):

> «Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger. Du har rett på en privat sfære som du selv kontrollerer, hvor du kan handle fritt uten tvang eller innblanding fra staten eller andre mennesker.»

Som EØS-medlem er Norge forpliktet til å følge **personvernforordningen (GDPR)** – EUs regelverk for behandling av personopplysninger. Forkortelsen GDPR står for **General Data Protection Regulation**, eller på norsk: Personvernforordningen.

I Norge er GDPR innført gjennom **personopplysningsloven**, som stiller krav til hvordan vi samler inn, bruker, lagrer, overfører og sletter personopplysninger. Målet er å beskytte individets rettigheter og hindre misbruk av informasjon. Forordningen trådte i kraft i 2018 og gjelder fullt ut i Norge. Den er særlig viktig å forstå når vi vurderer hvordan M365 skal settes opp og brukes i kommunal og skolebasert virksomhet.

Eksempler på personopplysninger:



Ulike former for personopplysninger (tjenesten Wordclouds.com benyttet til framstillingen av figur).

Spesielt må behandlingen av **særlige kategorier av personopplysninger** (sensitive personopplysninger) skje med stor varsomhet. Opplysninger som inngår i denne kategorien er: helseopplysninger, fagforeningsmedlemskap, religiøst standpunkt, politisk standpunkt, rase eller etnisitet, seksuelle forhold og legning, filosofisk overbevisning, biometriske opplysninger og genetiske opplysninger.

Grunnprinsipper for behandling av personopplysninger ifølge artikkel 5 i personvernforordningen, forkortet og fritt gjengitt nedenfor:

Personopplysninger skal:

- Behandles lovlig, rettferdig og åpent
- Kun brukes til klart definerte / spesifikke formål
- Begrenses til det som er nødvendig (dataminimering)
- Være korrekte og oppdaterte
- Ikke lagres lenger enn nødvendig
- Sikres mot uautorisert tilgang, ulovlig bruk og tap (konfidensialitet, integritet, tilgjengelighet)

I en kommune er (overordnet) **behandlingsansvarlig kommunedirektøren**.

Det kan **stilles spørsmål ved om innebygd personvern er tilstrekkelig ivaretatt i M365**, og om standardinnstillingene faktisk reflekterer de mest personvernvennlige valgene og innstillingene. (Svaret heller fort mot nei, i og med at produktet er utviklet i en annen jurisdiksjon (USA), med et regelverk og en praksis for personvern som skiller seg markant fra europeiske krav.)

Det blir (stilltiende?) inngått **databehandleravtale (DBA)** mellom Microsoft og den enkelte kommune eller IKT-samarbeid. Denne avtalen legger føringer for personvernet og informasjonssikkerheten ved bruk av Microsoft 365. Samtidig er det viktig å være klar over at Norge er en liten aktør i den globale sammenhengen, og det er derfor begrensede muligheter for å få gjennomslag for større tilpasninger i avtalen for å styrke personvernet ytterligere.

Bruken av M365 og andre digitale verktøy har ført til en **omfattende digitalisering og digital transformasjon,** også i skolen. Denne utviklingen skjer til tider uten en kritisk vurdering av konsekvensene for personvernet. Etter mine observasjoner ser det ut til at **personvernhensyn ofte kommer i bakgrunnen**, mens pedagogiske gevinster og muligheter for læring (+ teknologi-optimisme) får større oppmerksomhet.

Opplæring, kunnskapsdeling, involvering og informasjon (kommunikasjon i klart språk!) til hele organisasjonen er avgjørende for personvernområdet. Sikkerheten er aldri sterkere enn det svakeste leddet.

Microsoft 365 leveres av Microsoft, et amerikansk teknologiselskap (teknologigigant, «big tech»-selskap) med hovedbase i USA. Selv om selskapet er underlagt amerikansk lovgivning, har **Microsoft forpliktet seg til å overholde EUs personvernforordning (GDPR)** og tilbyr kontraktsfestede garantier for dette. Det vil uansett være **en viss grad av usikkerhet** knyttet til om personvernet er tilstrekkelig ivaretatt.

Microsoft oppgir at de **ikke selger personopplysninger til tredjeparter**. Innsamlede data brukes til å **levere og forbedre tjenestene**, men ikke til reklameformål i kommersielle skytjenester. F. eks. har EU-kommisjonen nylig bekreftet (juli 2025) at deres interne bruk av Microsoft 365 nå er i samsvar med europeiske personvernkrav, etter innføring av ekstra tekniske og kontraktsmessige tiltak. Muligens er det mulig å få til noe tilsvarende innenfor den norske skolesektoren.

Problemstillingen er?

Det er god grunn til å tro at **mange kommuner** – og også interkommunale IKT-samarbeid, kommunale foretak (KF) og interkommunale selskaper (IKS) – ofte **deler / har én felles (single/enkel) tenant i Microsoft 365**. Dette kan skape **utfordringer med å holde data og personopplysninger tilstrekkelig adskilt eller segregert**. Kravene til **konfidensialitet**, gyldig **behandlingsgrunnlag** og **dataminimering** fra regelverket rundt personvern kan stå i fare for å bli brutt.

Når det gjelder skolesektoren, omfatter denne **mindreårige elever** (barn og unge), som i personvernsammenheng regnes som **sårbare registrerte**. Dette innebærer at de har krav på et **særlig vern og beskyttelse av sine personopplysninger**. I tillegg finnes det elever med **adressesperre** (hemmelig adresse), noe som stiller ekstra krav til sikkerhet og tilgangsstyring. I en felles tenant kan det derfor være spesielt utfordrende å ivareta tilstrekkelig informasjonssikkerhet og personvern for denne elevgruppen. Det er heller **ikke akseptabelt at kommunalt ansatte utenfor skole**sektoren – uten tjenstlig behov – har tilgang til eller **kan søke opp elever** og deres personopplysninger.

Utgangspunkt for tenant-oppsett

Av **økonomiske, organisatoriske, praktiske, kunnskapsmessige og tekniske grunner** (+ ut fra makelighetshensyn?) velger mange kommuner ut fra min erfaring å **samle all kommunal virksomhet i én felles tenant**. Dette gjelder også flere interkommunale IKT-samarbeid, hvor flere kommuner og ulike virksomheter deler samme løsning og tenant. En slik struktur kan imidlertid føre til sikkerhetsutfordringer som kan være krevende å håndtere på en tilfredsstillende måte.

For organisasjoner med under én million brukere anbefales det som hovedregel å benytte én felles tenant for hele virksomheten, med mindre det foreligger særskilte behov som tilsier en annen løsning. Dette rådet støttes også bredt blant leverandører av M365-tjenester til norske kommuner, inkludert konsulenthus, Microsoft-partnere og Microsoft selv.

Å etablere en arkitektur med flere tenants kan være hensiktsmessig dersom det foreligger særskilte krav knyttet til **sikkerhet, personvern** eller **administrasjon/styring**. I oppvekstsektoren, hvor det behandles sensitive personopplysninger om barn og unge (mindreårige elever), kan slike krav i enkelte tilfeller gjøre en slik løsning nødvendig eller ønskelig.

Kommunene må derfor nøye vurdere om det er tilstrekkelig å samle all kommunal virksomhet, inkludert skole, i **én felles tenant**, eller om det er behov for å etablere **flere tenants** for å ivareta krav til personvern og informasjonssikkerhet. Det finnes ingen universell fasit – beslutningen vil blant annet avhenge av **kommunens risikovilje og hvilke sikkerhetstiltak som planlegges eller allerede er på plass**.

Det er grunn til å anta at **en overgang fra én tenant-struktur til en annen kan medføre betydelige kostnader i form av tid og ressurser**. I enkelte tilfeller kan disse **kostnadene overstige den forventede nytten**. Valg av tenant-arkitektur har samtidig direkte betydning for både **risikovurderinger (ROS) og personvernkonsekvensvurderinger (DPIA)**, som må gjennomføres i samsvar med gjeldende regelverk på personvernområdet. Kommunens vurdering av **akseptabelt risikonivå (risikoappetitt)** vil også ha innvirkning på disse valgene og analysene.

