FUNN FRA SKOLETILSYNET

Samlerapport fra Datatilsynets brevkontroll med skolesektoren.

Mai 2025

Datatilsynet

Innhold

Del 1 – Om prosjektet og arbeidsmetodikken

Datatilsynet har gjennomført et større antall tilsyn med norske kommuners etterlevelse av personvernforordningens krav innenfor skolesektoren. Vi har kontrollert kommunenes ivaretakelse av krav til personvern og personopplysningssikkerhet i digitale læringsverktøy for opplæringsformål i skolen.

Datatilsynet sendte den 14. januar 2025 ut likelydende brevkontroller til 50 kommuner, hvor vi ba om en redegjørelse av nærmere angitte tema innenfor personvern og personopplysningssikkerhet.

Denne rapporten er en samlet tilsynsrapport for alle de 50 brevkontrollene, og den er basert på de besvarelsene vi har mottatt. Rapporten inneholder beskrivelse av personvernregelverkets krav, oppsummering av besvarelsene vi har mottatt og relevant veiledning om temaene vi har undersøkt.

Datatilsynet gjennomførte stedlige tilsyn med fire kommuner i mars og april 2025, med samme tema som brevkontrollene. Formålet med de stedlige tilsynene var å nærmere kontrollere etterlevelse av personvernregelverket i praksis. I den forbindelse besøkte vi også fire barne- og ungdomsskoler for å kontrollere om det var samsvar mellom hva kommuneledelsen ga uttrykk for og hva som faktisk skjer i praksis på skolene. Det utarbeides individuelle tilsynsrapporter for disse tilsynene.

1. Bakgrunnen for skoletilsynet

De siste ti årene har det skjedd en digital omvelting av skolesektoren. I dag har nesten alle norske elever tilgang på hver sin digitale enhet, og undervisningen er i stor grad understøttet av digitale hjelpemidler. Det benyttes mange ulike digitale læringsverktøy som tilbys av forskjellige private aktører. Dette har ført til at det behandles flere personopplysninger i skolen i dag, i forhold til tidligere da man brukte tavle, kritt og lærebøker. Personopplysningene som samles inn kan gi et omfattende og detaljert bilde av den enkelte elevs faglige og sosial atferd gjennom hele skolegangen.

Personvernkommisjonens rapport fra 2022 beskriver utførlig hvilke utfordringer personvernet møter i skolen i dag. Der understrekes det at digitaliseringen av skolen har skjedd svært raskt uten at roller og ansvar for personvernarbeidet, eller konsekvenser for barns personvern, er drøftet i tilfredsstillende grad.[1] Mangel på tilstrekkelige sentrale føringer, i kombinasjon med varierende grad av kompetanse og ressurser ute i kommunene, medfører en risiko for at tjenesteleverandører kan legge premissene for hvordan elevenes personvern ivaretas i skolen.

Samtidig har barn et særskilt krav på beskyttelse av sine rettigheter og friheter, herunder retten til personvern. Den enkelte elev er i dag prisgitt at kommunen eleven går på skole i gjør de nødvendige vurderingene av digitale læringsverktøy som tas i bruk og at de tar beslutninger som ikke bryter med personvernregelverket.

Kommunene må sørge for å ha kontroll på ansvarsforholdene mellom kommune og leverandør, ha en oversikt over hvilke personopplysninger som behandles i tjenestene, og sørge for at uvedkommende ikke får tilgang til personopplysningene til elevene. Dette er en krevende jobb. Gjennomføring av

[1] Personvernkommisjonens rapport, NOU 2022: 11, kapittel 8.4, https://www.regjeringen.no/contentassets/e4c60a6c51b147628b2c2e55db7e08e3/no/pdfs/nou20222022001 1000dddpdfs.pdf

risikovurderinger er tidkrevende og forutsetter både teknisk og juridisk kompetanse. De fleste kommuner har begrensede midler og kompetanse å avsette til personvernarbeidet.

Det overordene formålet med tilsynsarbeidet er å forbedre personvernet i skolen gjennom å lage relevant og praktisk veiledning for kommunene knyttet til arbeidet med personvern i skolen. Med både tilsynet og samlerapporten ønsker vi å bidra til å gjøre kommunene bedre rustet til å ivareta elevenes personvern.

2. Hjemmel for tilsynene

Tilsynene ble gjennomført med hjemmel i personvernforordningen artikkel 58 nr. 1. Bestemmelsens bokstav a gir Datatilsynet myndighet til å pålegge behandlingsansvarlige å fremlegge all informasjon som er nødvendig for at Datatilsynet skal kunne utføre sine oppgaver.

Gjennom tilsynet har vi kontrollert kommunens tekniske og organisatoriske tiltak for å ivareta personvern og personopplysningssikkerhet i digitale læringsverktøy for opplæringsformål, herunder kommunens gjeldende retningslinjer. Dette er forpliktelser som følger av personvernforordningen artikkel 24 nr. 1 og 2 og artikkel 32.

3. Gjennomføringen av brevkontroller og tilsyn

Tilsynsarbeidet ble gjennomført i to faser. Den første fasen ble gjennomført som en brevkontroll hvor et større antall kommuner ble pålagt å svare på spørsmål om etterlevelse av konkrete plikter etter personvernregelverket. Brevkontrollen bestod av et krav om redegjørelse som var obligatorisk for kommunene å svare ut, i tillegg til tre frivillige spørsmål.

Kommunene ble gitt en frist på litt over 3 uker til å besvare kravet om redegjørelse fra Datatilsynet. Alle 50 kommuner besvarte brevkontrollen innen fristen 7. februar 2025.

I den andre fasen ble det gjennomført stedlige tilsyn med fire kommuner i løpet av mars og april 2025, med samme tema som brevkontrollene. I denne fasen av tilsynsarbeidet var formålet å nærmere kontrollere etterlevelse av kommunens plikter i praksis. De fire kommunene ble valgt ut basert på et representativt utvalg ut fra besvarelsene vi mottok i brevkontrollene, både de med godt dokumenterte rutiner, og de som etterlot et inntrykk av mangler eller avvik. Vi valgte også kommuner ut ifra ulik størrelse og innbyggertall. Datatilsynet vil utarbeide individuelle tilsynsrapporter for de stedlige tilsynene, og funnene fra de stedlige tilsynene er ikke er en del av denne samlerapporten.

4. Datatilsynets krav om redegjørelse

Datatilsynet ba om å få tilsendt følgende beskrivelse og dokumentasjon av følgende:

1. **Kommuneledelsens overordnede ansvar**
   En oversikt over kommunens relevante rutiner/retningslinjer/policy for innkjøp og implementering av digitale læringsverktøy, herunder:
   a. En oversikt over rutinene
   b. Rutine for gjennomføring av risikovurderinger
   c. Rutine for gjennomføring av personvernkonsekvensvurderinger (DPIA)
   d. Rutine for inngåelse av databehandleravtaler

2. **Gjennomførende rutiner**
   En lærer ønsker å ta i bruk et nytt digitalt læringsverktøy i undervisningen. Legg ved

kommunens relevant(e) rutine(r) for, og/eller beskrivelser av, prosessen frem til verktøyet eventuelt kan tas i bruk. Beskriv hvordan denne prosessen blir kommunisert til ansatte ved skolene.

3. **Oversikt over digitale læringsverktøy**
   Beskriv hvordan kommunen holder oversikt over alle digitale læringsverktøy som er i bruk i skolene i deres kommune. Last opp eventuell oversikt, for eksempel utdrag fra behandlingsprotokoll.

4. **Administrasjon av ordinær drift og vedlikehold**
   Beskriv hvordan kommunen administrerer de digitale læringsverktøyene som allerede er implementert og tatt i bruk.
   a. Gi en liste over roller på skolen eller i kommunen som har brukerrettigheter i operativsystemet for å administrere enhetsinnstillinger.
   b. Redegjør for hvilke roller som har ansvar for ordinær drift av digitale læringsverktøy, for å følge opp samt implementere oppdateringer.
   c. Legg ved kommunens rutiner for operativ drift, vedlikehold samt opphør av programvarelisens knyttet til digitale læringsverktøy.

5. **Leverandørenes viderebruk av elevers personopplysninger**
   Redegjør for hvilke tekniske og organisatoriske tiltak dere har iverksatt for å hindre at elevenes personopplysninger behandles til formål utenfor opplæringslovens anvendelsesområde. Dette er eksempelvis behandling av personopplysninger til leverandørene av digitale læringsverktøy sine egne formål (kommersielle formål, videreutvikling av leverandørens tjenester og analyse).

5. Avklaringer og begreper

5.1 Begrepet digitale læringsverktøy

I brevkontrollen presiserte vi at begrepet «digitale læringsverktøy» skulle forstås å omfatte både digitale læringsressurser og læringsplattformer som brukes til undervisningsformål. Dette inkluderer både betalte- og gratisverktøy, applikasjoner installert lokalt i utstyret til kommunen og bruk av webapplikasjoner. En læringsplattform er et system som gir mulighet for kommunikasjon, bruk av skrive- og presentasjonsverktøy samt nettnavigasjon. De største læringsplattformene som er i bruk i dag er Microsoft 365, Google Workspace for Education og Apple Classroom. Applikasjoner lastes ned på elevenes enhet for bruk i undervisningen og kan være lisensbasert eller gratis. Et eksempel på en nettbasert tjeneste er digitale lærerbøker fra Cappelen Damm, Aschehoug og Gyldendal, Campus Matte, Google søk, Youtube mm.

Vi avgrenset tilsynet mot digitale verktøy som benyttes til administrasjon, herunder tekniske støtteverktøy, skoleadministrasjon, kommunikasjon mellom skole og foresatte og evalueringssystemer. Dette er eksempelvis tjenester for identitetshåndtering, skoleadministrative løsninger som Visma og Vigilo, kommunikasjonsløsninger som Zoom, Showbie og Fronter, og evalueringssystemer som brukes til evaluering og karaktersetting, tilpasset opplæring og elevundersøkelser, som for eksempel ItsLearning, Canvas og Showbie.

5.2 Hva er en personopplysning?

Personvernforordningen gjelder ved helt eller delvis automatisert behandling av personopplysninger, jf. personopplysningsloven § 2. Personvernforordningen artikkel 4 nr. 1 definerer «personopplysninger» som enhver opplysning om en identifisert eller identifiserbar fysisk person. En identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske fysiologiske genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet. Begrepet skal etter rettspraksis tillegges en vid tolkning.[2]

Eksempler på personopplysninger som behandles i digitale læringsverktøy er:

- Informasjon for opprettelse av bruker, herunder navn, bilde, kontaktopplysninger, kjønn og alder.
- Opplysninger om faglige prestasjoner og resultater som brukes for å tilpasse tjenesten til den enkelte elev.
- Informasjon om atferd ved bruk av læringsverktøyet.
- Mange av applikasjonene har tilgang til kamera, mikrofon, bildebibliotek, geolokasjon, kontakter mm.
- En IP-adresse anses som personopplysning fordi den kan spores tilbake til en bestemt maskinvare og dermed til en enkeltperson. Personopplysninger som er blitt pseudonymisert, og som kan knyttes til en fysisk person ved hjelp av tilleggsopplysninger, skal anses som opplysninger om en identifiserbar fysisk person.
- Sporingsteknologi i applikasjonene kan samle inn opplysninger om geolokasjon, enhetsidentifikatorer, interesser og brukerhistorikk.
- Nettbaserte digitale læringsverktøy som ikke krever innlogging kan behandle personopplysninger i form av IP-adresser, geolokasjon, brukerens atferd, opplysninger i fritekstfelt mm.

IP-adresse

En IP-adresse (Internet Protocol address) er en unik identifikator eller adresse som blir tildelt en enhet, for eksempel en PC eller nettbrett, for at de skal kunne skilles fra hverandre på internett.[1] Dette regnes normalt som en personopplysning fordi informasjonen ofte kan knyttes til en enkeltperson, jf. personvernforordningen artikkel 4 nr. 1.

[2] Begrepet personopplysninger skal etter rettspraksis tillegges en vid tolkning, se blant annet EU-domstolens dom i sak C-582/14 Patrick Breyer v Bundesrepublik Deutschland. I denne dommen la retten til grunn at det må foretas en vurdering av risikoen for at en fysisk person kan identifiseres, der det avgjørende spørsmålet er om det er rimelig sannsynlig at kombinasjonen av informasjonen kan brukes til å identifisere en enkeltperson. Retten la vekt på at det må vurderes om det kreves en uforholdsmessig stor innsats i form av tid, kostnader eller arbeidsinnsats for å identifisere en enkeltperson. For Norge er ikke EU-domstolens praksis direkte bindende. Rettspraksis fra EU-domstolen vil likevel ha betydning på personvernområdet ettersom det er en grunnleggende forutsetning at personvernforordningens regler forstås og praktiseres likt i hele EU/EØS.

Personopplysninger er dermed ikke bare opplysninger om navn, kontaktinformasjon eller elevens identifikatorer som brukes på skolen. Opplysninger som kan knyttes til identifikatorer som hører til enheten som brukes, identifikatorer knyttet til informasjonskapsler (cookies) og øvrige sporingsteknologier, IP-adresse eller øvrige nettidentifikatorer, vil normalt også utgjøre personopplysninger.

5.3 Kommunen som behandlingsansvarlig

Som skoleeier er den enkelte kommune behandlingsansvarlig for alle behandlingsaktiviteter som foregår i den offentlige grunnskolen. Uavhengig av hvor mange innbyggere som bor i kommunen eller hvordan kommunen er organisert, er det overordnede ansvaret for behandlingen av personopplysninger tillagt kommuneledelsen. Dette gjelder også i tilfeller hvor kommunen inngår i et interkommunalt samarbeid med andre kommuner eller har en vertskommune som bistår kommunen. Det er fremdeles kommuneledelsen som sitter med behandlingsansvaret etter personvernregelverket.

Brevkontrollene var rettet mot kommuneledelsen sentralt, og ikke den enkelte skole. Når vi i denne samlerapporten omtaler «kommunen» eller «skoleeier» menes det kommunen sentralt og kommuneledelsen.

Vi ser at flere kommuner har inngått interkommunalt samarbeid om ansvaret knyttet til digitale læringsverktøy i skolen. Kommunene har i utgangspunktet stor frihet til å velge hvordan de skal samarbeide, selv om kommuneloven setter noen begrensninger og personvernforordningen krever at fordelingen av ansvar og oppgaver skal være tydelig regulert.

Datatilsynet ser at det å etablere IKT-samarbeid kan ha store fordeler, men det forutsetter at den enkelte kommune er sitt ansvar bevisst, og ikke i for stor grad støtter seg på hva de samarbeidende kommunene gjør. Behandlingsansvaret forblir hos den enkelte kommunen. Se punkt 12.3.2 for eksempler på hvordan enkelte av kommunene har organisert seg i interkommunale IKT-samarbeid.

5.4 Feide er en innloggingsløsning og ikke godkjenningsordning

Gjennom tilsynet har vi sett at mange kommuner har en misoppfatning om at Feide innebærer en godkjenningsordning og at personvernet er ivaretatt i de digitale læringsverktøyene som bruker Feide.

Feide står for Felles Elektronisk Identitet og er en sentralisert innloggingsløsning med tofaktorautentisering. Det er SIKT sammen med Utdanningsdirektoratet som forvalter Feide-løsningen. Det lages en unik elektronisk identitet for hver enkelt elev som brukes som legitimasjon overfor ulike bibliotek, nettsteder og digitale tjenester innenfor utdanningssektoren. I følge SIKT var det 450 tjenester som benyttet Feide-pålogging i grunnskolen i 2024 med 127 millioner innlogginger i 550 kommuner.
For at et digitalt læringsverktøy skal få tilgang til Feide-innlogging, stiller SIKT krav til at tjenesten tilfører en verdi innenfor forskning- og utdanningssektoren. I tillegg er kommunen gjennom avtalen med Feide forpliktet til å inngå databehandleravtaler med leverandørene av de enkelte tjenestene. SIKT garanterer imidlertid ikke for at personvernet ivaretas i de enkelte tjenestene som bruker påloggingsløsningen og undersøker heller ikke hva de underliggende databehandleravtalene inneholder.

Det er kommunene som er ansvarlig for å vurdere om personopplysningene som behandles i tjenestene er nødvendig for formålet, at det inngås databehandleravtaler og at det gjennomføres risikovurderinger.

6. Om samlerapporten

Datatilsynet har i rapporten vist til de relevante rettsreglene som regulerer de konkrete temaene vi undersøkte i tilsynene. Vi har i tillegg hatt som mål å gi veiledning om hva pliktene som følger av rettsreglene innebærer i praksis.

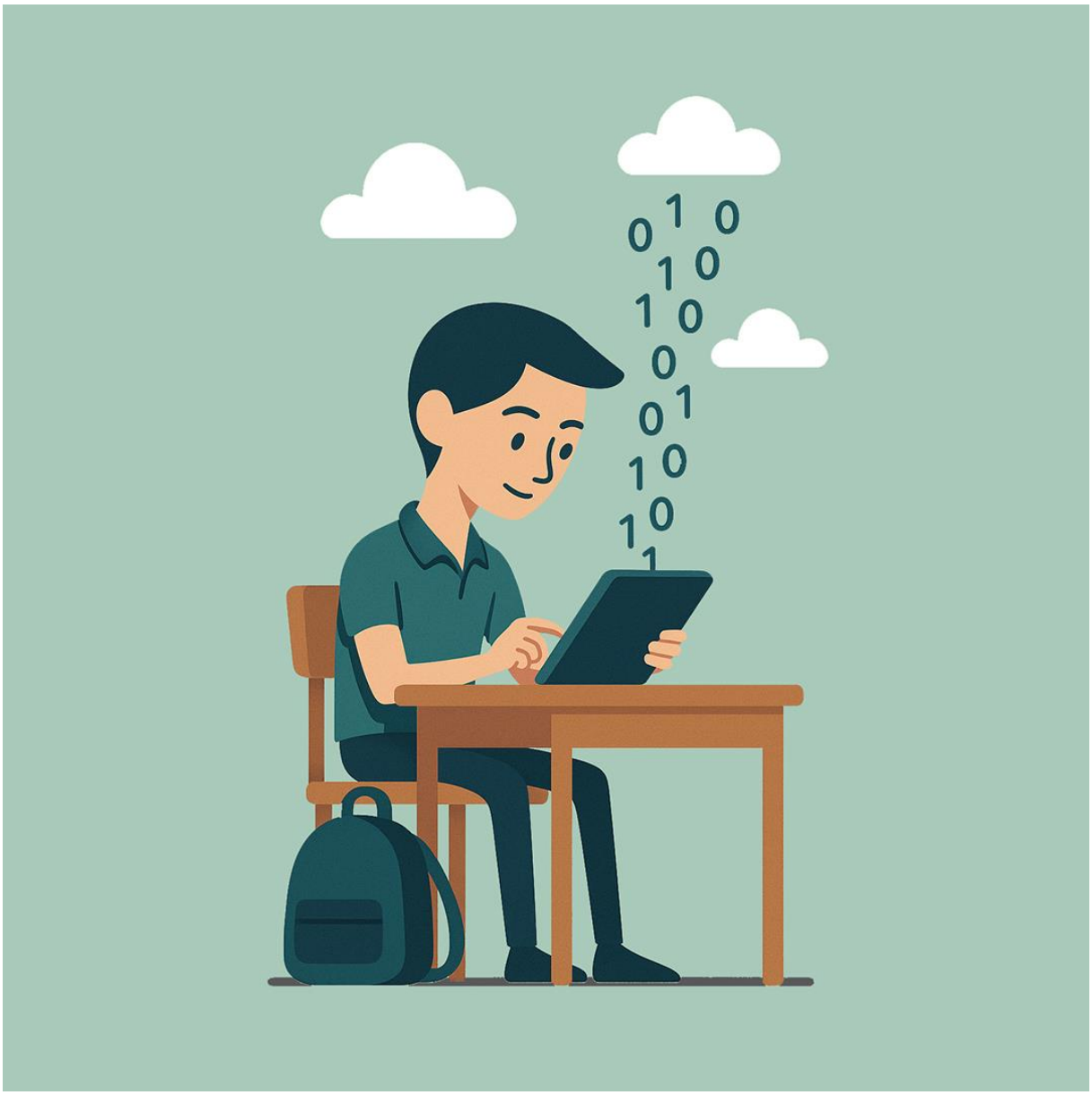
Det overordnede formålet med tilsynsarbeidet har vært å gi kommunene praktisk og konkret veiledning om personvernregelverkets krav ved bruk av digitale læringsverktøy til opplæringsformål.