Fordeler og ulemper med å samle alt i en felles tenant

Når flere kommuner, avdelinger og/eller offentlige enheter deler én Microsoft 365-tenant, kan det gi både fordeler og utfordringer. Her er en kraftig forenklet oversikt.

Fordeler:

- **Enklere samarbeid og samhandling:** Deling, kommunikasjon og samhandling på tvers av organisasjoner og internt mellom ulike avdelinger blir enklere og mer sømløst. Løsningen er brukervennlig, oversiktlig og eliminerer behovet for gjestekontoer, inn-/utlogginger / vekslinger mellom ulike kontoer eller dobbelt-kontoer for nøkkelpersonell. I tillegg gir en felles tenant en enklere og mer oversiktlig lagringsstruktur enn om man opererer i et miljø med flere tenants.
- **Effektiv administrasjon:** Gir enklere og mer oversiktlig styring av brukere, tilgang og sikkerhet fra ett sentralt (felles) sted. Det er kun behov for å konfigurere nødvendige innstillinger én gang for alle brukere og enheter.
- **God tilgang på kompetanse:** Det er enklere å finne IT/IKT-personell med relevant erfaring når man benytter én felles tenant. Effektiv administrasjon av et oppsett med flere tenants krever ofte avansert skripting, noe det kan være begrenset kompetanse på. Med en felles tenant kan administrasjonen i større grad håndteres gjennom grafiske grensesnitt i Entra ID og Microsofts Endpoint Management-løsninger, som Intune og SCCM.
- **Lavere kostnader og kostnadseffektiv drift:** Redusert dobbeltarbeid, lavere kompleksitet og enklere – og dermed rimeligere – lisenshåndtering og drift.
- **Høy sikkerhet kan oppnås:** Med riktige tiltak, konfigurasjoner og nødvendige lisenser og/eller tilleggsprodukter, kan et relativt høyt sikkerhetsnivå oppnås.
- **Enklere integrasjoner mellom M365 og andre fagsystemer:** Når alt er samlet i én tenant og løsningen er standardisert, blir det enklere å koble til og integrere andre systemer og fagsystemer. Dette gir mer sømløse og effektive løsninger på tvers av plattformer. Enkelte fagsystemer er dessuten dårlig tilrettelagt for flere parallelle integrasjoner mot ulike M365-tenanter. Dersom man velger å dele opp løsningen i flere uavhengige tenanter, kan dette komplisere integrasjonsarbeidet og medføre økte drifts- og administrasjonskostnader (kostnadsdrivende).
- **Standardisering:** Felles løsninger med standardiserte fagsystemer og én felles tenant kan gi betydelige stordriftsfordeler i driften.
- **I tråd med anbefalinger:** Oppsettet støttes av Microsoft, samt av en rekke tredjeparts konsulenter og konsulentselskaper med erfaring fra lignende implementeringer.

Ulemper:

- **Datasikkerhet:** Risiko for at brukere får tilgang til feil eller for mye informasjon – altså data de ikke har tjenstlig behov for. Det kan lett glippe med nødvendig segregering av data.

- **Endringer i funksjonalitet:** Kontinuerlige oppdateringer og ny funksjonalitet i M365 kan svekke sikkerheten dersom man ikke følger utviklingen tett og justerer sikkerhetsinnstillingene i takt med endringene.
- **Skjerming av personer:** Det kan være utfordrende å beskytte skjermede identiteter (f. eks. elever med adressesperre) fullt ut i en felles tenant. For eksempel kan søkefunksjonalitet i M365 i noen tilfeller blottlegge for mye informasjon. Ifølge KI kan aktuelle tiltak for å sikre nødvendig skjerming være: Bruk av «Confidential Labels» (konfidensialitetsetiketter), «Information Barriers» (Informasjonsbarrierer, et konkret produkt/funksjon fra Microsoft) eller «Sensitivity Labels» (sensitivitetsetiketter). Slike tiltak kan komplisere driften noe.
- **Ytelse:** Store datamengder samlet i én tenant kan i teorien føre til redusert ytelse (i prosesseringen). Dette er imidlertid lite sannsynlig å bli en utfordring i norsk kommunesektor, der enhetene er små i global sammenheng.
- **Personvern og juss:** Det kan være uklart om det er lovlig å dele data mellom ulike juridiske eller organisatoriske enheter innenfor én felles M365-tenant. Dette skaper potensielle utfordringer knyttet til både personvern og databehandleransvar. Det er helt avgjørende at databehandleransvaret er klart definert og fordelt, at det er tydelig hvem som er behandlingsansvarlig for hvilke data og prosesser og at det foreligger nødvendige avtaler og dokumentasjon som regulerer dataflyt og ansvar. Klare databehandleravtaler (DBA) må foreligge, og behandlingsgrunnlag og formålsavgrensning må være klart definert. Noen aktuelle juridiske rammer og lovverk som gjelder: Personopplysningsloven med tilhørende EU-forordning (GDPR), kommuneloven, offentleglova og opplæringslova. Det må gjennomføres internkontroll og revisjon av et slikt oppsett.
- **Lite fleksibilitet:** Lokale tilpasninger (pr. avdeling eller organisasjon) kan være vanskelige å få til, da mange innstillinger i utgangspunktet kun kan gjøres på globalt nivå for hele tenanten.
- **Ulik risikovilje:** Det kan være krevende å implementere ulike sikkerhetsnivåer og risikoprofiler / risikonivåer innenfor én felles struktur.
- **Fare for feildeling:** Brukere kan ved en menneskelig feil eller uhell dele informasjon med uvedkommende, for eksempel ved å gi for brede delingstillatelser (f. eks. «alle i organisasjonen» og/eller inkludering av eksterne). Risikoen øker i miljøer med mange brukere og organisasjoner, spesielt der det er komplekse delingsmuligheter og manglende opplæring.
- **Håndtering av sensitiv informasjon:** M365 er ikke nødvendigvis egnet for behandling av sensitiv eller strengt konfidensiell informasjon. Slike data bør håndteres i dedikerte fagsystemer. Dette blir enda tydeligere hvis alt er samlet i en felles tenant.
- **Større konsekvenser ved dataangrep:** Et datainnbrudd i én tenant kan få større konsekvenser, da store mengder data fra flere enheter kan bli kompromittert samtidig.

- **KI (Copilot) og personvern:** Bruk av KI/AI-verktøy som Copilot kan medføre risiko for utilsiktet tilgang til sensitiv informasjon, dersom ikke nødvendige sikkerhetstiltak er på plass. (Virksomhet / organisasjon ikke «Copilot Ready» når tjenestene slås på. Å være «Copilot Ready» – klare for å ta i bruk Copilot – innebærer blant annet at man har på plass krav til dataklassifisering, tilgangsstyring og opplæring.) God datakvalitet kreves for å få nytte av KI.

Oppsummering:

Sjekkpunkter for vurdering av felles tenant-oppsett:

- Organisatorisk og teknologisk **modenhet**
- Tilgang til relevant **kompetanse** (teknisk, juridisk og organisatorisk)
- En gjennomarbeidet **sikkerhetsstrategi** med tilhørende tiltak
- Utførte og dokumenterte **juridiske vurderinger**, inkludert personvern og databehandleransvar.

En felles Microsoft 365-tenant (for all kommunal virksomhet inkludert skole) kan være en **attraktiv løsning for kommuner**, særlig med tanke på **forenklet drift, samhandling, høy brukervennlighet og potensielle kostnadsbesparelser**. Likevel krever en slik modell **grundige vurderinger knyttet til informasjonssikkerhet, personvern, risikohåndtering og behovet for lokal autonomi**.

Det er avgjørende at kommunene gjør **bevisste valg** basert på egne behov og **modenhet**, og at **nødvendige sikkerhetstiltak** og tekniske kontroller er på plass – uavhengig av om man velger én felles tenant eller deler opp i flere tenants.

Jeg antar at mange kommuner (de fleste?) **fortsatt vil foretrekke å ha en felles tenant**, men da må dette følges opp med **tydelige strategier og tiltak for sikkerhet, etterlevelse og effektiv forvaltning**.

Valg av tenant-oppsett eller oppdeling i flere tenants påvirker – eller **kan påvirke – de påfølgende ROS- og DPIA-analysene**, som omtales senere i dette innlegget.

M365, skyen, tenant og DPIA. Illustrasjon generert av Microsoft Copilot.

Aktuelle sikringstiltak

Den enkelte organisasjon kan gjennom **egne risikovurderinger komme fram til at risikoene ved en felles tenant-løsning er akseptable**, så lenge tilgjengelige sikkerhetsinnstillinger i standardlisensene benyttes korrekt. I slike tilfeller er det ikke nødvendigvis behov for verken tilleggsløsninger eller oppgradering til dyrere Microsoft 365-lisenser.

Med riktige tiltak kan man likevel oppnå et høyt sikkerhetsnivå. Dette forutsetter at sikkerhetsinnstillingene er godt planlagt, riktig konfigurert og kontinuerlig vedlikeholdt.

Enkle sikringstiltak uten store kostnader

Ved hjelp av innebygde administrasjonsverktøy og tilpassede brukerprofiler i Microsoft 365, kan det etableres effektive sikkerhetstiltak uten vesentlige ekstrakostnader eller stor ressursbruk.

Eksempler på slike tiltak inkluderer:

- **Begrensning av muligheten for at eksterne aktører kontakter elever** via Teams eller e-post.
- **Aktivering av adresseboksegregering**, slik at brukere kun ser relevante kontakter – noe som styrker både personvern og digital sikkerhet.
- Innføring av **streng tilgangskontroll og delingsrestriksjoner**, for å sikre at kun autoriserte brukere får tilgang til informasjon, og at data ikke deles utilsiktet.
- I enkelte tilfeller eventuelt benytte seg av **pseudonymisering**.

I dagens uforutsigbare trusselbilde er det nærmest en nødvendighet for kommuner å benytte et automatisert **MDR-system** («Managed Detection and Response», på norsk «Administrert oppdagelse og respons»). Slike løsninger tilbyr avanserte sikkerhetstjenester for å oppdage trusler, håndtere hendelser raskt og gi faglig rådgivning. Typisk består MDR av en kombinasjon av programvare med sensorer og automatiserte prosesser, samt et eksternt team av sikkerhetseksperter som kan bistå ved behov. I tillegg er samarbeid med aktører som HelseCERT og KommuneCERT en viktig del av et helhetlig sikkerhetsarbeid.

Spesielt for ansatte i skolen, med tilgang på konfidensiell informasjon: For å sikre god beskyttelse av brukerkontoer i Microsoft 365, bør det benyttes **multifaktorautentisering (MFA)**. Dette innebærer at brukeren må bekrefte identiteten sin med minst to uavhengige faktorer, for eksempel passord (noe du vet) og en kode fra en autentiseringsapp eller liknende (noe du har). MFA reduserer risikoen for uautorisert tilgang betydelig sammenlignet med kun bruk av passord.

Grunnleggende IKT-sikkerhetstiltak – som antivirus, brannmur, sikkerhetskopiering (backup), innlegging av sikkerhetsoppdateringer (patching) av programvare og systemer, god passordpraksis og detaljert tilgangsstyring – behandles ikke i dette innlegget. Det forutsettes at slike tiltak er implementert i samsvar med gjeldende krav og beste praksis.

Utvidede tiltak ved høyere sikkerhetsbehov

For organisasjoner med høyere krav til sikkerhet og kontroll, kan det være aktuelt å ta i bruk **mer avanserte lisenser som Microsoft 365 E5/A5**. Disse gir tilgang til utvidede sikkerhetsfunksjoner (f. eks. Information Barriers) og bedre loggføring. Alternativt kan man supplere E3/A3-lisenser med tillegg som ***Information Barriers* (IB)**, eller benytte tredjepartsløsninger med tilsvarende funksjonalitet. Information Barriers (IB) skal bidra til å hindre uønsket informasjonsflyt mellom grupper («vanntette skott»), forutsatt at funksjonen er riktig satt opp.

Selv om slike tiltak kan medføre økte lisenskostnader, kan behovet for høyere lisensnivå også være drevet av andre hensyn – som bedre logging, økt lagringskapasitet eller generell funksjonalitet. I slike tilfeller kan forbedret **sikkerhet sees som en positiv bieffekt**.

Sikkerhetstiltak i Microsoft 365

Tabellen nedenfor er generert av Microsoft 365 Copilot KI (GPT-5 påslått) pr. 05.09.2025. En del av tiltakene krever tilleggs-lisenser / abonnement på tilleggsprodukter. Opplistingen blir vel IKT-teknisk, og jeg har ikke hatt anledning til fullt ut å kvalitetssjekke innholdet da dette blir utenfor mitt primære kunnskapsområde. Tabellen ser imidlertid slik ut:

Kategori:	***Tiltak:***
Identitet og tilgang (Microsoft Entra ID)	• Multi-Factor Authentication (MFA) • Conditional Access • Privileged Identity Management (PIM) / Just-in-time • Identity Protection (risikobaserte policyer) • RBAC (minste privilegium)
Enhets- og applikasjonsstyring (Microsoft Intune)	• Enhetscompliance og konfigurasjon • App Protection Policies (MAM) • Endpoint Security-policyer (Defender, brannmur, disk-kryptering) • Windows Autopilot og Remote Help • (Tillegg) Endpoint Privilege Management (EPM)
Lokal/Hybrid enhetsforvaltning (Microsoft Configuration Manager, tidligere SCCM – System Center Configuration Manager og senere MECM – Microsoft Endpoint Configuration Manager)	• OS-utrulling og task sequences • Programdistribusjon og patching • BitLocker- og endpoint-beskyttelse • Co-management / tenant attach med Intune

Støtte for drift og overvåking (System Center)	• SCOM (overvåking) • SCVMM (virtualisering/kapasitetsstyring) • Relevante i datarom/hybrid-scenarier som støtteverktøy
Data- og informasjonsbeskyttelse	• Sensitivity Labels • Data Loss Prevention (DLP) • Kryptering (inkl. Customer Key)
Microsoft Purview	• Data Classification • Sensitivity Labels • Data Loss Prevention (DLP) • Insider Risk Management • Communication Compliance • eDiscovery og Audit • Records Management
Kommunikasjonskontroll	Information Barriers (hindre kommunikasjon mellom definerte grupper)
Trusselbeskyttelse	• Microsoft Defender for Office 365 • Microsoft Defender for Identity • SIEM/SOAR (f.eks. Microsoft Sentinel)
Overvåking og varsling	• Unified Audit Log • Alert Policies • Compliance-rapporter
Administrativ sikkerhet	• Reduser antall globale administratorer • Separate admin-kontoer og break-glass-kontoer • Prinsipp om minste privilegium

Hva inngår og hva inngår ikke i prosjektet

Hva vil inngå og ikke inngå i leveransene fra det nasjonale prosjektet, etter den lille kjennskap jeg fikk til prosjektet:

- **Avgrensinger i scope (rammer/omfang):** Det har blitt foretatt avgrensninger i scope (hva som er med, og hva som ikke er med). Microsoft 365 er en omfattende pakke med applikasjoner og tjenester, og det er ikke mulig å vurdere og analysere alt. Noen avgrensninger må derfor foretas, basert på hva som fremstår som de mest relevante problemstillingene i norsk skole.