Rapporten vil i det følgende presentere hvert tema vi har vurdert under brevkontrollene og trekke frem relevante funn fra besvarelsene. Vi vil også peke på tendenser der det er mulig. Knyttet til de forskjellige temaene i rapporten vil vi vise til konkrete anonyme eksempler fra besvarelsene i brevkontrollen. Formålet er å gi gode eksempler på etterlevelse av regelverkets krav og manglende etterlevelse.

Det er utarbeidet omfattende veiledning med god kvalitet av forskjellige aktører på personvernområdet. Datatilsynet har likevel et klart inntrykk av at det er utfordrende for kommuner å navigere i dette landskapet og finne relevant og kvalitetssikret veiledning på de forskjellige kravene personvernregelverket stiller opp. Datatilsynet har derfor hatt som mål å vise til konkret veiledning innenfor de spesifikke områdene vi har kontrollert.

For å begrense omfanget, har vi valgt å vise til konkret veiledning fra anerkjente veiledningsaktører, som har solid kompetanse og erfaring. Aktørene har også etablerte samarbeid med kommunene, og de har kunnskap om kommunene som gjør veiledningen målrettet. Vi har vist til veiledning fra KS, Digitaliseringsdirektoratet, Nasjonal sikkerhetsmyndighet, Foreningen Kommunal Informasjonssikkerhet (KiNS) og Datatilsynets nettside. Vi tar imidlertid et forbehold om at Datatilsynet ikke har kvalitetssikret alt som fremkommer av veiledningsmaterialet vi viser til.

Del 2 – Datatilsynets brevkontroll



7. Oppsummering av hovedfunn

Brevkontrollen viser at det er betydelige forskjeller mellom kommunene når det gjelder ivaretakelse av personvern og personopplysningssikkerhet i digitale læringsverktøy. Det gjøres en del bra arbeid for å ivareta elevenes personvern og et stort flertall av kommunene har «sentraliserte vurderinger» før det tas i bruk nye digitale læringsverktøy. Brevkontrollen avdekker imidlertid flere avvik og utfordringer for personvernet til elevene. Nedenfor har vi trukket frem syv hovedfunn fra brevkontrollen:

Syv hovedfunn:

1. **Feil forståelse av hva som er personopplysninger**
   Det er uklart for mange kommuner hva som regnes som personopplysninger, der mange legger til grunn en for snever forståelse av hva som utgjør en personopplysning. Konsekvensen av en feil forståelse er at kommunene ikke anser at personvernregelverket kommer til anvendelse for en del digitale læringsverktøy som faktisk behandler personopplysninger. Dette gjelder særlig gratistjenester og nettbaserte tjenester som ikke krever innlogging. I praksis innebærer dette at hundrevis av digitale læringsverktøy ikke blir risikovurdert, og omfattes ikke av kommunens samlede oversikt over behandlingsaktiviteter.

2. **Mangelfulle rutiner**
   Mange kommuner har ikke gode nok rutiner på plass for å ivareta personvernregelverkets krav til bruk av digitale læringsverktøy. Det mangler særlig tydelig oversikt over roller og ansvar, føringer for når det kreves en risiko- og sårbarhetsanalyse og gjennomføring av DPIA. En del kommuner har ikke systematikk for styring av personvernarbeidet, eksempelvis føring av behandlingsprotokoll og inngåelse av databehandleravtaler. Vi ser at gjennomføringen av disse forpliktelsene ofte er vilkårlig og personavhengig.

3. **Digitale læringsverktøy tas ofte i bruk på bakgrunn av en beslutning av rektor eller lærer**
   Flere digitale læringsverktøy vurderes ikke av kommunen sentralt. Dette gjelder særlig for gratisverktøy og nettbaserte tjenester der det ikke kreves innlogging. For verktøy som ikke koster penger ser vi en tendens til at kommunen sentralt ikke involveres på samme måte som når det innebærerkostnader eller kreves lisens. Manglende forståelse av at det behandles personopplysninger i tjenestene påvirker hvilket ansvar kommunen velger å ta.

4. **Mange misforstår hva Feide innebærer**
   Feide står for Felles Elektronisk Identitet og er en sentralisert innloggingsløsning med tofaktorautentisering. At et digitalt læringsverktøy har Feide-innlogging blir av mange kommuner oppfattet som en godkjenningsordning og at personvernet er ivaretatt. Personvernet i tjenesten er imidlertid ikke vurdert og kommunene er selvstendig ansvarlig for å gjøre nødvendige vurderinger av personvernet.

5. **IKT-oppgaver ivaretas av roller uten tilstrekkelig kompetanse**
   Vi ser at enkelte kommuner har delegert teknisk ansvar for administrasjon og forvaltning av enheter og brukertilganger til roller som ikke har tilstrekkelig kompetanse innenfor IKT, informasjonssikkerhet og personvern. I enkelte kommuner finner vi eksempler på at dette ansvaret er lagt til lærere eller rektor.

6. **Fordeler ved interkommunale samarbeid**
   Kommuner som er en del av et interkommunalt IKT-samarbeid har i større grad skriftlige rutiner og kvalifiserte personer som utfører oppgaver av teknisk karakter. Disse har også bedre oversikt over hvilket ansvar som ligger til hvilke roller.

7. **Mange forholder seg ikke til om leverandører bruker personopplysninger til sine egne formål**
   Mange digitale læringsverktøy leveres av private aktører som har forretningsmodeller som baserer seg på innsamling, bruk og deling av personopplysninger. Dersom elevenes personopplysninger tilgjengeliggjøres for kommersielle formål eller for videreutvikling av leverandørens egne tjenester, er ikke dette forenelig med opplæringslova og personvernforordningen. Mange kommuner er ikke klar over denne problemstillingen og har derfor ikke iverksatt tilstrekkelige tiltak.

8. Kommuneledelsens overordnede ansvar

8.1 Datatilsynets krav om redegjørelse

Det første spørsmålet i brevkontrollen handlet om kommuneledelsens overordnede ansvar for å etablere en velfungerende internkontroll (også kalt styringssystem, rammeverk eller kvalitetssystem e.l), med særlig fokus på rutiner for risikovurdering, DPIA og databehandleravtaler innenfor kontrollens tema.

Vi ba kommunene legge ved en oversikt over relevante rutiner/retningslinjer/policyer for innkjøp og implementering av digitale læringsverktøy:

a) En oversikt over rutinene
b) Rutine(r) for gjennomføring av risikovurderinger
c) Rutine(r) for gjennomføring av DPIA
d) Rutine(r) for inngåelse av databehandleravtaler

Hensikten med spørsmålet var at vi skulle få et bedre innblikk i hvordan kommuneledelsen ivaretar sitt overordnede ansvar ved bruk av styrende rutiner i forbindelse med innføring av digitale læringsverktøy i skolen. Slike rutiner skal bidra til at kommunen har en systematisk og konsistent tilnærming til arbeidet med risikovurderinger, DPIA og databehandleravtaler. Styrende rutiner retter seg i stor grad mot ledelsen, herunder hvilke beslutninger og føringer de legger for virksomhetens internkontroll.[3]

Med «risikovurderinger» mener vi risiko- og sårbarhetsanalyser.

[3] Les mer om styringssystem i veilederen «Etablere internkontroll» på Datatilsynets hjemmeside: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/

For enkelthets skyld omtales rutiner/retningslinjer/policyer som «rutiner» i denne rapporten. Rutinene kan være retningslinjer, prosedyrer eller standarder som gir veiledning for hvordan oppgaver skal utføres og hvilke krav som skal overholdes.

8.2 Relevante rettsregler

8.2.1 Ansvarlighet

Det følger av ansvarsprinsippet i personvernforordningen artikkel 5 nr. 2 at den behandlingsansvarlige har ansvar for å sikre at de grunnleggende prinsippene for behandling av personopplysninger overholdes og at dette kan påvises.

Ansvarsprinsippet innebærer at den behandlingsansvarlige må gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med regelverket, jf. personvernforordningen artikkel 24 nr. 1.

Som skoleeier er den enkelte kommune behandlingsansvarlig for alle behandlingsaktiviteter som foregår i den offentlige grunnskolen.

Uavhengig av hvor mange innbyggere som bor i kommunen eller hvordan kommunen er organisert, er det overordnede ansvaret for behandlingen av personopplysninger tillagt kommuneledelsen. Dette gjelder også i tilfeller hvor kommunen inngår i et interkommunalt samarbeid med andre kommuner eller har en vertskommune som bistår kommunen – det er ikke mulig å avtale seg bort fra behandlingsansvaret.

8.2.2 Krav til internkontroll

Tekniske og organisatoriske tiltak omtales ofte som internkontroll, styringssystem eller rammeverk. Rammeverket skal være ledelsens verktøy for å ivareta sitt ansvar og for å kunne demonstrere etterlevelse etter personvernregelverket i sin organisasjon. Tiltakene skal også være de ansattes verktøy for å utføre oppgaver på en forsvarlig og sikker måte.

Regelverket legger opp til en viss skjønnsmargin knyttet til hva som kreves av styringssystemet, ettersom det «skal stå i et rimelig forhold til behandlingsaktivitetene». Det er opp til den behandlingsansvarlige å sikre at systemet er egnet til å oppfylle hensikten med det innenfor den aktuelle virksomheten.

Norske kommuner har en kompleks organisasjonsform med mange underliggende enheter innenfor forskjellige ansvarsområder. Øverste leder er behandlingsansvarlig etter personvernregelverket. En velfungerende og oversiktlig systematikk i organisatoriske og tekniske tiltak er et nødvendig verktøy for den behandlingsansvarlige for å sikre at personvernregelverket er ivaretatt.

En slik systematikk kalles gjerne for styringssystem eller internkontrollsystem. Et velfungerende styringssystem vil gjøre kommunene i stand til å sørge for operasjonell og faktisk etterlevelse, og at de i praksis behandler personopplysninger lovlig, sikkert og forsvarlig.

Det er ikke nødvendig eller hensiktsmessig å etablere en egen internkontroll for personvernregelverket dersom kommunen allerede har en internkontroll for andre regelverk eller for andre formål. Kommunen bør heller sørge for å utvide det eksisterende systemet med elementene som er påkrevd etter personvernregelverket.

Strava-saken

I 2021 ga Datatilsynet en kommune et overtredelsesgebyr på 50 000 kroner for at skoler i kommunen hadde pålagt elevene å bruke treningsappen Strava. Kommunen hadde ikke rutiner for anskaffelse av apper, det var ikke gjennomført risikovurderinger av tjenesten, og det var heller ikke gjennomført en vurdering av personvernkonsekvensene etter personvernforordningen artikkel 35. Kommunen hadde dermed brutt personvernforordningen artikkel 24, 32 og 35.

Les mer på: https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2021/gebyr-til-alesund-kommune-for-bruk-av-strava/

8.2.3 Gjennomføring av risiko- og sårbarhetsanalyser (ROS)

Krav til gjennomføring av risiko og sårbarhetsanalyser er forankret i personvernforordningens artikkel 24 og artikkel 32, og disse bestemmelsene angir også eksempler på hvilke momenter som må vurderes i slike analyser.

Artikkel 24 krever at det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoen behandlingen kan utgjøre for de registrertes rettigheter og friheter ved etableringen av egnede tiltak. Videre følger det av personvernforordningen artikkel 24 nr. 2 at den behandlingsansvarlige skal iverksette egnede retningslinjer for vern av personopplysninger når dette står i et rimelig forhold til behandlingsaktivitetene.

Den behandlingsansvarlige er også forpliktet til å gjennomføre egnede tekniske og organisatoriske tiltak slik at behandlingen oppnår et sikkerhetsnivå som er egnet med hensyn til risikoen, jf. personvernforordningen artikkel 32 nr. 1.

Forordningen forutsetter videre at innførte tiltak både skal «sikre og påvise» at regelverket etterleves. Dette forutsetter en systematikk som i praksis etableres gjennom rutiner i et styringssystem. Rutinene må også være egnede for å ivareta kravet, noe som innebærer at de må ha et klart innhold om blant annet ansvar og oppgaver ved gjennomføring av ROS-analyser.

Rutinene bør inneholde informasjon om når risikovurderinger skal gjennomføres, hvordan man skal gå fram og hvem som er ansvarlig. I tillegg bør rutinene si noe om hvordan risikoreduserende tiltak følges opp, om ledelsen har fastsatt en tålegrense for hva som er akseptabel risiko, revisjon og kontrollaktiviteter.

Personvernforordningen stiller krav til at sikkerheten skal være «tilfredsstillende». Dette innebærer at sikkerhetsnivået som kreves, vil variere etter hvilken type behandling og typen opplysninger det er snakk om. For å kunne si at sikkerhetsnivået er tilfredsstillende må kommunen gjøre en vurdering av hvilke trusler opplysningene er utsatt for, og hvilke konsekvenser det vil kunne få dersom disse truslene blir realisert. Sentralt i denne vurderingen er behandlingens formål, mengden personopplysninger og hvorvidt personopplysningene er sensitive eller ikke.

Kommunen må vurdere hvor stor konsekvens og sannsynlighet det er for:

- at uvedkommende vil forsøke å få tilgang på opplysningene (brudd på konfidensialitet),
- at noen vil forsøke å endre opplysningene (brudd på integritet), og
- at opplysningene ikke er tilgjengelige når de er nødvendige (brudd på tilgjengelighet).

Videre må kommunen vurdere risikoen for at det kan skje systemtekniske eller menneskelige feil som påvirker sikkerheten rundt opplysningene. Dette vil gi et risikobilde som gir kommunen grunnlag for å vurdere hvilke sikkerhetstiltak som må etableres for å oppnå kravet om tilfredsstillende informasjonssikkerhet. Sikkerhetstiltakene skal omfatte både organisatoriske, fysiske og tekniske sikkerhetstiltak.

8.2.4 Vurdering av personvernkonsekvenser (DPIA)

Det følger av personvernforordningen artikkel 35 nr. 1 at den behandlingsansvarlige skal gjennomføre en DPIA dersom det er sannsynlig at en behandling av personopplysninger vil medføre «høy risiko» for fysiske personers rettigheter og friheter.

Nærmere krav knyttet til når det er nødvendig å gjennomføre en DPIA følger av personvernforordningen artikkel 35 nr. 3. Minstekrav til hva en DPIA skal inneholde følger av artikkel 35 nr. 7. Videre følger det av artikkel 35 nr. 11 at den behandlingsansvarlige ved behov skal gjennomgå at behandlingen utføres i samsvar med gjeldende DPIA, særlig dersom risikoen ved behandlingen blir endret.

Hva som utgjør en «høy risiko for fysiske personers rettigheter og friheter» må vurderes ut ifra behandlingens art, omfang, formål og sammenhengen den utføres i. Det europeiske personvernrådet har skissert ni kriterier som kan gi en indikasjon på at det skal gjennomføres en DPIA.[4] Datatilsynet legger til grunn at det skal gjennomføres en DPIA dersom minst to av kriteriene er oppfylt. Et av kriteriene er «sårbare registrerte» som innebærer behandling av barns personopplysninger.

Kommuneledelsen er ansvarlig for at det foreligger rutiner for å gjennomføre DPIA. Rutinene må blant annet inneholde informasjon om når en DPIA skal gjennomføres, hvordan man skal gå fram for å vurdere om det er nødvendig å gjennomføre DPIA og hvem som er ansvarlig. For hvert digitalt læringsverktøy som behandler personopplysninger, og som kommunen ønsker å ta i bruk, plikter Kommunen å vurdere om det skal gjennomføres en DPIA.

8.2.5 Krav til databehandleravtaler (DBA)

Forholdet mellom behandlingsansvarlig og databehandler er nærmere regulert i personvernforordningen artikkel 28. Her følger det av artikkel 28 nr. 1 at den behandlingsansvarlige kun skal bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene etter forordningen.

Enhver behandling av personopplysninger utført av en databehandler skal være underlagt en databehandleravtale, jf. personvernforordningen artikkel 28 nr. 3. Det stilles videre en rekke krav til hva en slik avtale skal inneholde, blant annet at databehandlere kun skal behandle opplysninger på dokumentert instruks fra den behandlingsansvarlige, jf. bokstav a, og at databehandleren skal slette eller tilbakelevere alle personopplysninger etter den behandlingsansvarliges valg, jf. bokstav g.

---

[4] Datatilsynet, oversikt over kriteriene under punkt 4 i veilederen «Vurdering av personvernkonsekvenser (DPIA)», https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdering-av-personvernkonsekvenser/nar-er-risiko-hoy/

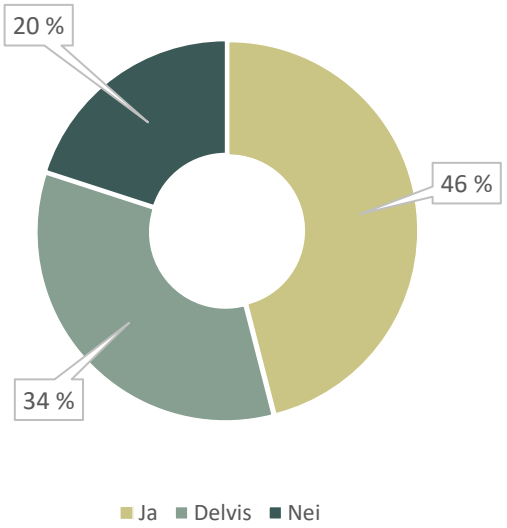
Kommunen har en plikt til å inngå databehandleravtale med alle databehandlere som behandler personopplysninger på vegne av kommunen. Som en del av kommunens internkontroll skal det foreligge rutiner som sikrer at det inngås databehandleravtaler med alle leverandører av digitale læringsverktøy som behandler personopplysninger på instruks fra kommunen. Rutinene bør inneholde informasjon om hvordan man skal gå fram for å inngå databehandleravtale, hva den bør inneholde og hvem som er ansvarlig for gjennomføring og oppfølging.

8.3 Kommunenes besvarelser

Datatilsynet har mottatt svar fra alle kommunene, hvorav de aller fleste har oppgitt at de helt eller delvis har rutiner på plass. Et fåtall kommuner har svart at det ikke foreligger relevante rutiner.

Vi har inndelt besvarelsene i kategoriene «ja» dersom rutinene foreligger i det vesentlige, «delvis» dersom rutinene foreligger delvis og «nei» dersom rutinene ikke foreligger eller besvarelsen er svært mangelfull.

8.3.1 Har kommunen sendt inn (a) en oversikt over rutinene, (b) rutiner for gjennomføring av risikovurderinger, (c) rutiner for gjennomføring av DPIA og (d) rutiner for inngåelse av databehandleravtaler?



I gjennomgangen av besvarelsene har vi observert stor variasjon i hvordan tilsynsobjektene har valgt å besvare spørsmål om kommuneledelsens overordnede ansvar. Noe av forklaringen kan være at det ikke foreligger en ensformig praksis for internkontroll blant kommunene, eller at noen kommuner ikke har etablerte rutiner å vise til.

Det ser ut til at kommunene har gjort ulike vurderinger av hvordan spørsmålene skulle besvares. I gjennomgangen har vi gått ut ifra at dokumentasjonen som kommunene har oversendt ikke nødvendigvis gir et helt representativt bilde av hvordan kommuneledelsen ivaretar sitt overordnede ansvar.

Bokstav a: En oversikt over rutinene

Vi ba om å få tilsendt *en oversikt* over relevante rutiner i forbindelse med innkjøp og implementering av digitale læringsverktøy.

Vi observerer at kommunene har vurdert hvordan denne delen av spørsmålet skal besvares på svært ulikt vis. Flere kommuner har oversendt kommunens anskaffelsesregelverk eller styringssystemet for informasjonssikkerhet og personvern. I tillegg har det blitt oversendt diverse veiledere, sjekklister, håndbøker, instrukser for ansatte og behandlingsprotokoller.

Mange kommuner har sendt over en overordnet liste med relevante dokumenter. Andre kommuner har lagt ved alle dokumenter som kan være av relevans, uten at det er nærmere angitt om det foreligger en systematikk mellom dokumentene.

Bokstav b: Rutine for gjennomføring av risikovurderinger

Vi ba videre kommunene om å oversende rutiner for gjennomføring av risikovurderinger.

Kommunene har sendt over varierende typer av dokumenter. De fleste kommunene har sendt prosedyrer for risikostyring av informasjonssikkerheten, rutine for gjennomføring av risikovurderinger eller veileder for risikovurderinger. Noen kommuner har oversendt egne sjekklister for risikovurdering av digitale læringsverktøy, policy for risikostyring eller protokoll for datasystemer.

Bokstav c: Rutine for gjennomføring av DPIA

Kommunene har sendt over forskjellige typer dokumenter for gjennomføring av DPIA. Mange kommuner har sendt over prosedyre for gjennomføring av personvernkonsekvensvurderinger, vurdering av behov for DPIA eller mal for gjennomføring av DPIA. Noen kommuner har sendt over skjema for initialvurdering av DPIA, sjekkliste for DPIA, guide for DPIA eller resultatet av DPIAer som tidligere har blitt gjennomført.

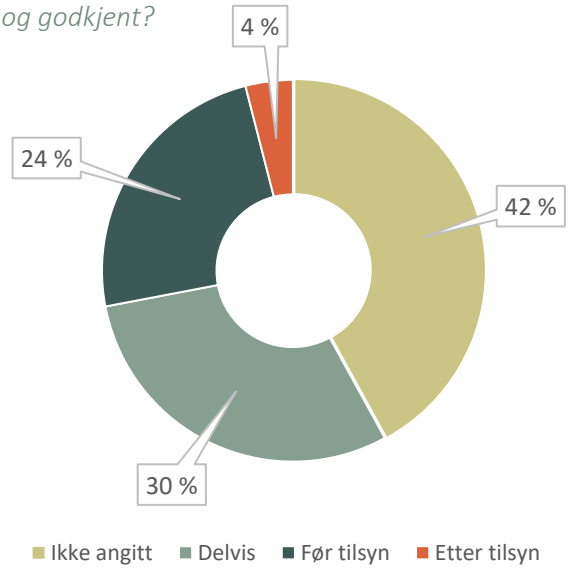
Flere kommuner oppgir at det ikke har vært behov for å gjennomføre DPIA for digitale læringsverktøy, men dette vurderer vi som en manglende forståelse for når regelverket krever at det skal gjennomføre en DPIA. Andre kommuner oppgir at det er for ressurskrevende å gjennomføre DPIA, så da lar de heller være å ta i bruk digitale læringsverktøy hvor dette er påkrevd.

Bokstav d: Rutine for inngåelse av databehandleravtale

Vi ba kommunene oversende rutiner for inngåelse av databehandleravtaler.

Kommunene har sendt over forskjellige typer dokumenter. Mange kommuner har vedlagt rutiner for inngåelse av databehandleravtaler, mal for databehandleravtaler eller sjekkliste for hva en databehandleravtale skal inneholde. Noen kommuner har sendt over flytskjema for inngåelse av databehandleravtale og prosedyre for kontroll av databehandleravtaler.

8.3.2 Når ble rutinene opprettet og godkjent?



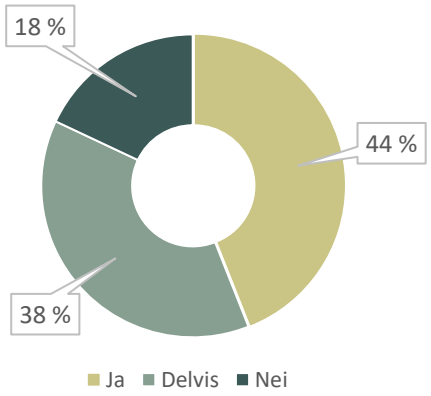
Videre har vi gjennomgått når rutinene ble opprettet og godkjent. Her er datagrunnlaget mangelfullt siden dateringen ikke alltid fremgår av rutinene som er oversendt oss. Dette trenger imidlertid ikke bety at rutinene er utdaterte, og kan forklares med at dateringen ikke er påført selve dokumentene, men at det f. eks. finnes en oversikt et annet sted i kommunens styringssystem. I brevkontrollen ble det ikke presisert at dokumentene skulle være daterte. I de tilfellene det ikke foreligger rutiner, har vi i vår gjennomgang ført opp at dateringen ikke er angitt.

Som figuren viser har omtrent en fjerdedel av kommunene lagt ved rutiner hvor det framgår at de ble opprettet og godkjent før brevkontrollen. En tredjedel av kommunen har rutiner som delvis var opprettet og godkjent. Et par kommuner har rutiner som ble opprettet etter at de mottok pålegg om å sende oss informasjon gjennom brevkontrollen. Nesten halvparten av kommunen har ikke oppgitt når rutinene eventuelt er opprettet og godkjent. En del av disse besvarelsene bærer preg av at rutinene er opprettet, men ikke godkjent.

8.4 Datatilsynets vurdering

I gjennomgangen av besvarelsene har vi gjort en overordnet vurdering av om det foreligger en systematikk bak rutinene, og om styringssystemet fremstår som etablert og hensiktsmessig i praksis. Indikatorer på dette er at rutinene er skriftliggjort og at det finnes en logisk sammenheng mellom de dokumentene som har blitt oversendt.

8.4.1 Foreligger det en systematikk bak rutinene til kommunen?



Som figuren viser anser vi at det foreligger en god systematikk bak rutinene hos omtrent halvparten av kommunene. Samtidig vurderer vi at nesten like mange kommuner kun har en «delvis» systematikk på plass. Datatilsynet vurderer det som bekymringsfullt at en så stor andel av kommunene ikke har vært i stand til å dokumentere en systematikk bak rutinene som indikerer at rutinene har en hensiktsmessig funksjon i praksis. Vi observerer at en del kommuner, særlig de små, ikke har skriftlige rutiner. Selv om mindre kommuner kan ha en god prosess i praksis, vil skriftlighet være mindre personavhengig og sikre kommunen notoritet.

Mange kommuner uttaler imidlertid at de er i pågående prosesser med å innføre, gjennomgå eller utbedre rutiner. Dette tyder på at brevkontrollen har gjort kommunene oppmerksomme på viktige problemstillinger knyttet til behandling av personopplysninger i digitale læringsverktøy.

Et gjennomgående trekk i besvarelsene er at kommunene angir at det skal gjennomføres ROS analyser, DPIA og databehandleravtaler uten at det står noe om hvordan dette skal gjennomføres i praksis.

Det samme gjelder for databehandleravtaler. Flere kommuner oppgir at det er oppført i rutiner at det er påkrevd å inngå databehandleravtaler med alle leverandører som behandler personopplysninger på vegne av kommunen, men at dette i liten grad følges opp i praksis. Dette kan tyde på manglende ressurser, at rutinene ikke er godt nok kjent i organisasjonen eller at de ikke er spesifikke nok.

Som følge av at vi ba om en oversikt over relevante rutiner, er det imidlertid vanskelig å foreta fullstendige kvalitative vurderinger av hvorvidt rutinene som er sendt inn er egnede. Det har videre vært utfordrende å foreta kvalitative vurderinger av rutinene for gjennomføring av risikovurderinger, DPIA og inngåelse av databehandleravtaler. De fleste kommuner har sendt over mange ulike rutiner som må ses i sammenheng for å vurdere egnethet. For å få et tilstrekkelig vurderingsgrunnlag må det gjennomføres stedlig tilsyn hos kommunene. Vi finner det derfor mest hensiktsmessig å fokusere på veiledning knyttet til temaet om kommuneledelsens overordnede ansvar.

8.5 Veiledning

Selv om kommunene varierer i størrelse, er tjenesteområdene de samme for alle kommunene. Innenfor den offentlige grunnskolen behandler kommunene de samme kategoriene av personopplysninger til samme formål, selv om omfanget varierer.

Kommuneledelsen må ha en oversikt over relevante styringsdokumenter og ha dokumenterte krav til gjennomføring av risikovurderinger, gjennomføring av DPIA og inngåelse av databehandleravtaler i sin internkontroll. En forutsetning for å ha orden i eget hus er at rutinene er oppdatert og angir relevante roller med riktig kompetanse.

Kommunen må videre etablere en systematikk bak rutinene. Det må være en avklart og logisk sammenheng mellom styrende, gjennomførende og kontrollerende rutiner. Det bør fremgå av rutinene hvem som er ansvarlig for dokumentet, når det er datert og når det sist ble revidert. Kommunen må sørge for jevnlig revisjon av rutinene.

Rutinene skal videre være skriftlige for at kommunen kan dokumentere etterlevelse av personvernregelverket. Selv om en kommune har en god etterlevelse i praksis, vil skriftlige rutiner også kunne føre til mindre personavhengighet og vilkårlighet.

Det er opp til den enkelte kommune å velge om man ønsker å etablere spesifikke rutiner for digitale læringsverktøy, eller om de generelle rutinene i kommunen er dekkende også for digitale læringsverktøy. Det er uansett viktig at problemstillinger som er spesifikke for digitale læringsverktøy og opplæringssektoren adresseres.

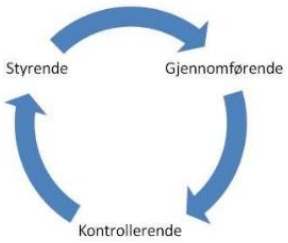
Kommunens rutiner skal beskrive hvordan en risikovurdering, DPIA og databehandleravtale skal gjennomføres. Rutinene bør klarlegge når en risikovurdering eller DPIA skal gjennomføres, hvem som er ansvarlig og hvordan man skal gå fram for å gjennomføre risikovurderingen steg for steg. Rutinene bør inneholde henvisninger til relevante maler.

Rutinene for inngåelse av databehandleravtaler bør klarlegge når en databehandleravtale skal inngås, hvem som er ansvarlig, hvor avtalene oppbevares i kommunens system og hvordan det foretas kontroll av om avtalene samsvarer med realiteten. Rutinene bør videre ha spesifikke kriterier for hva databehandleravtalen skal inneholde, og gjerne involvering av personvernombud for en gjennomgang av avtalen. Kommunen må særlig være oppmerksom på hva som skjer med personopplysningene når tjenesten opphører og om personopplysningene overføres til land utenfor EU/EØS.

8.6 Annen relevant veiledning

- **KS**
  - Orden i eget hus – kommunedirektørens internkontroll
  - Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet
- **Digitaliseringsdirektoratet (Digdir)**
  - Styrende
  - Gjennomførende
- **Nasjonal sikkerhetsmyndighet (NSM)**
  - NSMs grunnprinsipper for IKT-sikkerhet 2.1
- **Foreningen Kommunal Informasjonssikkerhet (KiNS)**
  - Verktøykasse for styringssystem
- **Datatilsynet**
  - Vurdering av personvernkonsekvenser (DPIA)
  - Styringssystem og internkontroll
  - Samlerapport fra brevkontroll med norske kommuner 2023

9. Gjennomførende rutiner



9.1 Datatilsynets krav om redegjørelse

Kommunen som skoleeier skal, som del av sin internkontroll,[5] ha en systematisk tilnærming i etterlevelsen av personvernregelverket. Denne internkontrollen består av, i tillegg til styrende og kontrollerende elementer, gjennomførende elementer. De gjennomførende elementene retter seg i hovedsak mot de ansatte og her finner man rutiner som er tilpasset den enkeltes arbeidssituasjon.

Datatilsynet ba i brevkontrollen kommunene om deres gjennomførende rutiner knyttet til når et digitalt læringsverktøy eventuelt kan tas i bruk. Mer presist ba vi kommunene om å legge ved relevant(e) rutine(r), og/eller beskrivelser av, prosessen frem til verktøyet eventuelt kan tas i bruk. Vi ba også om en beskrivelse av hvordan denne prosessen blir kommunisert til de ansatte ved skolene.

9.2 Personvernregelverkets krav til gjennomførende rutiner som en del av internkontrollen

Vi viser til samlerapportens punkt 8.2 hvor vi beskriver personvernforordningen artikkel 5 nr. 2 om ansvarlighetsprinsippet og artikkel 24 om pliktene knyttet til internkontroll og risikoanalyser.

Personvernforordningen stiller krav til internkontroll i form av egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med personvernforordningen. Tiltakene skal gjennomgås på nytt og skal oppdateres ved behov.

[5] Internkontroll kan defineres som planlagt og systematisk styringssystem som virksomheter etablerer for å oppdage brudd på gjeldende regler. Les mer om etablering av internkontroll på Datatilsynets nettsider, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/.

Gjennomførende rutiner/dokumentasjon beskriver de organisatoriske og tekniske tiltak som er foreslått som følge av at virksomheten har vurdert risiko[6] for rettigheter og friheter, for eksempel tiltak for å ivareta ulike rettigheter for de registrerte eller tiltak for å oppnå tilstrekkelig informasjonssikkerhet.

9.3 Kommunenes besvarelser

I Datatilsynets gjennomgang av gjennomførende rutiner har vi undersøkt hvorvidt kommunene har en bestemt fremgangsmåte for når en lærer ønsker å ta i bruk et nytt digitalt læringsverktøy i undervisningen. Datatilsynet mottok varierte besvarelser på dette punktet og det er tydelig at kommunene har ulike tilnærminger til hvordan de utarbeider slike gjennomførende rutiner.

Et flertall av kommunene - 23 kommuner – har sendt over en form for fremgangsmåte. Fremgangsmåten kunne for eksempel være angitt som «Rutiner ved innkjøp eller bruk av nytt digitalt læringsverktøy», som en rutine/bestillerskjema av app/program, «Prosess ved anskaffelse av nytt digitaltopplæringsverktøy» eller rutine "Ny app til læringsbrett - vurdering og søknad".

7 kommuner har ikke i noen eller tilstrekkelig grad svart på spørsmålet. Datatilsynet har observert at dette kan være fordi det ikke finnes faste gjennomførende rutiner for innføring av nye læringsverktøy i kommunen eller at disse rutinene er under arbeid, men ikke vedtatt på svartidspunktet.

De resterende 20 kommunene har delvis vist at de har en etablert fremgangsmåte. I disse kommunene ser vi at det eksempelvis foreligger en kortfattet punktliste om hvilke vurderinger som skal gjøres på de ulike stadiene av prosessen, en sjekkliste for skolen, eller et flytskjema som overordnet beskriver stegene/vurderingene. I disse kommunene er det *noe* som er på plass, men Datatilsynet ser at disse er mangelfulle – enten fordi de er korte, overordnede eller inneholder overfladiske beskrivelser. Typisk for disse fremgangsmåtene er at det foreligger en svært kort beskrivelse av prosessen uten at denne fremgår av et skriftlig dokument, eller at det skriftlige dokumentet kun gjelder for en avgrenset aktivitet, som f. eks. å åpne en tjeneste i Feide.

Eksempler

To eksempler på vår vurdering av mangelfulle fremgangsmåter:

- En lærer foreslår et nytt digitalt verktøy
- Rektor vurderer leverandør og verktøy, eventuelt i kommunikasjon med kommunedirektør
- Avtale blir inngått mellom oss og leverandør
- Tilganger blir aktivert på relevante ster (sic.) og verktøyet kan tas i bruk.

Lærerne som ønsker å ta i bruk et nytt digitalt verktøy tar dette opp med rektor eller avdelingsleder. Dersom de blir enige om å ta verktøyet i bruk, får ansatt ved IT-avdelingen spørsmål å hjelpe til med det.

[6] Risiko kan defineres som hypotese om hvilken fare en hendelse representerer eller sannsynlighet kombinert med konsekvens.

9.4 Datatilsynets vurdering

I brevkontrollen ba vi kommunene oversende relevante rutiner, og/eller beskrivelser av prosessen, som gjør det vanskelig å gjennomføre en konkret vurdering av hver enkelt kommune. Vurdering vår nedenfor er derfor overordnede betraktninger basert på det helhetlige inntrykket fra kommunenes besvarelser på dette spørsmålet.

Datatilsynet ønsker imidlertid å påpeke at siden et stort antall av kommunenes gjennomførende rutiner er mangelfulle så vil de derfor ikke være fullt ut egnede til å ivareta barnas personvern i skolen når kommunen skal ta i bruk nye digitale læringsverktøy. Det er likevel varierende grad av modenhet, og vi ser at flere kommuner nylig har påbegynt mer omfattende arbeid med å få dette på plass.

9.5 Veiledning

Vi ser at kommunene har tolket spørsmålet ulikt og mange av de kommunene som har oppgitt å ha en fremgangsmåte på plass har ikke nødvendigvis omtalt denne som «rutine». Noen har lagt ved det de omtaler som retningslinjer, beskrivelse av fremgangsmåter, en veileder, et flytskjema/prosessflyt eller beskrevet en overordnet prosess/innarbeidet kultur. Hva det gjennomførende dokumentet blir kalt er ikke avgjørende, det viktigste er at dokumentet beskriver oppgaver eller aktiviteter i en prosess. I det følgende vil vi omtale den nødvendige gjennomførende dokumentasjonen som rutine, se nærmere omtale under punkt 9.2.

Personvernregelverket oppstiller ingen formkrav for gjennomførende rutiner eller hva de konkret må inneholde. Samtidig så er det viktig at kommunen utarbeider de rutiner som er nødvendige for oppfyllelse av virksomhetens plikter og de registrertes rettigheter.

Generelt bør gjennomførende dokumentasjon inneholde:

(1) rutiner og prosedyrer
(2) arbeidsinstrukser

Gjennomførende rutiner bør inneholde formål, omfang, roller/ansvar, en beskrivelse av aktiviteten(e) som skal utføres, samt eventuelle frister. Dette er viktig å ha på plass for å vise at vurderingene er satt i system, slik at en enkelte lærer/ansatte i kommunen vet hva som skal gjøres før nytt digitalt læringsverktøy kan tas i bruk.

For å sikre at kommunen ikke begår lovbrudd ved behandlingen av personopplysninger i digitale læringsverktøy er det en rekke vurderinger som må være på plass før verktøyet kan tas i bruk. Dersom kommunen som behandlingsansvarlig ikke vet at slike verktøy er tatt i bruk, eller at disse verktøyene ikke i tilstrekkelig grad blir vurdert før bruk, oppstår det følgefeil. Den gjennomførende rutinen vil kunne bidra til å sikre at bruk av digitale læringsverktøy i opplæringsøyemed samsvarer med kommunens definerte mål og retningslinjer for personvern og reglene for øvrig. For de ansatte i kommunen kan gjennomførende rutiner være et sett med interne kjøreregler som sikrer at kommunen ikke begår lovbrudd med noen av sine aktiviteter.