- **For lite fokus på KI:** Det eneste punktet jeg stiller meg noe kritisk til, er det begrensede fokuset på Microsofts KI-teknologi, spesielt Copilot i Microsoft 365. Begrunnelsen for å i stor grad utelate denne teknologien var at den har lav relevans, ettersom aldersgrensen for bruk tidligere var satt til 18 år. Imidlertid har Microsoft nå endret dette. Ifølge deres nettsider (fritt gjengitt): Tidligere var Copilot KI kun tilgjengelig for brukere over 18 år, men nå er tilgangen utvidet til også å inkludere brukere mellom 13 og 18 år – riktignok med krav om foreldreinnstillinger og visse begrensninger i funksjonalitet. Dette betyr at teknologien potensielt kan være relevant (i hvert fall privat) for elever i ungdomsskolen og videregående skole, og bør derfor vurderes nærmere i prosjektet.
- **Behandlinger:** Det er utarbeidet – eller pågår arbeid med å utarbeide – kartlegging av behandlinger og forslag til behandlingsprotokoll for Microsoft 365.
- **Overføring av data og personopplysninger til USA:** Microsoft er en amerikansk leverandør, og det vil i noen grad skje overføring av personopplysninger fra Norge og Europa til USA. Slike overføringer skjer i henhold til Data Privacy Framework (DPF) og bygger på EUs adekvansbeslutning knyttet til personvern. I dagens usikre geopolitiske situasjon – med blant annet Trump som president – kan dette imidlertid skape utfordringer. Mange peker derfor på behovet for å ha en klar exit-strategi fra avhengighet til amerikanske big tech-aktører. Det er allerede gjennomført noe arbeid på dette området rundt overføringsgrunnlag, og mer vil komme.
- **Behandlingsansvarlig og databehandler:** Grensegangen mellom når kommunen er behandlingsansvarlig og når Microsoft opptrer som databehandler – og vice versa – må tydeliggjøres.
- **Risikovurderinger (ROS):** Ansvar for gjennomføring av risikovurderinger (ROS) er fullt og helt lagt til den enkelte kommune, og er ikke en del av det nasjonale prosjektets leveranser.
- Hoved-leveransen fra prosjektet blir **DPIA-en** for M365 skole.

Jeg nevner nok en gang at jeg ufrivillig har blitt ekskludert som prosjektmedarbeider fra det nasjonale KS SkoleSec DPIA-prosjektet, så jeg har ikke full oversikt over den videre utviklingen.

I fortsettelsen vil det bli presentert **en teoretisk tilnærming med praktiske implikasjoner**, i form av omtale av behandlingsprotokoll, ROS og DPIA:

Behandlingsprotokoll

Forut for ROS og DPIA er det nødvendig (jf. artikkel 30) og naturlig å få på plass en **behandlingsprotokoll**, som i en forenklet form også kan gjøres om til en offentlig **personvernerklæring** for behandlingen. Det nasjonale prosjektet har på sin side (foreløpig) presentert:

> KS SkoleSec: Forslag til behandlingsprotokoll for Microsoft 365

Denne har jeg foreløpig ikke satt meg grundig inn i. I stedet har jeg forholdt meg til den måten vi gjør det i Kinn kommune. På min arbeidsplass benytter vi oss av IKT-systemet **Sikri Samsvar Personvern**, som i praksis er et IKT-system bestående av en samling av maler for å forenkle arbeidet med å få laget **behandlingsprotokoller** og offentlige **personvernerklæringer**. **Samsvar-systemet legger opp til noen få samlede protokoller for hele skoledriften**, i stedet for å ha en for hver av de enkelte IKT-systemene/fagsystemene.

Protokollene inneholder noen konfidensielle / fortrolige data, så jeg kan ikke dele en komplett behandlingsprotokoll her. Imidlertid kan jeg i stedet dele en offisiell **personvernerklæring relatert til skoledriften/skolehverdagen** hentet fra vår personvern-nettside:

- Kinn kommune personvernerklæring: Skulekvardagen – dagleg skuledrift
- Flere personvernerklæringer: Personvern og personvernerklæringar – Kinn kommune

Personvernerklæringene mangler følgende som kun er tilgjengelig i behandlingsprotkollene: Nødvendigheten av personvernkonsekvensvurdering (DPIA), systemoversikt (IKT-systemer/fagsystemer brukt i behandlingen) og eventuelt behovet for samtykke.

Hva er det naturlig å inkludere i en behandlingsprotokoll?

Innledningsvis:

- Navn og kontaktopplysninger til behandlingsansvarlig og personvernombud, og eventuelt andre involverte i behandlingen.
- Praktisk også å knytte behandlingen opp mot relevant intern sektor/avdeling.
- Få en oversikt over om det er snakk om håndtering av personopplysninger relatert til egne ansatte (internt), eller om det er informasjon om innbyggere/tjenestemottakere (eksternt).
- Protokollene dateres. Det bør også framgå hvem som har utarbeidet dem.

Momentliste – protokollinnhold

- Formålet med behandlingen av personopplysninger
- Personopplysninger som registreres (kategorier)
- Sensitive personopplysninger som registreres (kategorier)
- Kategorier av registrerte
- Systemer inkludert i behandlingen (IKT-system/fagsystem)
- Innsamling av personopplysninger (hvordan og hvor opplysningene hentes fra)
- Behandlingsgrunnlag (personopplysningsloven med forordning artikkel 6.1.a-f og artikkel 9.2.a-j)
- Hjemmelsgrunnlag (hvis lovhjemmel i annen lov som behandlingsgrunnlag)
- Hvis behov for samtykke fra de registrerte (som behandlingsgrunnlag)
- Viderebehandling av personopplysninger
- Interne brukere av personopplysninger
- Interne brukere av sensitive personopplysninger
- Mottakere av personopplysninger (eksterne aktører/kategorier av aktører som opplysningene deles med)
- Mottakere av sensitive personopplysninger (eksterne aktører/kategorier av aktører som opplysningene deles med)
- Eventuell overføring til tredjeland (lovligheten og grunnlaget for slik overføring)
- Sletting og lagring (rutinene og slettefrister)
- Datalagring (hvor opplysningene lagres)
- Bruk av automatiske avgjørelser
- Vurdering av personvernkonsekvenser (initial vurdering av behov for DPIA eller ikke? Eventuelt lenke til DPIA.)
- I noen tilfeller aktuelt: Eksplisitte opplysninger om straffedommer/lovovertredelser (art. 10).
- Også ha med noe om: Generell beskrivelse av tekniske og organisatoriske sikkerhetstiltak, skriftlig dokumentert.

Risikovurdering (ROS) forut for DPIA – Microsoft 365 i skolen

Datatilsynet beskriver risikovurdering slik:

> «Gjennom en **risikovurdering** skal virksomheten identifisere uønskede hendelser og risikoen for at disse skal inntreffe.»

I praksis innebærer dette å **kartlegge mulige uønskede hendelser**, **vurdere sannsynligheten** for at de inntreffer, og hvilke **konsekvenser** de kan få. Basert på dette foreslås **tiltak** for å redusere risikoen, og det gjøres en vurdering av **restrisikoen** etter at tiltakene er implementert.

Innledende risikovurderinger (forut for en DPIA) får ofte en mer **IKT-teknisk vinkling** enn en DPIA. Fokus rettes da gjerne spesielt mot **informasjonssikkerheten** (jf. KIT). Som utgangspunkt for en risikovurdering kan f. eks. malen til KiNS bli benyttet (lenke).

Risikovurderinger (ROS) må gjøres av den enkelte kommune, da dette ikke inngår i den nasjonale DPIA-en. Før det gjennomføres en fullstendig DPIA, er det viktig å identifisere og vurdere relevante risikomomenter knyttet til bruk av Microsoft 365 i skolekontekst. Nedenfor følger en oversikt over potensielle risikoer, strukturert etter tema:

1. Tilgjengelighet og tilgangsstyring

- **Bruker får ikke tilgang til systemet** (f. eks. glemt passord, bruker ikke opprettet, utstyrs-/linjefeil).
- **Systemet er utilgjengelig** pga. problemer hos driftsleverandør, linjeleverandør, nedetid, nettverksfeil, eksterne datangrep eller lignende.
- **Bruker beholder tilgang etter fratreden** (f. eks. etter avsluttet ansettelsesforhold eller endret rolle).
- **Uvedkommende får tilgang til konto** via kompromittert passord eller svak autentisering.
- **Feil i AD- eller FEIDE-integrasjon** fører til feil tilgangsstyring (f. eks. elever får lærerrettigheter).