Den følgende veiledningen bygger delvis på veiledningen til KS' SkoleSec «Hva må jeg gjøre før jeg kan ta i bruk en ny digital tjeneste?».[7] Vi ser i brevkontrollen at flere kommuner allerede er kjent

[7] KS SkoleSec, Hva må jeg gjøre før jeg kan ta i bruk en ny digital tjeneste?, https://www.ks.no/fagomrader/digitalisering/skolesec/hva-ma-jeg-gjore/

med denne veiledningen og bygger sine rutiner på denne. Datatilsynet anser dette som positivt, da denne veiledningen inneholder de viktigste elementene knyttet til de gjennomførende rutinene.

9.5.1 Mer konkret om innholdet i rutinen

Rutinen skal være dekkende for alle typer digitale læringsverktøy

Det viktig at rutinen klart definerer hvilke digitale læringsverktøy som omfattes, for å sikre at vurderingene er dekkende for alle typer verktøy som kan benyttes i undervisningen. Vi minner om at med begrepet «digitale læringsverktøy» mener vi både digitale læringsressurser og læringsplattformer som brukes til undervisningsformål. Dette omfatter både betalte- og gratisverktøy.

Det påpekes at det kan se ut som at et stort flertall av kommunene har lagt til grunn en for snever tolkning av «digitalt læringsverktøy». I gjennomgangen av kommunenes svar ser vi at flere kommuner har rutiner som kun dekker apper, apper til iPad, anskaffelse av programvare i kommunen eller apper som krever betaling. Rutinene har derfor et for snevert anvendelsesområde – i tillegg til å inkludere apper bør rutinene også dekke programvare, innhold eller nettsteder – både de som er gratis og de som innebærer en kostnad.

Datatilsynet ser at noen kommuner viser til rutiner som gjelder «anskaffelse» av digitale læringsverktøy. Ordet anskaffelse blir som regel brukt i forbindelse med innkjøpsprosesser. Dersom rutinen er avgrenset til de tilfellene hvor man enten må anskaffe etter anskaffelsesregelverket eller betale for bruken/kjøpe lisens, så står skolen i fare for å ha rutiner som ikke er dekkende for gratisverktøy. Det kan eksempelvis være når det brukes en nettside i undervisningen som behandler personopplysninger om elevene. Som redegjort for under punkt 5.2 kan bruk av gratisverktøy, som for eksempel en nettside i undervisningen, innebære behandling av personopplysninger.

Rutinen skal være systematisert og dokumentert

Rutinen bør utformes etter en felles mal. Rutinen blir da enklere å bruke for de ansatte, og det blir lettere å vurdere om den er fullstendig. I tillegg bør rutinen være datert, vise til dokumentversjon, samt hvem som er ansvarlig for dokumentet.

Ved å systematisere og dokumentere rutinene, sikrer kommunen både notoritet for internkontrollen samt sikrer at oppgavene utføres på samme måte hver gang, uavhengig av hvem som utfører dem. Datatilsynet ser at flere kommuner har uformelle former for rutiner, ved at fremgangsmåten fremgår i skolens IT-chat på Teams eller at det er en innarbeidet kultur for hvordan ting skal gjøres. Uformelle former for rutiner kan øke sannsynligheten for at ikke alle nødvendige vurderinger gjøres eller at relevante personer ikke er kjent med sin rolle.

Rutinen skal inneholde klare beskrivelser av roller og ansvar

Siden de gjennomførende elementene i internkontrollen i hovedsak retter seg mot de ansatte, er det spesielt viktig å entydig definere hvem som har ansvaret for hva. Beskrivelsene som fremgår av rutinen må derfor være tilpasset den enkeltes arbeidssituasjon.

Vurderingen av hvorvidt et nytt digitalt læringsverktøy kan brukes i undervisningen kan være komplisert og krevende for mange. Vurderingene vil – i tillegg til å kunne være av pedagogisk karakter – oftest kreve teknisk, juridisk og personvernfaglig kompetanse. Rolle- og ansvarsfordeling skal være dokumentert og det er viktig at personer med riktig kompetanse blir involvert til riktig tid. Datatilsynet ønsker å presisere at selv om lærerne er et ledd i å ivareta personvernet til elevene, så er det kommuneledelsen som sitter på ansvaret og skal etablere klare rolle- og ansvarsforhold nedover i organisasjonen.

Eksempel

Et eksempel på vår vurdering av en utydelig rolle- og ansvarsfordeling:
Kommunen beskriver at «IKT-kontaktene er derfor kompetansebærere innenfor tematikken og vil fungere for lærernes første kontaktpunkt når ny digital ressurs skal vurderes».

I rutine for lærerne står det imidlertid at:
Som lærer tar du (…) avgjørelser som ivaretar elevenes trygghet. Dette gjelder også på det digitale området. Siden du velger digitale løsninger på vegne av elevene, så må du føle deg trygg på at løsningen er sikker, at personvernet er ivaretatt og at den er i samsvar med gjeldende regler. Spør gjerne IKT-kontakten om råd.

Dersom ansvar for vurdering av digitale læringsverktøy delegeres til den enkelte lærer risikerer man at vurderingene blir tilfeldige og mangelfulle. Nedenfor har vi plukket ut noen eksempler på hva noen kommuner mener at lærer skal vurdere i henhold til kommunenes rutiner.

Eksempel

- Hvem *er leverandøren? Er leverandøren seriøs og pålitelig*?
- *Lagrer appen/programmet personopplysninger? Hvis ja, hvilke personopplysninger?*
- *Behandler systemet taushetsbelagte eller sensitive personopplysninger?*
- *Ved interesse for en nettside, søker man opp informasjon om personvern på siden og vurderer dette: Bruk av personopplysninger og eventuell bruk til markedsføring og profilering og videreformidling.*
- *Vil personopplysninger behandles i en skyløsning?*
- Har *appen/programmet reklame?*
- Læringsressursen *har informasjon om betingelser for bruk og deling?* (ja/nei/delvis)
- Hvilke *funksjoner har tjenesten? Er det mulig å begrense tilgangen til visse funksjoner for elever eller ansatte?*

Datatilsynet påpeker at en lærer normalt sett ikke har tilstrekkelig kompetanse for å vurdere disse punktene alene, men kan bidra inn i de innledende vurderingene av et læringsverktøy. I noen kommuner har læreren ansvaret for å ta en innledende vurdering av verktøyet, mens i andre kommuner melder læreren kun inn et ønske. Deretter kobles andre fagpersoner med ulikt ansvar på.

Eksempler på fagpersoner som kan involveres på ulike stadier i vurderingsprosessen kan være IKT-veileder/fagleder/rådgiver/drift/support, (spesial)pedagoger, personvernombudet, personvernrådgiver, digitaliseringsrådgiver, informasjonssikkerhetsrådgiver, personer i oppvekstavdelingen, eller skoleledelsen/rektor.

Noen kommuner opererer med råd eller andre sammenslutninger av fagpersoner med ulik kompetanse som på jevnlig basis vurderer innkomne ønsker om å ta i bruk nye digitale læringsverktøy i fellesskap.

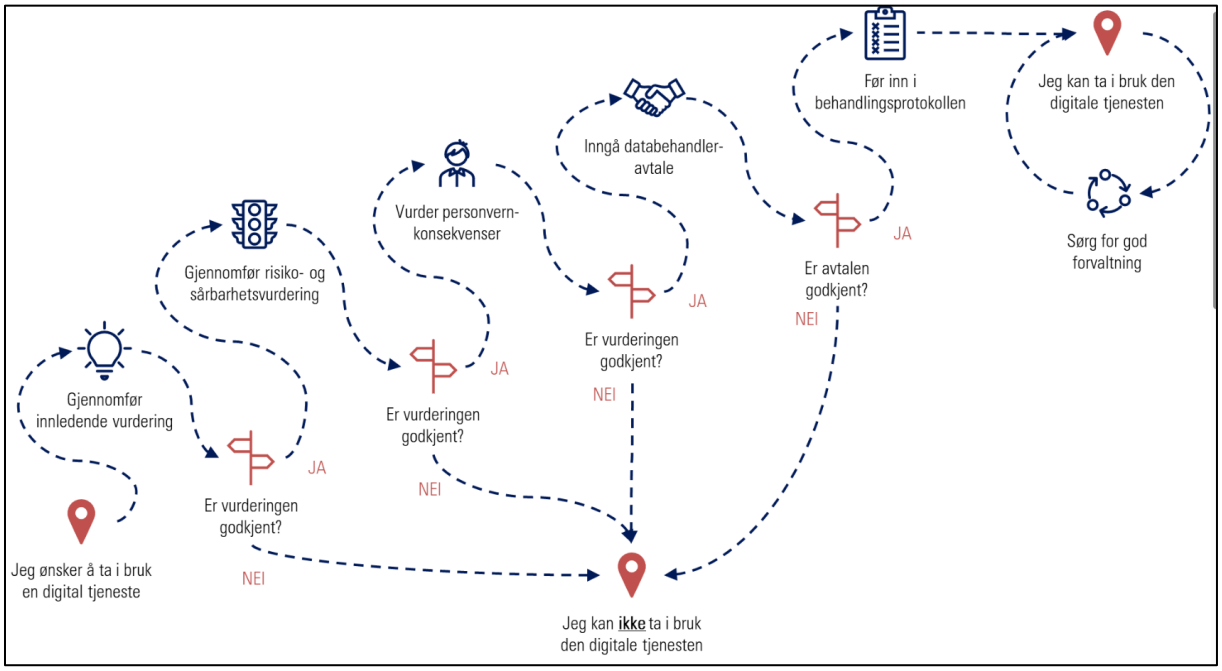
Rutinen må gjøres kjent i organisasjonen

Et flertall av kommunene besvarte ikke spørsmålet om hvordan prosessen blir kommunisert til de ansatte ved skolene. Datatilsynet vil her poengtere at vi i brevkontrollen ikke har undersøkt om lærerne og andre ansatte faktisk er kjent med rutinen, gitt at det foreligger slik rutine. Samtidig ser vi at flere kommuner har på plass ulike metoder for å gjøre rutinen kjent, for eksempel:

- Prosessen blir kommunisert til skolene i nyhetsbrev eller informasjonsskriv.
- Informasjon finnes på kommunes intranett eller på skolens nettside.
- Lærere og skoleledelsen får påminnelse om rutine før starten på nytt skoleår.
- Rutinen er sendt på e-post til alle ansatte.
- Rutinen ligger i kommunens internkontrollsystem og rektor har ansvar for å videreformidle til alle ansatte ved skolen.

9.5.2 Rutinen bør identifisere plikter

Illustrasjonen nedenfor viser KS SkoleSec sin «steg for steg»-veiviser for å identifisere pliktene til kommunen ved vurdering av et nytt læringsverktøy.[8] Datatilsynet mener at kommunens gjennomførende rutiner skal inneholde tekst og vurderingsmomenter opp mot alle disse stegene i veiviseren, med henvisning til konkrete roller og ansvar.



[8] KS SkoleSec, Hva må jeg gjøre før jeg kan ta i bruk en ny digital tjeneste?, https://www.ks.no/fagomrader/digitalisering/skolesec/hva-ma-jeg-gjore/.

Rutinen bør kreve en innledende vurdering av det digitale læringsverktøyet

Formålet med den innledende vurderingen er å undersøke hva slags personopplysninger som blir behandlet, for deretter å kunne identifisere om og i så fall hvilke etterfølgende vurderinger som må gjøres for å ivareta personvern og informasjonssikkerhet, før verktøyet kan tas i bruk.

Den innledende vurderingen kan inneholde følgende punkter:

- Få oversikt over behandlingene av personopplysninger i det digitale læringsverktøyet og vurder behandlingens art, omfang, formål og sammenheng,
- Kartlegg kilder, mottakere og ansvarsforhold,
- Vurdering av lovlighet, nødvendighet og proporsjonalitet

Mer informasjon om den innledende vurderingen finnes på Datatilsynets nettsider «Hvordan gjennomføre internkontroll i praksis».[9]

KS SkoleSec har også utarbeidet noen maler for gjennomføring av den innledende vurderingen, se:

- Mal: Informasjon om digital ressurs og ønsket bruk (for lærere)
- Mal: Innledende vurderinger (for IKT-ansvarlig)[10]

Rutinen skal inneholde en beskrivelse av risiko og sårbarhetsanalyser (ROS)

Det er kommunen som er ansvarlig for at risiko og sårbarhetsanalyser blir gjennomført før en behandling av personopplysninger starter og at de blir gjentatt ved endringer som har betydning for informasjonssikkerheten.

Den gjennomførende rutinen bør inneholde hva en risiko- og sårbarhetsanalyse er, når de skal gjennomføres og hvordan det skal gjøres. Videre må det være identifisert hvilke roller som har ansvaret for analysene. Rutinen trenger ikke selv å vise til alle vurderingene som skal gjøres i analysen, det kan være tilstrekkelig her å vise til kommunens eksisterende maler for risikovurderinger.

Mer informasjon om risiko- og sårbarhetsanalyse finnes på Datatilsynets nettsider «Risiko og risikovurdering»[11]. Datatilsynet har også utarbeidet en mal for risikovurdering.[12] På KS SkoleSec sine nettsider finnes det maler for «Forberedelser til ROS» og «Risikovurderinger».[13]

Datatilsynets erfaringer er at risikovurderinger gjennomføres godt i gruppearbeid slik at flere ulike perspektiver involveres og alle relevante problemstillinger drøftes. En slik gruppe kan for eksempel bestå av rektor, IKT-ansvarlig, sikkerhetsansvarlig, system- /fagansvarlig og lærere/pedagoger.

---

[9] Datatilsynet, Hvordan gjennomføre internkontroll i praksis, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/hvordan-gjennomfore-internkontroll-i-praksis/.

[10] KS SkoleSec, begge malene ligger her https://www.ks.no/fagomrader/digitalisering/skolesec/hva-ma-jeg-gjore/.

[11] Datatilsynet, Risiko og risikovurdering, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdering-av-personvernkonsekvenser/risikovurdering/

[12] Datatilsynet, mal for risikoanalyse, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/vedlegg/.

[13] KS SkoleSec, begge malene ligger her https://www.ks.no/fagomrader/digitalisering/skolesec/hva-ma-jeg-gjore/.

Nedenfor har vi trukket frem et eksempel på vår vurdering av en kommune som ikke involverer relevante roller og kompetanse i analysen.

Eksempel

Ved bruk av nye webapplikasjoner som skolene selv tar i bruk, gjøres det veldig sjelden risikovurderinger. Ansatte som ønsker å bruke nye gratis webapplikasjoner, tar selv en vurdering. Ved applikasjoner som koster penger, kontaktes administrasjonen for godkjenning.

Rutinen skal inneholde en beskrivelse av vurdering av personvernkonsekvenser (DPIA)

Den gjennomførende rutinen skal inneholde tekst som beskriver hva en DPIA er, når kommunen er pliktig til å gjennomføre en DPIA og hvordan dette skal gjøres. Rutinen skal også identifisere hvilke roller som har ansvaret for vurderingen. Vi presiserer at selve rutinen ikke trenger å vise til alle stegene i vurderingen, men at det er tilstrekkelig å vise til kommunens eksisterende mal for DPIA.

Mer informasjon om DPIA finnes på Datatilsynets nettsider «Vurdering av personvernkonsekvenser (DPIA)»[14]. Datatilsynet har også utarbeidet en sjekkliste for vurdering av personvernkonsekvenser.[15] KS SkoleSec har utarbeidet en mal for vurdering av personvernkonsekvenser samt et eksempel på en Dummy-DPIA.

- Mal: Vurdering av personvernkonsekvenser
- Eksempel: Dummy-DPIA[16]

I likhet med risikovurderinger er vurdering av personvernkonsekvenser godt egnet for gruppearbeid, hvor ulike roller med relevant kompetanse blir involvert. Gjennom brevkontrollen erfarte vi at flere kommuner gjennomfører ROS og DPIA som en del av IKT-samarbeidet kommunen har med andre kommuner. På denne måten vil kommunene samle kompetanse og ressurser på tvers av kommunegrensene. Rutinene knyttet til vurdering av DPIA kan differensieres mellom en innledende

Eksempel

Det skal sammen med personvernombudet foretas en forhåndsvurdering av personvernkonsekvenser i kommunens DPIA-verktøy (…). Forhåndsvurderingen avdekker behov for fullstendig DPIA. Fullstendig DPIA skal gjøres i samarbeid med personvernombud.

[14] Datatilsynet, Vurdering av DPIA, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdering-av-personvernkonsekvenser/
[15] Datatilsynet, Sjekkliste for vurdering av personvernkonsekvenser, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdering-av-personvernkonsekvenser/.
[16] KS SkoleSec, Mal for personvernkonsekvenvurdering, begge malene ligger her https://www.ks.no/fagomrader/digitalisering/skolesec/hva-ma-jeg-gjore/.

vurdering og fullstendig vurdering. Ved å ikke involvere alle roller i den innledende fasen vil kommunen kunne spare tid og ressurser.

Rutinen skal ha en henvisning til kravene til databehandleravtale
De gjennomførende rutinene må inneholde informasjon om hva en databehandleravtale er, hva den skal inneholde og prosessen for inngåelse av en avtale. I tillegg skal rutinen identifisere hvilke roller som er ansvarlig for vurdering av avtaleinnholdet samt avtaleinngåelsen.

Datatilsynet har utarbeidet en veileder om databehandleravtaler og mal som ligger på våre nettsider.[17] KS SkoleSec har også utarbeidet en mal for databehandleravtaler.[18]

Rutinen skal inneholde en henvisning til kravet til behandlingsprotokoll
Det følger av personvernforordningen artikkel 30 at all behandling av personopplysninger skal føres inn i en protokoll. Kommunens gjennomførende rutiner må derfor inneholde beskrivelser av hva en behandlingsprotokoll er, hvilke opplysninger som skal føres inn, en beskrivelse av hvordan dette skal gjøres samt hvem som er ansvarlig for oppdatering av behandlingsprotokollen.

Datatilsynet har utarbeidet veiledning om behandlingsprotokoll samt mal som ligger på våre nettsider.[19] SkoleSec har også utarbeidet en mal og veileder om behandlingsprotokoll.[20]

9.6 Annen relevant veiledning

- **Datatilsynet**
  - Veileder om informasjonssikkerhet og internkontroll
  - Veileder om bruk av skytjenester i skolen
  - Bruk av digitale hjelpemidler i skolen
  - Krav til skoleeiere som skal bruke læringsplattformer
- **KS**
  - Hva må jeg gjøre før jeg kan ta i bruk en ny digital tjeneste?
  - Slik sikrer du oppfølging av personvern og informasjonssikkerhet
- **Digitaliseringsdirektoratet (Digdir)**
  - Gjennomførende risikovurderinger

10. Leverandørers behandling av elevers personopplysninger for egne formål

10.1 Datatilsynets krav om redegjørelse

Kommunen må som behandlingsansvarlig iverksette tiltak for å sikre at behandling av personopplysninger knyttet til digitale læringsverktøy som tas i bruk, skjer i samsvar med

[17] Datatilsynet, Veileder og mal for databehandleravtaler, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/hvordan-lage-en-databehandleravtale/
[18] KS, SkoleSec, begge malene ligger her https://www.ks.no/fagomrader/digitalisering/skolesec/hva-ma-jeg-gjore/.
[19] Datatilsynet, veiledning om behandlingsprotokoll, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/protokoll-over-behandlingsaktiviteter/
[20] KS, Skolesec, begge malene ligger her https://www.ks.no/fagomrader/digitalisering/skolesec/hva-ma-jeg-gjore/

personvernforordningen. Dette inkluderer å sikre at all behandling av personopplysninger har rettslig grunnlag, og behandlingen bare skjer for formål som har grunnlag i opplæringsloven eller andre regelverk kommunene er underlagt.

Digitale læringsverktøy leveres ofte av private aktører, og mange slike leverandører har forretningsmodeller basert på innsamling, bruk og deling av personopplysninger. I brevkontrollen ba vi derfor kommunene redegjøre for hvilke tekniske og organisatoriske tiltak de har iverksatt for å sikre at ikke elevenes personopplysninger behandles for formål utenfor opplæringslovens anvendelsesområde i forbindelse med bruk av digitale læringsverktøy. Dette gjelder særlig behandling av personopplysninger for leverandørenes egne kommersielle formål, for eksempel markedsføring, analyse og videreutvikling av deres egne tjenester.

10.2 Personvernregelverkets krav til internkontroll og rettslig grunnlag

Kommunen er som skoleeier behandlingsansvarlig for behandling av elevenes personopplysninger i forbindelse med bruk av digitale læringsverktøy i undervisningen.

For mange digitale læringsverktøy er det nødvendig å behandle personopplysninger for å levere tjenesten og at den skal kunne brukes for undervisningsformålet til skolen. Noen krever bare få eller ingen personopplysninger, mens i andre kan det være nødvendig å behandle en rekke personopplysninger for læringsverktøyets funksjonalitet.

Det er viktig å være klar over at personopplysninger omfatter alle opplysninger som direkte eller indirekte kan knyttes til enkeltpersoner, jf. personvernforordningen artikkel 4 nr. 1. Vi viser til definisjonen av personopplysninger under samlerapportens punkt 5.2.

I henhold til personvernprinsippene i personvernforordningen artikkel 5 nr. 1 må all behandling av personopplysninger skje på en lovlig, rettferdig og åpen måte. Behandling skal skje for spesifikke, uttrykkelig angitte og berettigede formål, og skal ikke viderebehandles på en måte som er uforenlig med disse formålene. Personopplysningene som behandles må også være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for. Den behandlingsansvarlige har ansvar for å sikre at de grunnleggende prinsippene for behandling av personopplysninger overholdes og skal kunne påvise at dette gjøres, jf. personvernforordningen art. 5 nr. 2.

Personvernforordningen artikkel 6 nr. 1 fastsetter at all behandling av personopplysninger må ha et rettslig grunnlag for å være lovlig. I forbindelse med skolenes undervisning er det personvernforordningen artikkel 6 nr. 1 bokstav c og e som er de relevante rettslige grunnlagene for behandling av elevenes personopplysninger. For behandling av personopplysninger gjennom bruk av digitale læringsverktøy er det oftest artikkel 6 nr. 1 bokstav e som er det mest aktuelle av disse grunnlagene å vurdere. Dette er lagt til grunn i tidligere veiledning fra Datatilsynet, og det er også slik Kunnskapsdepartementet har tolket opplæringsloven.[21] [22]

Grunnlaget for behandling av personopplysninger etter både artikkel 6 nr. 1 bokstav c og e må følge av nasjonal rett, jf. personvernforordningen artikkel 6 nr. 3. Dette kalles ofte kravet til supplerende rettsgrunnlag. Opplæringsloven og andre relevante lovverk kommunene er underlagt, setter dermed

[21] Datatilsynet, veiledning om skytjenester i skolen, https://www.datatilsynet.no/personvern-pa-ulike-omrader/skole-barn-unge/bruk-av-google-chromebook-og-g-suite-for-education-og-andre-skytjenester-i-grunnskolen/rettslig-grunnlag-for-behandlingen/

[22] Brev fra Kunnskapsdepartementet til KS av 19. juni 2024.

rammene for kommunenes behandlinger av personopplysninger om elevene og hvilke formål behandlingen kan skje for.

Behandling av personopplysninger som er nødvendig for at det digitale læringsverktøyet skal fungere til sitt formål, vil etter omstendighetene ha rettslig grunnlag i personvernforordningen artikkel 6 nr. 1 bokstav e og supplerende rettsgrunnlag i opplæringslovens bestemmelser.

Dersom elevenes personopplysninger imidlertid tilgjengeliggjøres for behandling til leverandørenes egne kommersielle formål, vil ikke dette være forenelig med skolens plikter og rettigheter etter opplæringsloven. Kommunene vil dermed ikke ha rettslig grunnlag i personvernforordningen for en slik tilgjengeliggjøring.

Dette gjelder for det første behandling av elevenes personopplysninger for markedsføringsformål knyttet til de digitale læringsverktøyene. Svært mange digitale tjenester har en forretningsmodell basert på markedsføring og deling av personopplysninger. Dette innebærer normalt sporing av brukerne og deres adferd for å gjøre antakelser om deres interesser. Personopplysningene deles i økosystemet for digital markedsføring hvor annonsører byr på å vise brukerne reklame. Deling i dette systemet for sanntidsauksjon (real time bidding/RTB) innebærer normalt at personopplysningene deles med svært mange aktører. Behandling av elevers personopplysninger på denne måten vil være i strid med personvernregelverket og utgjøre en stor krenkelse av deres rett til personvern.

Problemstillingen knyttet til leverandørenes behandling av elevers personopplysninger gjelder imidlertid ikke bare behandling av elevenes personopplysninger til markedsføringsformål, men også leverandørenes utlevering av personopplysninger for andre formål. I tillegg gjelder det dersom leverandørene for øvrig bruker elevenes personopplysninger til egne analyser og utvikling av leverandørens tjenester og produkter. At slike formål faller utenfor det supplerende rettsgrunnlaget i opplæringsloven er også lagt til grunn av Kunnskapsdepartementet i et brev til KS av 20. september 2024.

Eksempel

Det danske datatilsynets avgjørelse om kommuners bruk av Google Workspace
I denne saken vurderte det Danske datatilsynet at det var hjemmel i personvernforordningen artikkel 6 nr. 1 bokstav e og supplerende rettsgrunnlag i den danske folkeskoleloven for å tilgjengeliggjøre personopplysningene til leverandøren for formål knyttet til levering av tjenestene, forbedring av sikkerheten og påliteligheten av tjenestene, kommunikasjon med kommunene og overholdelse av rettslige krav.
Det ble imidlertid vurdert at det ikke var hjemmel for å tilgjengeliggjøre personopplysningene til leverandøren for blant annet vedlikehold og forbedring av tjenestene samt utvikling av nye funksjoner og tjenester.
Vi understreker for ordens skyld at denne saken gjelder tolkningen av de supplerende rettsgrunnlagene i den danske folkeskoleloven, og ikke den norske opplæringsloven.

Personvernforordningen artikkel 6 nr. 4 fastsetter videre at dersom personopplysningene behandles for et annet formål enn det som personopplysningene er blitt samlet inn for, må dette formålet være forenelig med formålet personopplysningene opprinnelig ble samlet inn for. Unntaket er dersom den registrerte samtykker eller viderebehandlingen har hjemmel i lov. Behandlinger av personopplysninger i forbindelse med digitale læringsverktøy som ikke har supplerende rettsgrunnlag i artikkel 6 nr. 3, vil heller ikke kunne være lovlig viderebehandling etter artikkel 6 nr. 4.

Som behandlingsansvarlig har kommunene en forpliktelse til å gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med forordningen, jf. personvernforordningen art. 24. Kommunene må dermed i henhold til personvernforordningen artikkel 24 iverksetter egnede tekniske og organisatoriske tiltak for å sikre og påvise etterlevelse av personvernforordningen krav til rettslig grunnlag i artikkel 6 i forbindelse med bruk av digitale læringsverktøy, inkludert at personopplysningene til elevene ikke tilgjengeliggjøres for leverandørene for behandling for deres egne kommersielle formål.

At elevenes personopplysninger ikke skal tilgjengeliggjøres for behandling til leverandørenes egne kommersielle formål har også sammenheng med kravet i artikkel 32 nr. 1 om å iverksette tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, inkludert evne til å sikre vedvarende konfidensialitet for personopplysningene.

Å ta i bruk digitale læringsverktøy vil også etter omstendighetene kreve en vurdering av personvernkonsekvensene (DPIA) etter artikkel 35 nr. 1, og i denne vurderingen må det også hensyntas eventuelle risikoer knyttet til leverandørers egen behandling av elevenes personopplysninger hvorvidt elevenes personopplysninger kan tilgjengeliggjøres eller for øvrig behandles uten rettslig grunnlag.

Leverandøren av digitale læringsverktøy vil oftest være en databehandler for kommunen. I databehandlerrelasjoner stilles det krav om at det inngås en skriftlig databehandleravtale etter artikkel 28. Databehandleravtalen skal blant annet inneholde gjenstanden for og varigheten av behandlingen, behandlingens art og formål, typen personopplysninger og kategorier av registrerte. Det skal også angis at databehandleren bare behandler personopplysningene på dokumenterte instrukser fra den behandlingsansvarlige. En behandlingsansvarlig skal kun bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i personvernforordningen. Databehandleravtalene med leverandørene må fastsette tydelige skranker for hvilke formål elevenes personopplysninger skal behandles for.

10.3 Kommunenes besvarelser

10.3.1 Bevissthet om risiko for leverandørenes egen behandling av elevenes personopplysninger

Ut fra besvarelsene fremstår de aller fleste kommunene å ha en viss bevissthet rundt risikoen for leverandører av digitale læringsverktøy sin egen bruk av elevers personopplysninger. Graden av bevissthet rundt problemstillingen varierer imidlertid stort.

Et flertall av kommunene hadde i besvarelsene og dokumentasjonen kun fokus på leverandørenes behandling av elevers personopplysninger for markedsføring eller øvrig datadeling eller profilering, som det tradisjonelt er knyttet høyest risiko til. Det er bare noen få kommuner som også knyttet denne risikoen til for eksempel behandling av personopplysninger for formål om å videreutvikle leverandørenes tjenester. Et eksempel på sistnevnte er en kommune som ikke tok i bruk et digitalt læringsverktøy knyttet til lesing fordi leverandøren ville bruke resultater til egne formål.

Det betydelig variasjon i hvilke tekniske eller organisatoriske tiltak kommunene redegjorde at de har gjennomført for å hindre leverandørers kommersielle bruk av elevers personopplysninger. Fem av kommunene hadde imidlertid ikke iverksatt noen tiltak for å hindre slik bruk av elevenes personopplysninger fra leverandørene.

10.3.2 Skjema eller annen innledende vurdering av læringsverktøyet

I punkt 9 ovenfor redegjør vi fremgangsmåtene til kommunene når det gjelder vurdering av digitale læringsverktøy. Mange kommuner har beskrevet eller lagt frem et eget skjema, sjekkliste eller en annen type innledende vurdering som skal gjøres i forbindelse med digitale læringsverktøy. For en del av kommunene er det et eller flere sjekkpunkt i den innledende vurderingen eller skjemaet som omhandler hvorvidt tjenesten inneholder reklame eller hvorvidt tjenesten behandler personopplysninger for markedsføringsformål.

Eksempel

Enkelte kommuner har også sjekkpunkter knyttet til andre formål fra leverandøren, for eksempel:
Oppgir leverandør at de bruker personopplysninger som testdata, til forskning, statistikk eller lignende.

Som et ledd i en slik innledende vurdering har en del kommuner stilt krav om at personvernerklæringen til tjenestene skal gjennomgås, men mange kommuner pekte på at disse dessverre ofte er uklare og vanskelig å forstå. Enkelte kommuner trakk frem at de etterspør informasjon eller avklaringer fra leverandørene hvis tilgjengelig informasjon om behandling av personopplysninger er uklar, og at de har utformet rutiner med standardspørsmål for dette.

En av kommunene informerte om at de bruker verktøy for å gjennomføre tester av digitale læringsverktøy på apper og nettsider for å undersøke eventuell sporing i læringsverktøyet, og at dette er beskrevet i rutinene deres.

10.3.3 Inngåelse av databehandleravtaler

Et flertall av kommunene har redegjort for at de har et krav om inngåelse av databehandleravtaler med leverandørene, og at det stilles krav til at avtalene skal sette begrensningene for hvilke formål personopplysningene til elevene skal behandles for, og at leverandøren ikke kan gå utenfor kommunens instruks.

Eksempel

Et eksempel fra en kommunes mal for databehandleravtale er:
Databehandler har ikke råderett over personopplysningene utover det som er nødvendig for å oppfylle sine plikter etter databehandleravtalen, og kan ikke behandle disse til egne formål.

Det varierer hvorvidt kommunene har en egen mal for databehandleravtaler, eller om de bruker leverandørenes databehandleravtaler. De som har egne maler har ofte basert disse malene på maler fra Digitaliseringsdirektoratet, KS eller fra Datatilsynets nettsider. Kommunene informerer også om at noen leverandører stiller krav om å bruke sine egne databehandleravtaler selv om kommunene har egen mal, og kommunene har begrenset forhandlingsmakt knyttet til vilkår overfor store leverandører.

Dersom leverandørenes databehandleravtaler brukes, stiller de aller fleste kommunene krav til at denne skal gjennomgås. Noen kommuner har redegjort for at dette skal gjøres av personvernombud eller andre med den personvernkompetanse i sentralt i kommunen, mens andre kommuner informerte om at er det rektor eller andre ansatte på skolen som gjør denne vurderingen. Noen kommuner har lagt frem egne sjekklister for dette formålet.

Eksempel

En kommune skriver:
Leverandører ønsker av og til å bruke egne avtaler. Da diskuteres dette og sjekkes opp mot […] kommune sin avtale. Dersom leverandørene vil bruke personopplysninger til egne formål, f.eks forbedre tjenesten, kontakter vi dem for å informere om lovverk og følger opp gjennom videre dialog.

Selv om de fleste av kommunene beskrev eller fremla rutiner om at det skal inngås databehandleravtaler med leverandørene av digitale læringsverktøy, viste imidlertid flere av kommunenes fremlagte oversikter over digitale læringsverktøy at mange databehandleravtaler i praksis manglet. For noen kommuner var også den oversendte oversikten over digitale læringsverktøy svært kort, og fremsto dermed ikke ufullstendig eller med betydelige begrensninger i hva som var ført opp. For disse kommunene er det dermed sannsynlig at databehandleravtaler mangler for mange digitale læringsverktøy som i praksis brukes i skolene. Enkelte kommuner anerkjente at de per i dag ikke har oversikt over digitale læringsverktøy og om de har databehandleravtaler.

Flere kommuner beskrev ressursutfordringer knyttet til databehandleravtaler, og flere beskrev også at det er mangel på kompetanse i kommunen til å vurdere slike avtaler. Disse pekte også på at leverandører jevnlig gjør endringer i tjenestevilkår, databehandleravtaler og praksiser, og at det er ressurskrevende å vedlikeholde og følge opp kommunens portefølje med digitale læringsverktøy. Enkelte kommuner redegjorde for at de har en antallsbegrensning i hvor mange digitale læringsverktøy kommunen har i porteføljen sin til enhver tid for å håndtere disse ressursutfordringene.

10.3.4 Risiko- og sårbarhetsanalyser og vurdering av personvernkonsekvenser

Mange av kommunene svarte at de har risiko- og sårbarhetsanalyser og eventuell vurdering av personvernkonsekvenser som krav i rutinene for anskaffelse av digitale læringsverktøy. De fremlagte

rutinene for slike risikovurderinger og vurderinger av personvernkonsekvenser viste at de fleste kommunene har ikke har spesifikke punkter i disse rutinene som knytter seg til leverandørenes bruk av elevenes personopplysninger til egne kommersielle formål. For mange av de aktuelle kommunene kan imidlertid dette skyldes at rutinene for risiko- og sårbarhetsanalyser og vurdering av personvernkonsekvenser er generelle, og ikke spesifikke for digitale læringsverktøy.

Enkelte kommuner skrev de av ressurshensyn ikke anskaffer digitale læringsverktøy som krever at det gjennomføres en vurdering av personvernkonsekvenser. Andre skrev at de har samarbeid med andre kommuner om gjennomføring av vurdering av personvernkonsekvenser.

10.3.5 Feide-innlogging

Som et tiltak for å forhindre at elevers personopplysninger behandles for leverandørers kommersielle formål, trakk 15 av kommunene frem at de utelukkende eller nesten utelukkende bruker digitale læringsverktøy som tilby Feide-innlogging. Flere viste til at de får varslinger dersom leverandøren gjør endringer i hvilke personopplysninger de henter inn gjennom Feide.

10.3.6 Gratisverktøy og andre begrensninger i fremlagte rutiner og tiltak

Datatilsynet presiserte i kravet om redegjørelse at digitale læringsverktøy omfatter både betalte- og gratisverktøy samt både applikasjoner installert lokalt i utstyret til kommunen og webapplikasjoner. For en del kommuner fremgikk det at de beskrevne tiltakene gjaldt for både betalte og gratisapplikasjoner. Et par kommuner beskrev forenklede prosedyrer for å ta i bruk gratisapplikasjoner sammenlignet med betalte tjenester.

For mange av kommunene fremgikk det imidlertid enten at gratisapplikasjoner ikke var omfattet av de fremlagte rutinene eller tiltakene, eller at dette ikke var klart ut ifra fremlagt dokumentasjon. For disse kommunene er dermed uklart ut ifra besvarelsene hvilke rutiner som eventuelt gjelder for å ta gratis digitale læringsverktøy i bruk. Enkelte kommuner beskrev at ansatte i skolen selv vurderer å ta i bruk gratis webapplikasjoner.

For flere kommuner er det også andre begrensninger i hvilke digitale læringsverktøy rutinene og tiltakene gjelder for. Eksempler er at de kun gjelder for applikasjoner på en konkret plattform, at de ikke gjelder for webapplikasjoner, eller at rutinene kun gjelder for tjenester med innlogging – for eksempel gjennom Feide.

10.4 Datatilsynets vurdering

Hovedformålet med tilsynet er veiledning, og Datatilsynets har derfor ikke vurdert det som hensiktsmessig å gjøre en konkret vurdering av etterlevelsen til kommunene på dette punktet. I og med at vi ikke ba kommunene oversende konkrete rutiner vil det heller ikke være mulig å gjennomføre en konkret vurdering av hver enkelt kommune. Vurdering vår nedenfor er derfor overordnede betraktninger basert på det helhetlige inntrykket fra kommunenes besvarelser på dette spørsmålet.

Selv om flere kommuner har iverksatt gode og egnede tiltak for å sikre at personopplysninger ikke tilgjengeliggjøres for leverandører for behandling til deres egne formål, er Datatilsynet bekymret for det samlede bilde fra besvarelsene. Det er mange kommuner som ikke har iverksatt slike egnede tiltak, eller hvor tiltakene og rutinene er mangelfulle.

Datatilsynet er særlig bekymret for at digitale læringsverktøy som er gratis, webapplikasjoner og/eller læringsverktøy som ikke bruker innlogging, for mange kommuner ikke omfattet av rutinene kommune har for å ta i bruk digitale læringsverktøy. For disse kommunene kan slike verktøy derfor

tilsynelatende tas i bruk uten forutgående personvernvurderinger. Dette strider med kommunenes forpliktelser etter personvernregelverket.