2. Informasjonssikkerhet og personvern

- **Mangelfull opplæring** fører til feilaktig bruk som svekker sikkerheten.
- **Feilaktige eller uriktige data** legges inn i systemet, eller feil oppstår i integrasjoner.
- **Data kommer på avveie** (f. eks. via datainnbrudd/angrep, hacking, sårbarheter, leverandørfeil eller interne trusler).
- **Uvedkommende får tilgang til personopplysninger** (f. eks. via feil deling eller svak tilgangskontroll).
- **Snoking** i elevmapper eller logger uten hjemmel.
- **Samskriving eller deling** fører til utilsiktet deling av sensitive personopplysninger.
- **Bilder/video av elever** deles uten samtykke eller til feil mottakere.
- Bør det gjøres risikovurderinger knyttet opp mot **metadata og automatisk generert informasjon**?

3. Leverandør og databehandlerforhold

- **Leverandør samler inn mer informasjon** enn avtalt, eller bruker data til andre formål.
- **Databehandleravtale mangler** eller er ikke oppdatert.
- **Manglende kontroll over endringer** i tjenestevilkår eller funksjonalitet.
- **Tjenester hvor Microsoft er behandlingsansvarlig** benyttes uten tilstrekkelig vurdering (f. eks. Copilot, Bing Chat).
- Hva med **manglende DPIA fra underleverandører**, som ikke nødvendigvis blir snappet opp av kommunenes kontroller.

4. Juridiske og organisatoriske forhold

- **Manglende hjemmels- og formålsvurdering** for behandlingen.
- **Manglende vurdering av ressursenes egnethet** for bruk i undervisning.
- **Manglende rolleavklaringer** mellom skole, kommune og leverandør.
- **Manglende logging og sporbarhet** gjør det vanskelig å oppdage misbruk.
- **Manglende beredskapsplaner** for håndtering av sikkerhetsbrudd eller systemsvikt.

5. Skybaserte tjenester og internasjonal dataflyt

- **Risiko ved bruk av skytjenester**, som datalagring utenfor EU/EØS, manglende kontroll over dataflyt og uforutsigbare endringer.
- **Overføring av data til tredjeland** uten tilstrekkelig beskyttelse (f. eks. USA).
- **Bruk av AI-funksjoner** (f. eks. Copilot) som kan samle inn eller generere sensitiv informasjon.

6. Brukeratferd og kultur

- **Manglende bevissthet om personvern** blant ansatte og elever kan føre til uaktsom deling eller lagring av sensitive opplysninger.
- **Bruk av private kontoer eller enheter** til skoleformål kan føre til tap av kontroll over data.
- **Deling av brukerkontoer** (f. eks. felles elevkontoer) svekker sporbarhet og sikkerhet.
- Bør muligens vurderes: **Digitale vaner og kultur** (ukultur?) som har blitt utviklet over tid, og som kan påvirke etterlevelsen (f. eks. normalisering av deling via Teams-chat eller OneDrive).

7. Endringshåndtering og vedlikehold

- **Manglende rutiner for endringer i systemet** (f. eks. nye funksjoner, oppdateringer eller integrasjoner) kan introdusere nye risikoer uten at de blir fanget opp.
- **Manglende testing av endringer** før produksjonssetting kan føre til funksjonssvikt eller datatap.

8. Dokumentasjon og etterlevelse

- **Manglende dokumentasjon** av behandlingsaktiviteter, tilgangsstyring og sikkerhetstiltak kan gjøre det vanskelig å etterleve krav i personvernlovgivningen.
- **Manglende revisjon og kontrollrutiner** gjør det vanskelig å oppdage avvik eller svakheter i praksis.

9. Kommunikasjon og samtykke

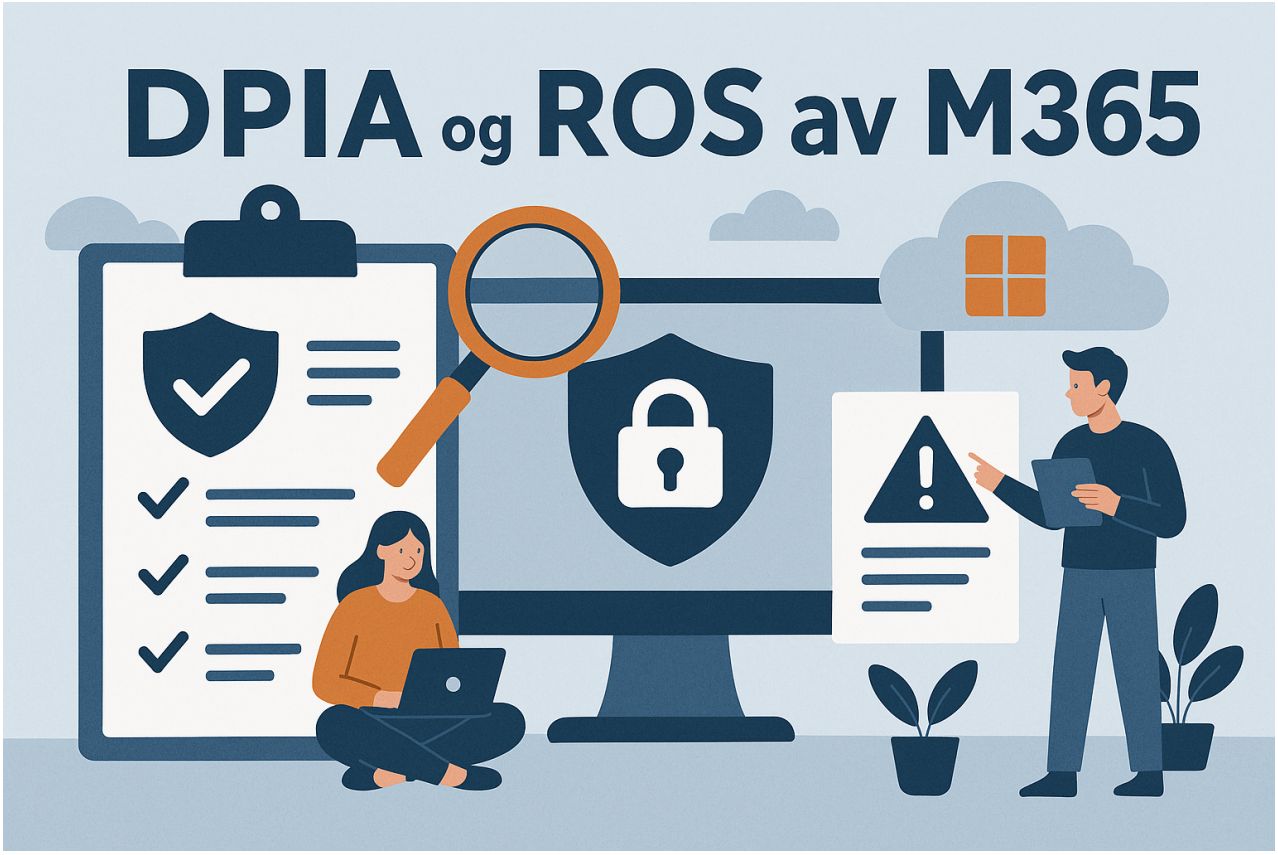
- **Manglende eller uklar informasjon til foresatte og elever** om hvordan data behandles, kan svekke tilliten og bryte med krav til åpenhet.
- **Samtykke innhentes ikke der det er nødvendig**, eller samtykke brukes feil som behandlingsgrunnlag.