Fra et personvernperspektiv er det ingen grunn til å ha lempeligere rutiner og vurderinger dersom et digitalt læringsverktøy ikke koster penger. Tvert imot har nettopp gratisapplikasjoner fra private aktører oftere forretningsmodeller som knytter seg til reklame, profilering og/eller videresalg av personopplysninger, og personvernrisikoen ved bruk av gratisapplikasjoner er derfor ofte vel så høy. For å unngå å krenke elevenes personvernrettigheter, bør derfor gratis digitale læringsverktøy omfattes av like strenge vurderinger og tiltak knyttet til personvern som digitale læringsverktøy med lisenskostnader.

Videre er det mange kommuner som undervurderer hva som utgjør personopplysninger og overvurderer hva det innebærer at de digitale læringsverktøyene har Feide-innlogging. Det er også få av kommunene som fremstår å være bevisst andre kommersielle formål enn markedsføringsformål fra leverandørene, slik som for eksempel behandling av elevenes personopplysninger for videreutvikling av leverandørens egne tjenester. Dermed risikeres det at elevenes personopplysninger behandles for formål som faller utenfor grunnlaget i opplæringsloven, og dermed behandles uten rettslig grunnlag.

10.5 Veiledning

10.5.1 Tiltak i skriftlige rutiner

De aller fleste kommunene som har iverksatt tiltak for å hindre kommersiell bruk av elevers personopplysninger fra leverandørene av digitale læringsverktøy, har integrert disse tiltakene i øvrige rutiner knyttet til anskaffelse, bruk og vedlikehold av digitale læringsverktøy.

Datatilsynet støtter denne tilnærmingen. Etter vårt syn er det som hovedregel ikke nødvendig eller mest hensiktsmessig for kommunene å utarbeide separate rutiner, prosedyrer eller arbeidsinstrukser utelukkende knyttet til tiltak for å hindre kommersiell behandling av elevers personopplysninger fra leverandører av digitale læringsverktøy. I stedet vil det normalt være hensiktsmessig for kommunene å integrere slike tiltak som en del av kommunens generelle rutiner som gjelder anskaffelse, bruk og vedlikehold av digitale læringsverktøy. Dette inkluderer blant annet relevante rutiner for databehandleravtaler, risiko- og sårbarhetsanalyser, vurdering av personvernkonsekvenser og behandlingsprotokoll.

Datatilsynet viser til veiledningen i punkt 9.5 ovenfor, og i det følgende gis det veiledning for spesifikke tiltak for å hindre at personopplysninger behandles for leverandørenes egne formål i de ulike stegene i rutiner for å ta i bruk digitale læringsverktøy.

10.5.2 Rutinene må også inkludere gratisverktøy og webapplikasjoner

I Bouvets rapport *Digitalisering i skolen: Har vi glemt personvernet?* fra 2021 rapporterer kommunene om et stort trykk fra lærerne som ønsker å ta i bruk gratisverktøy i undervisningen.[23] Et slikt trykk rapporteres også i besvarelsene i dette tilsynet.

Dersom de digitale læringsverktøyene har en lisenskostnad, tvinges ofte beslutningene om bruk oppover i skolesystemet. Som nevnt er imidlertid personvernrisikoene ofte vel så høye for

[23] Bouvets rapport, *Digitalisering i skolen: Har vi glemt personvernet?,* Side 20, https://www.bouvet.no/bouvet-deler/rapport-personvern-i-skolen/Digitalisering%20i%20skolen%20-%20Har%20vi%20glemt%20personvernet.pdf

gratisverktøy, fordi mange slike tjenester har forretningsmodeller basert på sporing, markedsføring og deling av personopplysninger. Det er derfor viktig at kommunens rutiner for bruk av digitale læringsverktøy også omfatter gratisverktøy, og at det iverksettes egnede tiltak for å sikre at elevenes personopplysninger tilgjengeliggjøres for behandling for leverandørenes egne kommersielle formål knyttet til bruk av slike gratisapplikasjoner.

Det er videre viktig at de relevante rutinene også omfatter webapplikasjoner, og ikke bare applikasjoner som installeres lokalt på kommunens utstyr. Det er ingen grunn til å ha lempeligere krav og vurderinger av webapplikasjoner enn lokalt installerte tjenester. Det at en tjeneste er nettbasert innebærer i noen tilfeller at den ikke omfattes av de begrensninger kommunen har for hvem som har brukerrettigheter til å installere tjenester lokalt i enheten. Såfremt kommunen ikke bruker hvitlisting kan det dermed mangle tekniske hindre for bruk av nettbaserte applikasjoner uten forutgående vurderinger av kommunen sentralt. At tjenesten er en webapplikasjon vil på denne måten medføre at beslutningen om bruken av verktøyet i praksis ikke tas sentralt i kommunen. Les mer om dette tema under punkt 12.5.

Lærerne må gjøres kjent med, og læres opp i, kommunens rutiner for bruk av digitale læringsverktøy, herunder gratis webapplikasjoner, slik at det skapes bevissthet rundt risikoene og god personvernkultur knyttet til bruk av slike verktøy.

10.5.3 Om Feide-innlogging og andre innloggingstjenester

Feide er en innloggingsløsning, og ikke en godkjenningsordning. SIKT, som er leverandør av Feide, gjør ingen kontroll av databehandleravtalene med leverandørene og hvorvidt formålene og behandlingene av personopplysninger som beskrives i databehandleravtalen er i tråd med personvernregelverket og oppgavene skolene er pålagt gjennom opplæringsloven. Disse vurderingene er kommunene alene ansvarlig for, og dette må være tydelig ut ifra kommunens rutiner. Se en nærmere redegjørelse for Feide under punkt 5.4.

Feide er et nyttig verktøy for å bidra til en sikker innlogging og overføring av personopplysninger. Når det gjelder problemstillinger knyttet til bruk av elevers personopplysninger til leverandørenes egne formål, har kommunen fremdeles ansvaret selv om det digitale læringsverktøyet tilbyr Feide-innlogging.

Det er også viktig å være klar over at selv om Feide-portalen kan gi kommunene en oversikt over kategoriene av personopplysninger som deles gjennom Feide, er ikke denne oversikten nødvendigvis uttømmende for hvilke personopplysninger som behandles i det digitale læringsverktøyet. Digitale læringsverktøy kan i tillegg samle inn personopplysninger om elevene på andre måter, for eksempel cookies eller lignende sporingsteknologier. Feide gir heller ikke kontroll eller oversikt over hvilke personopplysninger elevene eventuelt selv legger inn i det digitale læringsverktøyet. Kommunene må dermed alltid gjøre selvstendige undersøkelser og vurderinger av de digitale læringsverktøyenes behandlinger av personopplysninger.

Det er videre viktig at kommunenes rutiner for digitale læringsverktøy også omfatter verktøy som ikke krever innlogging. Selv om elevene ikke logger inn på tjenestene, kan tjenestene likefullt samle inn og bruke personopplysninger om brukerne. Dette kan for eksempel skje gjennom tillatelser til å bruke opplysninger lagret på enheten til eleven – for eksempel geografisk lokasjon – eller andre former for sporingsteknologier.

Som tidligere nevnt er det viktig at kommunene er oppmerksomme på at opplysninger ikke trenger å kunne knyttes til navn, kontaktinformasjon eller elevens identifikatorer knyttet til skolen for å utgjøre personopplysninger. Opplysninger som kan knyttes til identifikatorer knyttet til enheten som brukes,

identifikatorer knyttet til informasjonskapsler (cookies) og øvrige sporingsteknologier, IP-adresse eller øvrige nettidentifikatorer vil normalt også utgjøre personopplysninger. Selv om det skulle være felles IP-adresse for alle elevene når de er på skolen, kan dette stille seg annerledes dersom kommunen ikke har innført VPN via kommunens nettverk når elevene bruker det digitale læringsverktøyet hjemmefra. Det kreves normalt sett få datapunkter for å kunne identifisere en person basert på geografisk lokasjon over en viss tid.

10.5.4 Innledende vurdering av det digitale læringsverktøyet

En innledende vurdering av det digitale læringsverktøyet bør inkludere en undersøkelse av hvorvidt leverandøren behandler elevenes personopplysninger til egne formål. At et læringsverktøy inneholder reklame er en indikasjon på at leverandøren behandler og deler personopplysninger for markedsføringsformål. Selv om det ikke er reklame i selve tjenesten er det imidlertid ikke en garanti for at tjenesten ikke utleverer personopplysninger til kommersielle formål. Det er dermed ikke tilstrekkelig å bare ha et sjekkpunkt med «Er det reklame i appen?» eller tilsvarende.

Datatilsynet mener at rutinene skal fastholde at det gjennomføres ytterligere undersøkelser for de tilfeller der det er uklart for kommunen hvordan et digitalt læringsverktøy behandler personopplysninger, ut ifra tilgjengelig informasjon. Dette kan for eksempel være oppfølging overfor leverandøren, eller gjennom å bruke ulike verktøy for å sjekke sporing på nettsider og tjenester.

10.5.5 Risikovurderinger og vurdering av personvernkonsekvenser (DPIA)

I gjennomføring av risiko- og sårbarhetsvurderinger og DPIA av digitale læringsverktøy må kommunen vurdere tjenestens datastrøm og foreliggende risikoer for at elevenes personopplysninger behandles for markedsføring eller andre kommersielle formål.

I Datatilsynet veiledning om vurdering av personvernkonsekvenser er det blant annet trukket frem at det i risikovurderingene skal vurderes konsekvensen av og sannsynligheten for at:

- personopplysninger behandles uten rettslig grunnlag
- det samles inn mer personopplysninger enn det som er nødvendig for formålet
- personopplysninger lagres lengre enn det som er nødvendig for formålet
- det ikke er tilstrekkelig åpenhet rundt behandlingen av personopplysninger

Dette er alle relevante risikoer knyttet til leverandørers behandling av personopplysninger for egne formål.

10.5.6 Databehandleravtaler

Personvernforordningen legger til grunn at databehandleravtalen blant annet skal inneholde behandlingens art og formål, typen personopplysninger og en forsikring om at databehandleren kun skal behandle personopplysningene på dokumentert instruks fra den behandlingsansvarlige. Når kommunen ønsker å ta i bruk et nytt digitalt læringsverktøy så har ikke kommunen adgang til å inngå databehandleravtaler om behandling av elevers personopplysninger som det ikke finnes hjemmel for i personvernforordningen eller opplæringsloven.

Det må derfor foretas en grundig gjennomgang av alle databehandleravtalene der det sikres at avtalen ikke inneholder behandling av personopplysninger til formål som ikke er nødvendig for de oppgavene skolene er underlagt etter opplæringsloven. Dette gjelder for eksempel behandling av elevenes personopplysninger for videreutvikling av leverandørens tjenester.

Kommunen må videre ha tiltak for å følge med på, og følge opp, eventuelle endringer som gjøres i avtalene fra leverandørene.

10.6 Annen relevant veiledning:

- **KS**
  - Hva må jeg gjøre før jeg kan ta i bruk en ny digital tjeneste?
  - Nasjonal DPIA for Google Workspace for education

- **Det danske datatilsynet**
  - Chromebook-sagen: Kommunerne efterlever Datatilsynets seneste påbud
  - Datatilsynet giver påbud i Chromebook-sag

11. Oversikt over digitale læringsverktøy som en del av internkontrollen

11.1 Datatilsynets krav om redegjørelse

Kommunen som skoleeier, har behandlingsansvar for alle behandlingsaktiviteter som skjer i de digitale læringsverktøyene som er i bruk i kommunen. For å kunne etablere en god internkontroll i praksis er det nødvendig med oversikt over de digitale læringsverktøyene som er i bruk på skolene i kommunen og som behandler personopplysninger.

I brevkontrollen ba vi kommunene om å beskrive hvordan de holder oversikt over alle digitale læringsverktøy som er i bruk i skolene i deres kommune. Vi ba dem legge ved en oversikt over alle digitale læringsverktøy, for eksempel et utdrag av behandlingsprotokollen.

11.2 Personvernregelverkets krav til å ha en oversikt over behandlingsaktivitetene som en del av internkontrollen

Den behandlingsansvarlige har ansvar for å sikre at de grunnleggende prinsippene for behandling av personopplysninger overholdes og skal kunne påvise at dette gjøres, jf. personvernforordningen art. 5 nr. 2.

Ansvaret innebærer en forpliktelse til å gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med forordningen, jf. personvernforordningen art. 24. Det skal i den forbindelse tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter.

Personvernforordningen artikkel 30 stiller krav om at den behandlingsansvarlige skal føre en protokoll over alle personopplysningene som behandles og nærmere informasjon om behandlingsaktivitetene. Protokollen er blant annet ment å være et arbeidsverktøy for den behandlingsansvarlige, som ledd i styringen av behandlingen av personopplysninger.

En oversiktlig og oppdatert oversikt over digitale læringsverktøy er et nødvendig virkemiddel for å sikre at personvernregelverket er ivaretatt. Oversikten over behandlingsaktiviteter er avgjørende for tilstrekkelig god internkontroll og å kunne dokumentere denne.

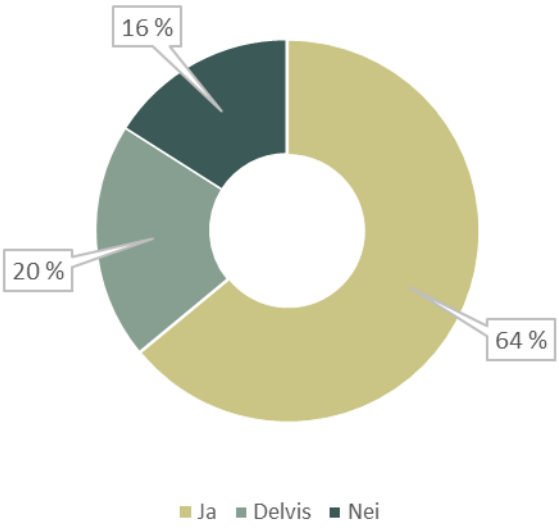
Informasjonen i oversikten skal utgjøre et grunnlag for prioritering og systematisering av arbeidet med informasjonssikkerhet og personvern i de digitale læringsverktøyene. Oversikten over digitale læringsverktøy som behandler personopplysninger er altså en forutsetning for å kunne sikre at det er inngått databehandleravtaler med alle leverandører, det er gjennomført ROS-analyser og DPIA.

11.3 Kommunenes besvarelser

11.3.1 Fremstår det som at kommunen har en hensiktsmessig oversikt over alle digitale læringsverktøy som er i bruk i skolene i kommunen?

Antall svar: **50**

Svar	Antall	% av svar
Ja	32	64 %
Delvis	10	20 %
Nei	8	16%



I gjennomgangen av besvarelsene har Datatilsynet observert at det er store variasjoner i hvordan kommunen holder oversikt over de digitale læringsverktøyene som behandler personopplysninger på skolene. Mange kommuner benytter eksterne leverandørers tjenester for å holde oversikt, eksempelvis Digiorden levert av KS digital, Samsvar fra SIKRI eller program som DraftIT.

Vi vurderte at 32 av de 50 kommunene hadde beskrivelser som var hensiktsmessig for å holde oversikt og kontroll over digitale læringsverktøy som benyttes i kommunen. Flere beskriver at oppdatering av oversikten skjer i forbindelse med de sentraliserte vurderingene kommunen utfører ved vurdering av et nytt digitalt læringsverktøy. Oppdatering av oversikten skjer på denne måten av kommunen sentralt og ikke ved den enkelte skole.

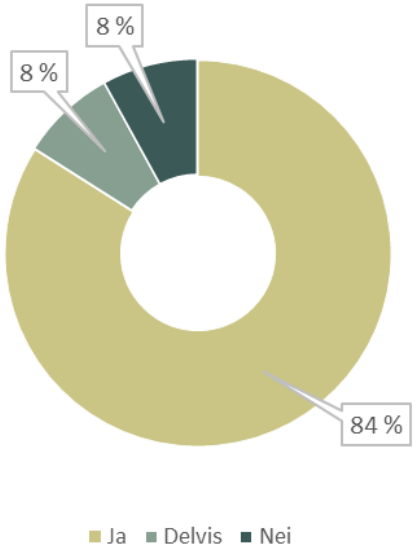
Det var 8 kommuner som ikke beskrev hvordan de holder oversikt, eller vi anså ikke den foreliggende beskrivelsen tilfredsstillende. I denne kategorien finnes de kommunene som ikke sendte over beskrivelser av hvordan de holder oversikt, eller de kommunene som ikke har sentraliserte vurderinger av digitale læringsverktøy.

10 av kommunene ble ansett å ha en delvis tilfredsstillende oversikt over de digitale læringsverktøy som er i bruk. For disse fremstod den beskrevne prosessen som tilfeldig og ga oss en indikasjon på at det ikke foreligger en fullstendig oversikt over hvilke læringsverktøy som faktisk brukes på skolene.

11.3.2 Har Datatilsynet mottatt en oversikt over digitale læringsverktøy som er i bruk på skolene i kommunen?

Antall svar: **50**

Svar	Antall	% av svar
Ja	42	84 %
Delvis	4	8 %
Nei	4	8%



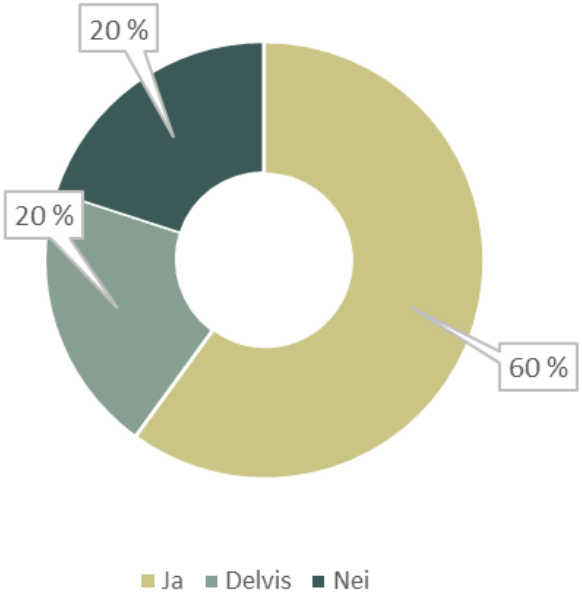
Det var et stort flertall av kommunene som sendte inn oversikt over digitale læringsverktøy som behandler personopplysninger. Fire kommuner har imidlertid ikke oversendt oversikt over digitale læringsverktøy. Det er vanskelig å si om spørsmålet er misforstått eller om kommunen ikke har en slik oversikt tilgjengelig. Gjennom å se på de øvrige punktene kommunene skulle redegjøre for har vi fått et inntrykk av at disse fire kommunene ikke har en slik skriftlig oversikt tilgjengelig.

De fleste kommuner har ikke én felles oversikt over alle digitale læringsverktøy, men oversikt fordelt i ulike systemer, eksempelvis fordelt som tjenester med Feide-innlogging, appbaserte verktøy eller via løsningene til Apple, Google eller Microsoft. Noen kommuner har også inndelt digitale læringsverktøy ut i fra om de benyttes på iPad eller PC.

11.3.3 Anser Datatilsynet oversikten som er mottatt som utfyllende og fullstendig for de digitale læringsverktøyene som er i bruk på skolene i kommunene?

Antall svar: **50**

Svar	Antall	% av svar
Ja	30	60 %
Delvis	10	20 %
Nei	10	20 %



Totalt 20 kommuner, som utgjør nesten halvparten, har enten ikke oversendt en oversikt eller har sendt over en svært kort liste over digitale læringsverktøy, som Datatilsynet anser å ikke være fullstendig.

Vi ser at en stor andel av disse kommunene har lagt til grunn en for snever definisjon av personopplysninger og er ikke klar over at læringsverktøyene som er i bruk i kommunen faktisk behandler personopplysninger. Det er eksempelvis oversendt en liste på rundt 10-15 digitale

læringsverktøy, som er ca. 10 % av den totale listen andre kommuner har oversendt. Andre kommuner har kun oversendt oversikt over digitale læringsverktøy kommunen har lisens på. I enkelte av disse kommunenes vedlagte rutiner beskrives det for eksempel at lærere selv skal vurdere gratisapplikasjoner som de ønsker å ta i bruk.

Eksempler

«Åpne gratis tjenester på internett kan tas i bruk uten installasjon eller sentral distribusjon.»

«Ved bruk av nye webapplikasjoner som skolene selv tar i bruk, gjøres det veldig sjelden risikovurderinger. Ansatte som ønsker å bruke nye gratis webapplikasjoner, tar selv en vurdering. Ved applikasjoner som koster penger, kontaktes administrasjonen for godkjenning. Elever kan logge seg inn med sin kommunale e-post adresse på enkelte webapplikasjoner.»

Vi har vurdert at det er 30 kommuner som har oversendt tilstrekkelige utfyllende oversikt, enten i form av behandlingsprotokoll eller kopi av lister fra ulike systemer.

11.4 Datatilsynets vurdering

Datatilsynet ser at det er forskjell på hvordan store og små kommuner holder oversikt over digitale læringsverktøyene som er i bruk. Dersom det kun finnes en eller to skoler i kommunen kreves det ikke like mye systematisk arbeid for å sikre en oppdatert og total oversikt over læringsverktøyene, i forhold til en kommune med mange skoler.

Vi mener det er bekymringsverdig at så mange som 20 kommuner enten ikke har oversendt en oversikt eller denne er ansett å være mangelfull. Det er dessverre et faktum at en stor andel av kommunene har en misoppfatning av hva personopplysninger er, og en manglende erkjennelse av at blant annet IP-adresse, geolokasjon og enhetsID også er personopplysninger.

Vi ser at de kommunene som har sentral godkjenning og flåtestyring av læringsverktøy på enhetene har en bedre forutsetning for å holde oversikt over hvilke læringsverktøy som er i bruk til enhver tid. Når det ikke er adgang for elever eller lærere å installere digitale læringsverktøy uten å involvere kommunen sentralt, vil kommunen også bevare kontrollen.

Datatilsynets oppfatning er at mange av kommunen erkjenner at de ikke har god nok oversikt og er i pågående prosesser med å opprette en felles oversikt over digitale læringsverktøy for å få en mer total oversikt over hvilke behandlingsaktiviteter som skjer i kommunen. Vi ser positivt på at flere kommuner har pågående prosesser for å oppdatere og fullføre oversikten over digitale læringsverktøy. Flere kommuner bemerker at de har redusert porteføljen av digitale læringsverktøy de senere årene som en konsekvens av en mer kritisk tilnærming til mengden personopplysninger som behandles, for å redusere risiko for brudd på personvernet og for å være i stand til å forvalte læringsverktøyene i tilstrekkelig grad.

Vi har forståelse for at kommunene opplever at det er mange digitale læringsverktøy å holde oversikt over. Desto viktigere er det å ha en oppdatert oversikt over de læringsverktøyene som faktisk er i

bruk, og som behandler personopplysninger, slik at kommunen kan overholde sitt behandlingsansvar etter personvernregelverket.

11.5 Veiledning

11.5.1 Hvordan kan kommunene holde oversikt over digitale læringsverktøy som behandler personopplysninger?

En forutsetning for god internkontroll er at kommunen starter med å kartlegge hvilke behandlingsaktiviteter som skjer under kommunens ansvar. For at oversikten skal være oppdatert til enhver tid forutsettes det at innføring av nye læringsverktøy en del av en systematisert prosess som involverer kommunen sentralt. Først når kommunen har identifisert hvilke digitale læringsverktøy som er i bruk, kan kommunen sørge for at kravene til ROS-analyser, databehandleravtaler og DPIA er innfridd.

11.5.2 Hvordan skal oversikten over digitale læringsverktøy se ut?

Vi ser at det er vanlig at kommuner tar i bruk flere hundre ulike digitale læringsverktøy til undervisningsformål. Datatilsynet mener det er nødvendig at kommunen har en fullstendig oversikt over digitale læringsverktøy som behandler personopplysninger for å sikre god internkontroll. Dette er dessverre ikke realiteten i alle kommuner, som eksempelet nedenfor viser.

Eksempler

«Det oppleves som overveldende å holde tritt med alt man burde ha gjort. En mindre kritisk tilnærming på et tidligere tidspunkt, har også medført rot i kommunens systemer. Eksempelvis lisenser til ulike applikasjoner. Et godt system der ansvar for å vurdere applikasjoner som godkjent eller ikke, mangler. Den nødvendige ryddejobben utsettes stadig. Noe av grunnen til dette er manglende kompetanse, og også på grunn av en del annet forefallende arbeid.»

Det er ingen formkrav til hvordan oversikten skal se ut eller hvilket verktøy som skal benyttes. Datatilsynet har utarbeidet to enkle maler for behandlingsprotokoll som kan brukes for å holde oversikt.

Oversikten skal være et levende dokument som er oppdatert til enhver tid. Det er derfor viktig å sørge for gode rutiner for gjennomgang og vedlikehold av en slik oversikt. Vi mener det kan være en fordel å koble på en systemeier/rolle som ansvarlig for hvert digitalt læringsverktøy. På denne måten er det større sannsynlighet for at verktøyet blir vurdert, innført i kommunens behandlingsprotokoll/oversikt og fulgt opp.

11.6 Annen relevant veiledning:

- **Digitaliseringsdirektoratet (Digdir)**
  - Foranalyse med identifikasjon av informasjonstyper
- **KS**
  - Hva må jeg gjøre før jeg kan ta i bruk en ny digital tjeneste?
  - Slik sikrer du oppfølging av personvern og informasjonssikkerhet
- **Datatilsynet**
  - Protokoll over behandlingsaktiviteter

12. Administrasjon av ordinær drift og vedlikehold

12.1 Datatilsynets krav om redegjørelse

I brevkontrollen ba Datatilsynet kommunene om å beskrive hvordan de administrerer de digitale læringsverktøyene som allerede er implementert og i bruk. Vi ba derfor kommunen om å:

9.1. Gi en liste over roller på skolen eller i kommunen som har brukerrettigheter i operativsystemet for å administrere enhetsinnstillinger.
9.2. Redegjør for hvilke roller som har ansvar for ordinær drift av digitale læringsverktøy, for å følge opp samt implementere oppdateringer.
9.3. Legg ved kommunens rutiner for operativ drift, vedlikehold samt opphør av programvarelisens knyttet til digitale læringsverktøy.

12.2 Personvernregelverkets krav til personopplysningssikkerhet

Artikkel 32 i personvernforordningen omhandler plikten til å ivareta sikkerheten ved behandling av personopplysningene, også kalt personopplysningssikkerhet. Den behandlingsansvarlige er forpliktet til å gjennomføre egnede tekniske og organisatoriske tiltak slik at behandlingen oppnår et sikkerhetsnivå som er egnet med hensyn til risikoen, jf. personvernforordningen artikkel 32 nr. 1. Ved vurderingen av hva som er et egnet sikkerhetsnivå, skal det særlig tas hensyn til risikoene forbundet med behandlingen, for eksempel som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet, jf. nr. 2.

Ifølge personvernforordningen artikkel 32 er den behandlingsansvarlige videre forpliktet til å ha evne til vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene- og tjenestene. Videre fremkommer det at den behandlingsansvarlige skal ha evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse.

Personopplysningssikkerhet omfatter:

- **Konfidensialitet** – at informasjonen ikke blir kjent for uvedkommende. Å sørge for konfidensialitet krever at de som konfigurerer, vedlikeholder og drifter systemer og applikasjoner, har kompetanse til å sette opp tilganger og rettigheter på riktig måte.
- **Integritet** – at informasjonen ikke blir endret utilsiktet eller av uvedkommende. Feil i autentisering eller autorisering kan medføre at uvedkommende kan endre informasjon i systemer som brukeren ikke skulle hatt tilgang til.

- **Tilgjengelighet** – at informasjonen er tilgjengelig for autoriserte ved behov. Personopplysningenes tilgjengelighet kan sikres ved at roller, brukere, systemer og applikasjoner vedlikeholdes og holdes oppdatert til enhver tid.
- **Robusthet** – at organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser. Dette innebærer at arbeidet med personopplysningssikkerhet må være en kontinuerlig prosess.

For å sørge for tilstrekkelig personopplysningssikkerhet må kommunene ha riktig kompetanse i riktige roller. Aktuelle roller må besitte teknisk kompetanse når det gjelder drift og vedlikehold av systemer og plattformer.

12.3 Kommunenes besvarelser

12.3.1 Har Datatilsynet mottatt en oversikt over roller med administrasjonsrettigheter?

Antall svar: **50**

Svar	Antall	% av svar	Diagram
Ja	39	78 %	78%
Delvis	10	20 %	20%
Nei	1	2 %	2%

Datatilsynet ba kommunene om å sende en liste med roller som har brukerrettigheter i operativsystemet for å administrere enhetsinnstillinger. Vi mottok svært varierende svar fra kommunene på dette punktet. Flere kommuner har i tekstform gitt en overordnet beskrivelse av navn på de forskjellige rollene, mens andre kommuner har kun beskrevet hvilken enhet eller organisasjon som har ansvaret for at ordinær drift og vedlikehold gjennomføres. I noen tilfeller beskrev kommunen hvilken enhet eller organisasjon som har ansvar, men de kunne ikke redegjøre for hvilke roller eller kompetanse disse besitter. Enkelte kommuner har oversendt en komplett liste med alle roller i alle systemer som har en form for tilgangsstyring og behandler personopplysninger.

12.3.2 Kommunens redegjørelse for roller og ansvar for ordinær drift av digitale læringsverktøy, for å følge opp og implementere oppdateringer

Flertallet av kommunene har gitt oss tilstrekkelig dokumentasjon på hvilke roller som har et slikt ansvar og hvor de organisatorisk er plassert. Ti av kommunene har delvis oppfylt kravet ved å beskrive hvilken organisatorisk enhet ansvar ligger hos, uten å gi detaljer om hvilke roller som har det gjennomførende ansvaret for drift og vedlikehold. Én kommune har ikke kunne redegjøre for hvordan drift og vedlikehold er organisert eller hvilke roller som har et ansvar for gjennomføring.

Det er et stort spenn i hvordan kommunene har valgt å organisere seg knyttet til dette ansvaret. Flere kommuner deltar i et interkommunalt IKT-samarbeid hvor man har etablert en sentral IKT-driftsorganisasjon. Andre kommuner er medeier i eller kjøper tjenester, herunder drift og vedlikehold, fra private IKT-selskaper. Mindretallet av kommunene organiserer IKT-drift og vedlikehold selv.

Datatilsynet observerer at det også er et stort spenn i hvilke roller for drift og vedlikehold kommunene opererer med. Flertallet av kommunene har satt hele ansvaret til roller i de interkommunale IKT-samarbeidene, eller hos en sentralisert IKT-avdeling i kommunen. Enkelte av kommunene har ikke en sentralisert løsning på drift og vedlikehold, og ansvaret for oppdatering,

innføring eller utfasing av applikasjoner ligger til hver enkelt skole. Dette gjelder også for administrasjon av tilgangsstyring, hvor enkelte kommuner har skoler hvor rektor og/eller inspektør har ansvaret for å gi tilgang til elevene.

Enkelte av kommunene har delt ansvaret på flere nivåer. Eksempelvis har en kommune lagt ansvaret for opprettelse og administrasjon av konto for enheten til sentral IKT-avdeling, mens noe ansvar som oppsett og administrering av enkelte applikasjoner er delegert til skolekonsulenter og lærere. Eksempler på slike applikasjoner eller tjenester er Skolestudio og Salaby levert av Gyldendal. Noen kommuner har skolen ansatt IKT-rådgivere eller pedagogisk IKT-konsulenter som blir delegert enkelte IKT-oppgaver og fungerer som et bindeledd mellom skolen og sentral IKT-avdeling i kommune eller interkommunal IKT-organisasjon.

Nedenfor har vi trukket frem to eksempler på hvordan kommuner har lagt opp fordeling av ansvaret knyttet til drift, vedlikehold og tilgangsstyring.

Eksempel

En kommune som har inndelt ansvaret i fem områder:
1. Tjenesteansvarlig
2. Systemeier
3. Systemkoordinator
4. tjenestekoordinator
5. Personvern og informasjonssikkerhet.
Antall og hvilke roller som brukes endres etter hvilke typer applikasjon, plattform eller system det gjelder.

Eksempel

En annen kommune har inndelt ansvaret i 3 nivåer:

1. *IKT-ansvarlig med sentral IKT-avdeling i kommunen. Overordnet teknisk ansvar og full administrativ tilgang til innstillinger i operativsystem og digitale enheter. Ansvaret innebærer blant annet konfigurering av policyer og brukerrettigheter.*
2. *Digitaliseringskoordinator ved skole. Ansvar for enklere administrasjon og lokal brukertilgang. Fører protokoll og deltar inn i arbeid med risikovurdering og oppfølging av personvern*
3. *Enkelte lærere. Utvidede rettigheter for klasseadministrasjon.*

12.3.3. Har kommunen dokumentert en hensiktsmessig rollefordeling?

Antall svar: **50**

Svar	Antall	% av svar	Diagram
Ja	33	66 %	66 %
Delvis	14	28 %	28 %
Nei	13	6 %	6 %

Overordnet ser Datatilsynet at flertallet av kommunene kun unntaksvis legger administratorrettigheter for utstyr, operativsystem og innstillinger til personer uten IKT-spesialkompetanse. I andre tilfeller oppgir kommunene at skoleleder eller enkelte lærere kan få administratorrettigheter og ansvar for å utføre operativ drift og vedlikehold *der det er relevant*.

Det kommer tydelig frem for Datatilsynet at kommunene er forskjellig stilt når det gjelder ressurser til ordinær drift, vedlikehold og tilgangsstyring. Noen av kommunene har en stor sentralisert IKT-organisasjon hvor ansvar er fordelt etter type system eller fagområde, mens andre kommuner har alt fra to til fem ressurser med et totalansvar for 700-1000 skoleelever.

Datatilsynet ser også tilfeller av at noen kommuner som benytter flere plattformer (Apple, Google, Microsoft) i skolen, har forskjellig roller med ansvar for enkelte plattformer. Et eksempel er en kommune som både benytter nettbrett med Apple operativsystem, laptoper med Windows operativsystem og Google Chromebooks. For nettbrettene med iOS og laptoper med Windows er det det interkommunale IKT-selskapet som har ansvar for drift, vedlikehold og tilgangsstyring, mens for Google Chromebooks er det skolene som har ansvaret og sitter med administrasjonsrettigheter.

Datatilsynet observerer at selv i en brevkontroll med kun 50 respondenter så er det et stort spenn i hvordan kommuner løser ansvaret knyttet til dette ansvarsområdet. For å eksemplifisere dette vil vi trekke frem to besvarelser fra brevkontrollen:

Eksempler

Et eksempel der Datatilsynet vurderer rollefordeling som god:
Verken skole- eller kommuneansatte har administrasjonsrettigheter i operativsystemet for å legge til/fjerne/endre innstillinger. Dette er satt ut til interkommunalt IKT-selskap.

Et eksempel der Datatilsynet vurderer at rollefordeling i kommunen er mangelfull:
Rektor og én annen ansatt på skolen har administratortilgang for alle Chromebooks. Det jobbes med å få til en ny ansvarsfordeling, men det trekker ut i tid.

12.3.4 Har kommunen oversendt rutiner for operativ drift, vedlikehold samt opphør av programvarelisens knyttet til digitale læringsverktøy?

Antall svar: **50**

Svar	Antall	% av svar	Diagram
Ja	19	38 %	
Delvis	14	28 %	
Nei	17	34 %	

Datatilsynet ba kommunene om å oversende deres rutiner for operativ drift, vedlikehold og opphør av programvarelisens knyttet til digitale læringsverktøy.

Det er stor variasjon blant kommunene når det kommer til kvaliteten på rutinene som er oversendt i forbindelse med brevkontrollen. Noen kommuner viser et høyt modenhetsnivå med tydelige og reviderte rutiner. Det er godt beskrevet hvilket ansvar som ligger til hvilke roller. Rutinene hører til en overordnet struktur i et styringssystem. Andre kommuner har etablerte rutiner, men de mangler ofte en oversiktlig struktur, eller sammenheng med et helhetlig styringssystem. Enkelte kommuner viser lav modenhet. Disse har kun oversendt uformelle beskrivelser av rutinene, og i noen tilfeller har kommunen svar at de ikke har noen rutiner knyttet til operativ drift, vedlikehold eller opphør av programvarelisens.

Flere av kommunene har generelle rutiner for dette som ikke gjelder digitale læringsverktøy spesielt. De generelle rutinene er i mange tilfeller godt dekkende også for disse verktøyene. Enkelte kommuner har beskrevet rutinene sine uten å legge de ved som vedlegg i brevkontrollen.

34% av kommunene svarte at de ikke har nevnte rutiner eller at disse er under utarbeidelse. Det er også flere kommuner som har enkelte rutiner, men som verken er datert eller signert av ansvarlig ledelse. Dette kan enten skyldes at det er gjort uttrekk fra et styringssystem uten at metadata som dato følger med, eller det kan skyldes at rutinene ikke er en del av en systematikk eller inngår i et styringssystem.

Svarene fra brevkontrollen viser at kommunene organiserer rutinene sine på forskjellige måter. Enkelte kommuner har rutiner som gjelder et veldig avgrenset område som eksempelvis «*vedlikehold og oppdatering av apper på plattform A*». Andre kommuner har mer vidtrekkende retningslinjer eller rutiner som tar for seg flere områder, eksempelvis at kommunen har sammenstilt flere rutiner inn i et større dokument med tittel «*Policy for informasjonssikkerhet i kommune A».*

Datatilsynet observerer at slike rutiner ofte er en del av en Service Level Agreement (SLA), når en kommune deltar i et interkommunalt IKT-samarbeid. En SLA er en avtale mellom leverandøren og kommunen som konkretiserer forpliktelser og hvilket servicenivå leverandøren forplikter seg til. I tillegg henviste flere kommuner til eksisterende retningslinjer for databehandleravtaler der det er satt krav til hva som skal skje med personopplysningene etter at behandlingen av personopplysninger er stanset eller en tjeneste opphører.

Flere av kommunene viser til sine interkommunal IKT-selskaper når det gjelder rutiner for operativ drift. Svarene indikerer at mange av kommunene ikke er kjent med hvordan rutinene er etablert eller operasjonalisert i disse IKT-selskapene.

12.4 Datatilsynets vurdering

Vi mener det er bekymringsverdig at flere av kommunene ikke kunne vise til en komplett oversikt over roller som har administrasjonsrettigheter for digitale enheter, systemer og applikasjoner i kommunen. For at kommunen skal sørge for tilstrekkelig personopplysningssikkerhet, så forutsettes det kontroll over hvilke roller som har hvilket ansvar.

Videre mener Datatilsynet at det er bekymringsverdig at noen kommuner har gitt administrasjonsrettigheter og ansvar for å styre tilgang til enheter i skolen til rektor eller enkelte ansatte i skolen. Slike oppgaver av bør forvaltes av roller med tilstrekkelig kompetanse innenfor IKT.