10. Tverrkommunal eller regional bruk

- **Deling av data mellom skoler eller kommuner** uten klare avtaler og vurderinger kan føre til brudd på personvernet (manglende behandlingsgrunnlag).
- **Fellesløsninger** (f. eks. interkommunale skytjenester) kan medføre behov for klare avtaler og behandlingsgrunnlag.
- **Ulik praksis mellom skoler** kan føre til ujevn risikohåndtering og svekket etterlevelse.

11. KI/AI-funksjoner og Copilot (hvis aktuelt)

- Muligheter for **uforutsigbar databehandling**. (Databehandlingen er ikke alltid forutsigbar, forståelig eller transparent for brukeren.)
- **Potensiell gjenbruk av elevdata i modelltrening** (selv om Microsoft sier de ikke gjør dette).
- **Mangel på transparens**: Vanskeligheter med å forklare hvordan KI kommer frem til sine svar.
- **Microsoft Graph** sin kraftige funksjonalitet kan være et faremoment. Microsoft Graph er et API som gir tilgang til data fra hele M365-økosystemet. Det er grensesnittet Copilot KI (hvis aktivert) bruker for å hente ut og analysere data, slik at den kan generere relevante og kontekstbaserte KI-svar. Hvis tilgangskontroll ikke er riktig satt opp kan man via KI få tilgang på sensitiv og/eller konfidensiell informasjon som man ikke skulle ha hatt tilgang på.



Visualisering av DPIA og ROS-prosesser knyttet til bruken av Microsoft 365 i kommune og skole. Illustrasjon generert av Microsoft Copilot.

Hva er en DPIA?

DPIA står for *Data Protection Impact Assessment*, eller på norsk: **vurdering av personvernkonsekvenser / personvernkonsekvensvurdering**. Her er et forsøk på en definisjon:

> En DPIA (vurdering av personvernkonsekvenser) er en analyse som gjennomføres for å identifisere og redusere risikoer for personvernet ved behandling av personopplysninger – særlig når det benyttes ny teknologi eller behandlingen innebærer høy risiko. Fokus rettes mot **personvernet til de registrerte**, i dette tilfellet spesielt mindreårige skoleelever (barn- og unge).

Regelverket for GDPR/personvern krever i en del tilfeller at slike analyser og vurderinger gjennomføres – slik som i dette tilfellet, hvor det behandles opplysninger om sårbare registrerte (barn og unge). **Det nasjonale prosjektet skal til slutt resultere i en slik DPIA-vurdering**. I prosjektet har de hele tiden uttrykt at man **i fellesskap skal utarbeide en 80 %-løsning**, som deretter **må tilpasses med 20 % lokalt** – til den enkelte kommune eller skole.

I forrige runde – i forbindelse med utarbeidelsen og leveransen av «Ny nasjonal personvernkonsekvensvurdering for bruk av Google Workspace for Education i skolen» – endte man opp med et omfattende Excel-ark med en lang rekke punkter for risikoer og tiltak. Selv foretrekker jeg en tilnærming mer i tråd med malen som KiNS har presentert. Hva man ender opp med i denne runden, relatert til M365, er foreløpig uvisst for min del.

Jeg har prøvd å få KI til å fange essensen fra KiNS sin DPIA-mal:

Punktvis oppsummering av DPIA-vurderinger

1. **Innledende vurderinger**
    - Må full DPIA-vurdering gjennomføres, basert på gitte vurderingskriterier: Ja/Nei?
    - Informasjon om fagsystemet / IT-systemet?
2. **Formål med behandlingen**
    - Hva er hensikten med behandlingen av personopplysninger?
    - Hvilket behov skal løses?
3. **Beskrivelse av behandlingen**
    - Systematisk beskrivelse av behandlingen og behandlingsaktiviteter.
    - Dataflyt?
    - Hvilke typer personopplysninger behandles?
    - Hvem er de registrerte (f.eks. ansatte, innbyggere)?
    - Hvordan samles, lagres, brukes og deles opplysningene?
4. **Behandlingsgrunnlag**
    - Hvilket rettslig grunnlag benyttes (samtykke, lovpålagt, avtale, etc.)?
    - Er det behov for særskilt hjemmel ved behandling av sensitive opplysninger?
5. **Systembeskrivelse**
    - Hvilket system eller teknologi benyttes?
    - Hvem er leverandør og hvor lagres data?
6. **Databehandlere og tredjeparter**
    - Databehandlere?
    - Hvem har tilgang til dataene?
    - Er det inngått databehandleravtaler?
7. **Risikovurdering**
    - Hvilke personvernrisikoer – risikoer for de registrerte – er identifisert?
    - Hva er sannsynligheten og konsekvensen av disse risikoene?
8. **Tiltak for risikoredusering**
    - Hvilke tekniske og organisatoriske tiltak er planlagt eller iverksatt?
    - Hvordan sikres informasjonssikkerhet og personvern?
    - Om innebygd personvern?
9. **Vurdering av nødvendighet og forholdsmessighet**
    - Vurdering opp mot personvernprinsippene: Lovlighet, rettferdighet og åpenhet, Formålsbegrensning, Dataminimering, Riktighet, Lagringsbegrensning, Integritet og konfidensialitet
    - Er behandlingen nødvendig for formålet?
    - Er det mulig å oppnå formålet med mindre inngripende tiltak?

10. **Registrertes rettigheter**
    - Hvordan ivaretas retten til innsyn, retting, sletting og dataportabilitet m. m.?
    - Informasjon til de registrerte – hvordan og når?
    - Synspunkter fra interessentene (de registrerte m. m.)?
    - Vurderinger rundt de registrertes friheter (jf. EMK)?
11. **Overføring til tredjeland**
    - Overføres data utenfor EU/EØS?
    - Hvilke garantier er på plass (f.eks. standardkontrakter)?
12. **Konklusjon og anbefaling**
    - Er risikoen akseptabel?
    - Skal behandlingen gjennomføres som planlagt?
13. **Behandlingsansvarliges beslutning**
    - Ledelsens validering
    - Endelig vurdering og godkjenning av behandlingen.
    - Eventuelle krav om konsultasjon med Datatilsynet.

Bruken av **Microsoft 365 i skolen innebærer utvilsomt flere potensielle risikoer og risikoscenarioer relatert til elevenes personvern, som må vurderes grundig i DPIA-en**.

DPIA-en utgjør selvsagt hoved-leveransen fra det nasjonale prosjektet. Mye av det øvrige arbeidet består av innledende og forberedende vurderinger som må være på plass før man kan gå videre med selve sluttleveransen / den sentrale leveransen.

Noen momenter og vurderinger som jeg antar i mer eller mindre grad vil inngå i DPIA-biten:

1. Tilgangsstyring og informasjonssikkerhet

- **Uvedkommende får tilgang** til personopplysninger om elever (f. eks. via feilkonfigurerte delingstillatelser eller svak autentisering, og via eventuelle vellykkede eksterne dataangrep).
- **Elever og lærere får tilgang** til filer de ikke skal ha tilgang til (f. eks. feil i deling eller mapper med for brede rettigheter).
- Risiko for **snoking i elevmapper eller logger** (internt eller eksternt).

2. Bruk av tjenester og behandlingsansvar

- Microsoft 365 inneholder **både databehandler- og behandlingsansvarlig-tjenester**, noe som krever særskilt oppmerksomhet i DPIA-arbeidet.
- Tjenester hvor Microsoft er behandlingsansvarlig blir benyttet (f. eks. Copilot eller Bing Chat uten tilstrekkelig kontroll).
- Bruk av **tredjeparts-apper eller tillegg** uten DPIA eller vurdering av databehandleravtale.

3. Innhold og digital samhandling

- Elever får **tilgang til uønsket eller skadelig innhold** (f. eks. via søk, lenker eller tredjepartsapper).
- Via samskriving eller deling blir det **delt for mye eller sensitive personopplysninger**.
- **Bilder og/eller video med identifiserbare elever** blir delt eller spredt uten samtykke.

4. Pedagogisk og organisatorisk risiko / vurdering

- Skoleeier har ikke gjort nødvendige vurderinger av **ressursenes egnethet for bruk** i undervisning (f. eks. pedagogisk verdi, personvernkonsekvenser, behandlingsgrunnlag m. m.).
- Manglende **opplæring** av ansatte og elever i sikker bruk av M365-tjenester.
- Det kan være behov for en systematisk vurdering av **pedagogisk egnethet,** og ikke kun rette fokus mot det tekniske og juridiske. Vurderingene bør dokumenteres, f. eks. i form av en pedagogisk konsekvensanalyse eller som del av ROS/DPIA.

5. Sårbare grupper og barns rettigheter

- Behandling av personopplysninger om spesielt **sårbare elever** (f. eks. elever med spesialundervisning eller tilretteleggingsbehov) uten tilstrekkelig beskyttelse.
- Manglende vurdering av **barns særlige behov for personvern** og rett til informasjon på et forståelig nivå.

6. Logging og overvåking

- Omfanget av **logging og overvåking** av bruk (f. eks. aktivitetslogger, chatlogger, dokumenthistorikk) og risiko for overvåkning uten rettslig grunnlag.
- **Manglende transparens** overfor elever og foresatte om hva som logges og hvorfor.
- To typer logging kan forekomme: Teknisk logging (for sikkerhet og feilsøking) og brukerlogging (som kan oppleves som overvåkning), hvor det kan være behov for tydelig informasjon til elever og foresatte (spesielt om den sistnevnte loggingen).
- **Brukerlogging** kan være i strid med prinsippet om **proporsjonalitet**, særlig hvis elevene ikke er informert eller tiltakene ikke strengt tatt er nødvendige.

7. Dataminimering og formålsbegrensning

- **Innsamling og lagring av flere personopplysninger enn nødvendig** for formålet (f. eks. automatisk lagring av metadata, bruk av AI-funksjoner som samler inn kontekstuell informasjon).
- **Gjenbruk** av data til andre formål enn opprinnelig angitt (f. eks. analyse, utvikling eller tredjepartsbruk).
- **Automatisk generert innhold** (f. eks. forslag fra Copilot) **kan inneholde sensitive data**, og det er behov for å få mest mulig kontroll med dette (unngå dette).

8. Overføring av data til tredjeland

Risiko knyttet til **overføring av personopplysninger til land uten tilstrekkelig personvernbeskyttelse** (f. eks. USA), særlig ved bruk av skytjenester og KI-funksjoner.

9. Manglende kontroll og styring

- Skoleeier eller kommunen har **ikke tilstrekkelig kontroll over konfigurasjon, databehandleravtaler eller endringer i tjenestene**, noe som kan gå ut over personvernet til elevene.
- **Endringer i Microsofts vilkår eller funksjonalitet** skjer uten at skoleeier blir varslet eller får mulighet til å gjøre nye vurderinger.
- Det bør presiseres her at endringer i Microsofts vilkår og funksjonalitet ofte skjer uten forhåndsvarsling, og at dette kan svekke skoleeiers mulighet til å gjøre nye og oppdaterte vurderinger.
- Kommunen bør strengt tatt ha **rutiner for å overvåke endringer i vilkår og funksjonalitet**, hvor dette inngår som en del av **internkontrollen**.

10. KI-funksjoner og dataminimering

- Eventuelt: Foreta eksplisitt vurdering av **generativ KI/AI** (primært Copilot i vårt tilfelle) og risiko for utilsiktet datainnsamling og gjenbruk.
- Hva med **metadata og kontekstuell informasjon** som samles inn automatisk?

M365, DPIA og ROS. Illustrasjon generert av Microsoft Copilot.

Anbefalinger til skoleeier på tenant-området

Hovedanbefaling: Egen tenant for skole

Den beste og mest anbefalte løsningen er å etablere en **egen Microsoft 365-tenant for skole**, adskilt fra øvrig kommunal virksomhet. Dette gir en tydelig organisatorisk og teknisk separasjon («pottetett» skille), og er den løsningen som i størst grad ivaretar krav til informasjonssikkerhet og personvern – særlig med tanke på barn og unge som en særskilt sårbar gruppe.

Fordeler med egen tenant:

- Tydeligere skille mellom skole og øvrig kommunal virksomhet
- Bedre kontroll over tilgangsstyring og databehandling
- Forenkler etterlevelse av personvernlovgivning (GDPR)
- Reduserer risiko for utilsiktet deling eller tilgang

Merk: En slik løsning bryter noe med Microsofts generelle anbefalinger om én felles tenant for hele organisasjonen, og med plattformens grunntanke om åpenhet og samhandling. Dette må veies opp mot behovet for sikkerhet og kontroll.

Alternativ løsning: Felles tenant med strenge tiltak

Dersom det ikke er praktisk mulig å etablere egen tenant for skole, kan en **felles tenant** vurderes. Dette krever imidlertid:

- **Grundige risikovurderinger** med fokus på informasjonssikkerhet og personvern
- **Iverksetting av tydelige sikkerhetstiltak** for å redusere risiko til et akseptabelt nivå
- **Bevissthet rundt risikovillighet** og hva som anses som akseptabel restrisiko

Tiltak som bør vurderes:

- Bruk av Microsofts sikkerhetsløsninger (f. eks. A5/E5-lisenser på M365 eller tilleggspakker)
- **Information Barriers** for å hindre uønsket kommunikasjon og deling (segmentering av brukere, begrensning av søk og deling, adressebokfiltrering og -segmentering m. m.)
- Segmentering av brukere og roller
- Begrensninger i deling og samhandling på tvers av organisasjonsenheter

Dette alternativet blir nok i praksis den mest benyttede løsningen, ut fra en totalvurdering.

Fleksibilitet og tilpasning

Andre tenant-oppsett kan også vurderes, for eksempel hybridløsninger eller delvis separasjon, **forutsatt at det gjennomføres grundige kartlegginger og innføres egnede sikringstiltak**.

Oppsummering

Modell	Fordeler	Ulemper
Egen tenant for skole	Høy sikkerhet, tydelig skille, bedre personvern	Mer kompleks drift, bryter med Microsofts anbefaling
Felles tenant	Enklere drift, bedre samhandling	Krever omfattende sikkerhetstiltak og risikohåndtering

Generelt: Bruken av Microsoft 365 i skolen krever omfattende vurderinger og bevisste valg for å sikre elevenes personvern. M365 er en kompleks og inngripende løsning, og det er urealistisk å forvente at leverandøren har ivaretatt personvernet tilstrekkelig gjennom standardinnstillinger alene. Tenant-problematikken er kun en liten brikke i det store bildet relatert til personvernet og informasjonssikkerheten til skoleelevene.

Min uttreden fra det nasjonale prosjektet

Mer om min uttreden fra det nasjonale prosjektet:

Jeg valgte å engasjere meg (mot betaling / frikjøp, inntil 20 %) innenfor KS SkoleSec-prosjektet **Nasjonal DPIA for Microsoft 365 (skole)**. Avtale ble inngått mellom meg, KS og Kinn kommune, og jeg fikk lov til å være del av prosjektet i perioden 24.02.2025-04.08.2025.

Snipp, snapp, snute – etter ca. 5 måneder som prosjektmedarbeider var jeg ute. Jeg har blitt «fristilt» fra prosjektet (les: «sparket»), mot min vilje. Tydeligvis var de ikke fornøyd med min innsats og framdrift. Gruppas manglende samarbeidsevne kan vel kanskje også ha vært noe av begrunnelsen, og muligens var jeg ikke aktiv nok i fellessamlinger.

KS sine til tider noe diffuse tilbakemeldinger, uklare forventninger, uklar bestilling (mandat) og tidvis mangelfulle veiledning gjorde det ikke akkurat enkelt å treffe mål eller blink. Min bruk av KI til idemyldring og språkvask var visstnok heller ikke helt stuerent, ifølge KS SkoleSec. Det er skuffende at det endte slik – for prosjektet var faktisk utrolig interessant mens det varte. Og jeg hadde så gjerne vært med videre.

Jeg bidro med omfattende tekst og refleksjoner inn i prosjektet. Selv om mye av dette sannsynligvis ikke ble videreført i den endelige versjonen, har prosessen gitt meg verdifull innsikt. Jeg har lært mye og hatt anledning til å delta i interessante møter med eksterne aktører som Datatilsynet, Microsoft og flere kommuner. I fortsettelsen blir det å følge prosjekter helt fra sidelinjen, som en ren bivåner (titter).

I og med min uttreden av prosjektet er alt skrevet i dette innlegget mine personlige tanker og vurderinger, som ikke nødvendigvis vil samsvare med de føringer og innspill som vil komme fra det nasjonale prosjektet.

Selv har jeg latt meg fascinere av de muligheter KI gir, så det føltes ganske naturlig å spørre KI til råds om hvordan min presentasjon som du nå leser framstår (lenke til PDF-fil): M365 Copilot KI sin vurdering av mitt innlegg. Selvsagt skal man ta KI sin vurdering med en klype salt – det er tross alt en maskinell og automatisert (matematisk) behandling, og ikke en menneskelig vurdering / fagfellevurdering.

Avsluttende kommentarer

Oppsett av tenant-struktur i Microsoft 365 for skolesektoren er et komplekst og sensitivt område, særlig med tanke på behandling av personopplysninger til **sårbare barn og unge**. Valg av løsning må baseres på **en helhetlig vurdering av tekniske, organisatoriske og juridiske forhold**.

Selv om en felles tenant-løsning kan være forsvarlig ved korrekt bruk av sikkerhetsinnstillinger og tilgangsstyring, er det avgjørende at hver enkelt kommune eller skoleeier gjennomfører **grundige risikovurderinger** og etterfølgende **sikringstiltak**. Disse vurderingene må ta utgangspunkt i **lokal kontekst, risikoappetitt og akseptabelt risikonivå**.

Til syvende og sist er det tydelig at **systematiske og grundige risikovurderinger og målrettede sikringstiltak** er avgjørende for å redusere **restrisiko** og sikre forsvarlig bruk av skytjenester. Forutsatt at slike vurderinger er gjennomført og nødvendige tiltak er iverksatt, kan **ulike varianter av tenant-oppsett være akseptable** og tilpasses lokale behov og forhold.

Rent generelt: **Bruk av Microsoft 365** i skole og kommune **kan være forsvarlig med hensyn til personvern og informasjonssikkerhet**, forutsatt at grundige **analyser** gjennomføres, nødvendige **tiltak** settes i verk og løsningen **følges opp kontinuerlig**. Dette innebærer både **tekniske og organisatoriske tiltak**, **bevisstgjøring** og **opplæring** av ansatte og elever, samt **involvering** av relevante aktører, i tillegg til etterlevelse av **GDPR** (personvernforordningen) og **nasjonale føringer**. **Restrisikoen** kan da bringes ned til et **akseptabelt nivå**, slik at selv for sårbare grupper som elever kan M365 benyttes som et forsvarlig og produktivt IKT-verktøy i opplæringen. Dette er ikke en engangsøvelse, men en **kontinuerlig prosess** som krever oppfølging og forbedring over tid.

Lenker

Mer informasjon og relevante lenker:

- KS: SkoleSec (prosjekt for å styrke arbeidet med personvern og informasjonssikkerhet knyttet til digitalt læringsmiljøer)
- KS (SkoleSec): Nasjonal DPIA for Microsoft 365 | KS starter arbeidet med å gjennomføre en nasjonal vurdering av personvernkonsekvenser (DPIA) for Microsoft 365 etter modell fra DPIAen for bruk av Google Workspace for Education i skolen.

- KS (SkoleSec): Ny nasjonal personvernkonsekvensvurdering for bruk av Google Workspace for Education i skolen
- KS: Anbefalte felles sikkerhetskrav for kommunal sektor | Trygg digitalisering er en forutsetning for at kommunene skal kunne levere tjenester til alle innbyggere, nå og i fremtiden. | Rammeverk for trygg digitalisering (RTD)
- Utdanningsdirektoratet (Udir): Personvern (GDPR) for barnehage og skole
- Kinn kommune: Personvern og personvernerklæringar
- Microsoft Learn (Tips: Søk f. eks. etter tenant)
- Microsoft: Privacy at Microsoft | Your data is private at work, at home, and on the go
- Microsoft: Microsoft 365 Copilot (Office) – innlogging og produktoversikt
- Kinn kommune: Handlingsplan for bruk av kunstig intelligens (KI)
- KiNS (Foreningen kommunal informasjonssikkerhet)

Datatilsynet:

- Datatilsynet (Norges uavhengige tilsynsmyndighet for personvern)
- Datatilsynet: Barn, unge og skole | Personvern
- Datatilsynet: Funn fra tilsyn med personvernet i skolen (2025)
- NRK Vestfold og Telemark (mai 2025): Datatilsynet slår alarm: – Utgjør en stor trussel for personvernet til barn og unge | Elever blir utsatt for målrettet reklame og er lykkelig uvitende om personopplysninger som kommer på avveier.
- Datatilsynet: Virksomhetens plikter
- Datatilsynet: NTNU, sluttrapport: Copilot med personvernbriller på

Standarder, maler, lovverk m. m.:

- NSM: Grunnprinsipper for IKT-sikkerhet
- Lovdata: Lov om behandling av personopplysninger (personopplysningsloven) m/forordning (EU)
- Standard Norge: Ledelsessystemer for informasjonssikkerhet – ISO/IEC 27001
- Standard Norge: Informasjonssikkerhetstiltak – NS-EN ISO/IEC 27002
- KiNS verktøykasse (DPIA-mal, styringssystem m. m.)

Flere mer eller mindre relevante Microsoft-lenker relatert til personvern, DPIA og sikkerhet (+ tenant) i M365 innenfor skole og utdanning:

- Microsoft Education: Microsoft 365 for Education Cybersecurity Solutions
- Microsoft: Oversikt over EUs personvernforordning (GDPR) | Beskytt individuelt personvern med skytjenestene fra Microsoft
- Microsoft Learn: Administrer personvern og beskyttelse – Microsoft Priva og Microsoft Purview
- Microsoft Learn: Microsoft Purview Compliance Manager
- Microsoft: Data Protection with Microsoft Privacy Principles | Microsoft Trust Center
- Microsoft Learn: Guidance for Data Controllers using Office 365 – Microsoft GDPR
- Microsoft Learn: Data protection impact assessments – Microsoft GDPR

- Microsoft: Download Customizable DPIA document from Official Microsoft Download Center
- Microsoft Learn: Tenant setup for Microsoft 365 for education baseline – M365 Education

Egne blogg-skriverier:

- blogg.brr.no: Datamaskiner (PC) og IKT i skolen
- blogg.brr.no: Notater relatert til Microsoft 365 og Teams
- blogg.brr.no: Microsoft 365 Family (delvis i skyen)
- blogg.brr.no: Skyen («Cloud Computing», nettsky)
- blogg.brr.no: Informasjonssikkerhet og cybersikkerhet
- blogg.brr.no: Personvern, informasjonssikkerhet, internkontroll
- blogg.brr.no: Nettvett og digital mobbing – barn og unge
- blogg.brr.no: Digitalisering av kommunal sektor
- blogg.brr.no: Kommunikasjonsmodellen
- blogg.brr.no: Tag/etikett personvern (andre skriverier her i bloggen om personvern)
- BRR sin testblogg!: Bruken av M365 i skole – og personvernet

 PDF-fil  Utskriftsvennlig versjon