Datatilsynet har gjennom brevkontrollen sett at flere av de kontrollerte kommunene har et strukturert og godt styringssystem med dekkende rutiner for dette ansvarsområdet. Flere av kommunene som viser høy modenhet på dette området har basert seg på Foreningen Kommunal Informasjonssikkerhet (KiNS) sin veiledning om styringssystem for informasjonssikkerhet.[24] Datatilsynet er likevel overrasket over at flertallet av kommunene mangler, eller delvis mangler, rutiner knyttet til operativ drift og vedlikehold av digitale læringsverktøy. Skriftlige rutiner er et sentralt krav i personvernforordningen for å kunne dokumentere etterlevelse av regelverket. Rutiner er også viktig for å sikre den behandlingsansvarliges kontroll med at oppgaver knyttet til personopplysningssikkerhet og personvern blir gjennomført i tråd med regelverket, og at dette ikke blir personavhengig.

12.5 Veiledning

12.5.1 Hvordan kan kommunen holde kontroll på identiteter og tilganger?

I Nasjonal Sikkerhetsmyndighets (NSM) grunnprinsipper er det et eget kapittel for hvordan ha kontroll på identiteter og tilganger. Målet med prinsippet er at virksomheten har oversikt over identiteter og kontoer i informasjonssystemene og styrer tilgang til ressurser effektivt og i henhold til virksomhetens retningslinjer.[25]

Å ha kontroll over alle identiteter og tilganger i kommuneorganisasjonen er viktig for å sikre at uvedkommende ikke kan få tilgang til en legitim brukerkonto i informasjonssystemet. Like viktig er det at en identitet eller bruker har riktig type tilgang til tjenestene som benyttes. En identitet eller brukerkonto skal ikke ha rettigheter utover det som er nødvendig ut ifra et tjenstlig behov. En identitet eller bruker som har rettigheter utover dette er et attraktivt mål for en angriper som forsøker å utnytte IKT-systemene til kommunen. Datatilsynet anbefaler derfor at det kun er personell med riktig kompetanse som administrerer identiteter og tilganger i organisasjonen. Administrasjon av tilgangsstyring er et løpende og systematisk arbeid som bør inngå i kommunens internkontroll og styringssystem.

12.5.2 Hvordan kan kommunen organisere operativ drift og vedlikehold av digitale læringsverktøy på en måte som ivaretar personvernet?

Det er grunnleggende for kommunen å ha et oppdatert og oversiktlig styringssystem som gir klare retningslinjer og rutiner for hvordan drift og vedlikehold skal styres, operasjonaliseres og kontrolleres. Arbeidet med operativ drift og vedlikehold omfatter både systemer og tjenester samt

[24] KiNS, styringssystem for informasjonssikkerhet, https://www.kins.no/verktoeykasse/kins-styringssystem/
[25] NSM, grunnprinsipper for IKT-sikkerhet, Punkt 2.6, https://nsm.no/getfile.php/1313975-1717589722/NSM/Filer/Dokumenter/Veiledere/NSMs%20Grunnprinsipper%20for%20IKT-sikkerhet%20v2.1.pdf

identiteter, brukerkontoer og andre tekniske innretninger som behandler personopplysninger. Arbeidet med informasjonssikkerhet og personopplysningssikkerhet i en virksomhet er en løpende prosess som omfatter hele livssyklusen til systemene og tjenestene kommunen benytter.

Det finnes flere rammeverk som virksomheter kan benytte for å sørge for tilstrekkelig god drift og vedlikehold av sine systemer og tjenester. Vi har i denne delen av rapporten tatt utgangspunkt i KiNS sitt styringssystem, da dette har kommuner som målgruppe. KiNS har en verktøykasse som inneholder ulike dokumenter for temaer knyttet til drift og vedlikehold, og som kan implementeres kommunens styringssystem. Eksempelvis finnes det maler for risikohåndteringsplan, risikoregistrering, policy for tilgangsstyring, prosedyre for innhenting av trusselinformasjon og prosedyre for sårbarhetskartlegging av IT-systemer.[26]

KiNS anbefaler at kommunene skal ha et styringssystem for informasjonssikkerhet som baserer seg på standarden ISO 27001. Ved å systematisere arbeidet og bruke et styringssystem som baserer seg på ISO 27001, kan kommunene redusere risiko for sikkerhetsbrudd, standardisere flere prosesser og forbedre informasjonssikkerheten over tid.

Datatilsynet ønsker også å trekke frem Digitaliseringsdirektoratets veiledning om internkontroll i praksis og informasjonssikkerhet. Veilederen er et godt verktøy for ledere som skal implementere og styre internkontroll i en virksomhet.

12.6 Annen relevant veiledning

- **Norsk sikkerhetsmyndighet (NSM)**
  - Grunnprinsipper for IKT-sikkerhet. NSM lister opp flere anbefalte tiltak vedrørende å ha kontroll på identiteter og tilganger. Datatilsynet viser spesielt til tiltak med ID 2.6.1 og 2.6.2 som relevant for temaet i brevkontrollen.
  -
- **Foreningen kommunal informasjonssikkerhet (KiNS)**
  - Styringssystem for informasjonssikkerhet
- **Digitaliseringsdirektoratet (Digdir)**
  - Internkontroll i praksis og informasjonssikkerhet

[26] KiNS, Styringssystem, https://www.kins.no/verktoeykasse/kins-styringssystem/

Del 3 – Frivillige spørsmål i brevkontrollen

13. Utfordringer, ønsker og praksis med kommunenes egne ord

Vi stilte kommunene følgende tre spørsmål de kunne velge å svare på:

1. **Hva ser kommunen som den største utfordringen i arbeidet med å ivareta elevenes personopplysninger ved bruk av digitale læringsverktøy?**

2. **Hva ønsker dere at Datatilsynet bistår med i forbindelse med kommunens ivaretakelse av personopplysningssikkerheten i digitale læringsverktøy?**

3. **Bruker kommunen annonseblokkeringsverktøy og/eller hvitlisting/svartelisting av nettsider på kommunens enheter? Beskriv gjerne hvilke verktøy som brukes.**

Av de 50 utvalgte kommunene som mottok brevkontrollen, svarte 37 på det første spørsmålet, 34 på den andre, og 41 på det siste. 8 avsto fra å svare på disse frivillige spørsmålene.

Svarene er tolket og kategorisert etter gjentakende temaer, og illustrert i grafer og sitater. En kommune kan ha beskrevet ett eller flere av disse temaene i sin besvarelse.

Ettersom vi har stilt spørsmålene til et avgrenset utvalg av kommuner, og det var frivillig å svare, må grafene forstås som visuelle fremstillinger av svarene til kommunene som valgte å svare på spørsmålene, og reflekterer ikke situasjonen for alle landets kommuner.

13.1 Hva ser kommunen som den største utfordringen i arbeidet med å ivareta elevenes personopplysninger ved bruk av digitale læringsverktøy?

Antall svar: **37**

Svar	Antall	% av svar	Diagram
Teknisk og/eller juridisk kapasitet	25	68 %	68%
Teknisk og/eller juridisk kompetanse	18	49 %	49%
Motstridende signaler mellom læreplan og GDPR (uklarheter i personvernlovgivningen)	4	11 %	11%
Mangelfull informasjon fra leverandør	21	57 %	57%
Krevende med opplæring av lærere/nå ut med felles retningslinjer for hele organisasjonen	14	38 %	38%

13.1.1 Teknisk og/eller juridisk kapasitet

25 av de 37 som valgte å svare på dette spørsmålet gir uttrykk for at det er begrensede tilgjengelige ressurser som hindrer dem i arbeidet med å ivareta elevenes personopplysninger.

Kommunene forteller at kapasitetsutfordringen primært skyldes to forhold:

Prosessen frem til godkjenning av nye verktøy er ressurskrevende:

«Lærere ønsker stadig å bruke nye verktøy som krever grundige risikovurderinger og DPIA. Der opplever vi å være til hinder for pedagogisk utvikling og bruk, da vi opplever å ha for lite kapasitet kommunalt. Vi avslår eller bruker altfor lang tid på å skulle godkjenne verktøy.»

Kontinuerlig oppfølging av digitale læringsverktøy:

«De digitale læringsverktøyene oppdateres jevnlig, og leverandører kan endre avtaler og praksis for behandlingen av data. Det mangler ressurser for å overvåke og revidere avtaler, for å sikre at kravene til personvern ivaretas.»

«En helhetlig systemforvaltning av hele porteføljen inkluderer oppfølgning av leverandører og oppdatering av ROS og DPIA. Dette arbeidet er noe underkommunisert i de nasjonale diskusjonene om utfordringene i kommunene. Det meste handler om de første risikovurderingene, og det er stort sett fokus på å få på plass ROS og DPIA.»

13.1.2 Teknisk og/eller juridisk kompetanse

Vurderingsarbeidet krever ikke bare ressurser, men også tilgang på den riktige kompetansen. 18 av de 37 som svarte på dette spørsmålet mener mangel på kompetanse er en stor utfordring.

Er det mer krevende for små kommuner enn for store?

«Å gjennomføre risiko- og sårbarhetsanalyser, DPIA-er, gjennomgå databehandleravtaler og holde behandlingsprotokoller oppdaterte innebærer kompetanse små og mellomstore kommuner ofte ikke har. Ofte vil små og mellomstore kommuner godkjenne eller overse risikoer de ikke har forutsetninger for å forstå.»

Økt kompleksitet krever økt kompetanse

«Læringsplattformer blir stadig mer avanserte. Bruk av kunstig intelligens og chatboter og personaliserte løsninger gjør det enda vanskeligere å forstå hvordan og hvor data lagres, spesielt ved bruk av skytjenester og tredjepartsaktører.»

«Mange kommuner mangler nødvendig kompetanse til å gjennomføre grundige vurderinger, særlig innenfor juridisk kompleksitet (tolkning av GDPR, opplæringsloven og offentlige anskaffelser), tekniske aspekter (variasjon i sikkerhetsstandarder og integrasjoner mellom ulike plattformer) og utvikling av KI og chatboter (behov for en felles forståelse av hvordan kunstig intelligens påvirker personvern og datasikkerhet i skolen).»

13.1.3 Mangelfull informasjon fra leverandører

21 av kommunene som svarte på dette spørsmålet mener at enkelte trekk ved leverandørene av digitale verktøy bidrar til at det blir utfordrende å ivareta elevenes personvern. Det er særlig fire forhold de trekker frem:

Leverandørene gjør endringer uten å si ifra

«Det var nok enklere før, når en faktisk måtte installere oppdateringer, men i dagens verden, der oppdateringer skjer over natten, og mange ganger uten at en merker det, kan slike endringer være vanskelige å fange opp.»

Verktøyene er ikke nødvendigvis laget for skole

«Den største utfordringen er at landskapet av leverandører og applikasjoner rettet mot skolen og elever er veldig stort. Dette gjelder alt fra apper som er spesialutviklet av pedagoger for barns læring i skolen, til gratisapper som av en lærer kan oppleves å være et morsomt supplement til læring i skolehverdagen. Det er derfor også stort spenn i hvilket fokus de ulike leverandørene har når det gjelder personvern for elevene.»

Kommunikasjon med leverandørene er utfordrende

Enkelte kommuner opplever at de ikke får nok informasjon fra leverandøren, andre opplever at de får motstand når de stiller kritiske spørsmål eller krever å bruke sin egen mal for databehandleravtale.

«En annen utfordring er manglende informasjon fra leverandører om løsningene de selger. Leverandørene burde kunne si noe om rett og trygg bruk av deres løsning, anbefalte organisatoriske tiltak, hvilke personopplysninger som behandles og hvilke tekniske tiltak som er mulig i løsningen (valgmuligheter).»

«Når det stilles spørsmål ved de løsningene som tilbys opplever vi også ofte et slags press fra leverandøren om å akseptere løsninger eller betingelser som gir et dårlig personvern, når en rekke kommuner allerede (på mer eller mindre godt grunnlag) har tatt i bruk løsningen de presenterer.»

«En ytterligere utfordring er at det finnes mange ulike databehandleravtaler, som alle kan dekke de krav som lovverket og kommunen stiller. Det er imidlertid kapasitetskrevende og utfordrende for kommunen å gjennomgå alle de ulike variantene som blir presentert. X kommune krever at vi får bruke vår egen mal, slik at vi har kontroll på innholdet i databehandleravtalene. Vi blir møtt med liten forståelse hos svært mange leverandører, og igjen møter vi holdninger som at «dette har allerede 60 kommuner godtatt».»

Behandlingen av personopplysninger i de digitale læringsverktøyene er uoversiktlige

Flere trekker frem lange verdikjeder og egenskaper ved enkelte digitale læringsverktøy som gjør det utfordrende å få oversikt over hvem og i hvilken grad det behandles personopplysninger i de ulike læringsverktøyene.

«Leverandørenes verdikjeder er etter hvert blitt lange og utfordrende å holde oversikt over. En leverandør av et digitalt læringsverktøy kan ha flere underleverandører, som igjen kan ha underleverandør på underleverandør. Dette gjør det i praksis svært komplisert å holde oversikt over

isfjellet som befinner seg under vannskorpen, og hvilke data som er innom hvem og hvor.»

«Flere av applikasjonene har utenlandske leverandører, der det er krevende å finne ut i hvilken grad personopplysninger behandles.»

«Enkelte leverandører av gratis applikasjoner inngår ingen databehandleravtale med kommunen hvis elevene ikke skal logge inn i appen. Å få oversikt over i hvilken grad disse leverandørene behandler elevens data, kan være en utfordring.»

13.1.4 Det er krevende å nå ut med felles retningslinjer for hele organisasjonen

14 av de 37 som svarte på dette spørsmålet synes det er vanskelig å få hele organisasjonen til å følge felles retningslinjer.

«Vi kan ikke garantere at lærere alltid sørger for at elevene kun logger inn på nettressurser som er aktivert i Feide. Mye handler om bevisstgjøring og opplæring, men det er krevende å nå ut til alle og sikre at dette forankres i hele organisasjonen.»

«[Det er en utfordring å] Sikre at alle er godt nok kjent med personvernet, og dets kompleksitet. Vi planlegger gjennomføring av kurs for ansatte, men ser utfordringer med å sikre at de ansatte tar dette på alvor og bruker det i skolehverdagen.»

13.1.5 Motstridende signaler mellom læreplan og GDPR

Fire av de 37 kommunene som valgte å svare på dette spørsmålet opplever at det er krevende å tilfredsstille kravene i læreplanen om å bruke digitale verktøy, læremidler og ressurser i det pedagogiske arbeidet, ivareta læreres handlefrihet og samtidig sørge for at elevenes personvern blir ivaretatt.

«Kommunens største utfordring med å sikre elevenes personopplysninger når vi bruker digitale læringsverktøy, er å finne en god balanse mellom solide personvernrutiner og de pedagogiske behovene.»

«Skolene får svært mange oppgaver som ofte kommer i tillegg til den tradisjonelle kjernevirksomheten. Dette utfordrer prioriteringsrekkefølgen. (…) Lærere baserer seg primært på pedagogiske kriterier når nye læremidler skal vurderes, og personvernskriteriene vurderes ikke alltid grundig nok.»

«Det er en utfordring å oppfylle kravene i opplæringsloven/læreplanverket og tilgjengeliggjøre de digitale verktøyene elevene skal lære/benytte, og samtidig ivareta hensynet til personvern og IKT-sikkerhet.»

«Lærere har i dagens læreplan veldig stor frihet til å legge opp undervisning og hvilke læringsverktøy de vil bruke. Lærere benytter seg av denne friheten i stor grad uten å, i mange tilfeller, ha noen form for kontroll på appens innhold eller informasjonssikkerhet og personvern.»

«Mange skoler ønsker mer dynamisk bruk av gratis ressurser. Dette for å skape variasjon i undervisningen. Det har vi sagt nei til. Det er likevel utfordrende å stå i presset fra lærere som ønsker å få ressurser.»

13.2 Hva ønsker dere at Datatilsynet bistår med i forbindelse med kommunens ivaretakelse av personopplysningssikkeheten i digitale læringsverktøy?

Antall svar: **34**

Svar	Antall	% av svar	Diagram
Sentralisert støtteverktøy for vurdering av digitale læringsverktøy	28	82 %	82%
Tydelige anbefalinger/veiledninger	22	65 %	65%
Tilsyn med leverandører av digitale læringsverktøy	3	9 %	9%

13.2.1 Sentralisert støtteverktøy for vurdering av digitale læringsverktøy

28 av de 34 kommunene som valgte å svare på dette spørsmålet ønsker at det krevende vurderingsarbeidet av digitale verktøy i skolen overlates til nasjonale myndigheter fordi:

«Det krever uforholdsmessig mye ressurser at hver enkelt kommune
skal gjøre mer eller mindre de samme vurderingene av databehandleravtaler, risiko og personvernkonsekvenser for slike applikasjoner.»

Noen beskriver konkrete forslag:

«Det hadde vært veldig nyttig for kommunene hvis en sentral aktør, med høy kompetanse på personvern, kunne hatt ansvar for å holde oversikt over hvilke apper og nettsider som er trygge i forhold til personvern. En form for nasjonal base med godkjente læringsverktøy som er kvalitetsstemplet av Datatilsynet.»

«En nasjonal kvalitetssikring kunne inkludert risiko- og sårbarhetsvurderinger av de mest brukte læringsplattformene og en nasjonal godkjenningsordning for tilbydere som tilfredsstiller krav til personvern og informasjonssikkerhet.»

13.2.2 Tydelige anbefalinger/veiledning

22 av de 34 kommunene som svarte på dette spørsmålet etterlyser veiledning, retningslinjer, praktiske eksempler og maler for å styrke deres eget vurderingsarbeid i kommunene.

«Det kunne evt. vært laget en veileder for skoleeiere (kommuner og andre) i samarbeid mellom Udir og DT som skisserte krav på systemnivå og anbefalte valg for skoleeier. Kunne vært framstilt i en framstilling som ga sjekkpunkter underveis i prosessen fra "initiativ til bestilling/opplasting av lærings-app".»

«Tydeligere retningslinjer for risikovurdering og DPIA i skolesammenheng. Det er utfordrende å avgjøre når en full DPIA er nødvendig for digitale læringsverktøy, spesielt for mindre verktøy med snevre bruksområder.»

«Balansen mellom pedagogiske behov og personvern. Vi søker veiledning i hvordan vi best kan kommunisere og forankre personvernhensyn i skolen, slik at både lærere og skoleledere får en felles forståelse av ansvaret.»

«Det ville vært nyttig å få praktiske eksempler og maler for ROS-analyser som er spesifikt rettet mot digitale læringsverktøy. (…) Datatilsynet kan spille en viktig rolle ved å tydeliggjøre hvordan behandlingsprotokoller for skole og utdanning kan føres på en god og effektiv måte.»

13.3 Annonseblokkeringsverktøy og hvitlisting/svartelisting av nettsider for å forhindre sporing

Som en del av de frivillige spørsmålene ba vi kommunene redegjøre for om bruk av annonseblokkeringsverktøy og/eller hvitlisting/svartelisting av nettsider på de digitale enhetene til elevene. Hensikten med stille dette spørsmålet var å få et innblikk i hvilke vurderinger kommunene har gjort hva gjelder filter og få en oversikt over hvilke spesifikke tjenester som er tatt i bruk.

Ved bruk av nettbaserte tjenester på elevenes enheter vil ulike selskaper kunne samle inn personopplysninger gjennom informasjonskapsler i nettleseren. Personopplysninger som typisk samles inn er informasjon om elevenes preferanser og atferd, stedslokasjon, hvilken informasjon det klikkes på, IP-adresse og hvor lenge brukeren er inne på en nettside. Disse dataene blir kjøpt og solgt på internasjonale børser for at markedsførere skal kunne utforme skreddersydde annonser. Selv om denne problemstillingen gjelder generelt for bruk av internett, har kommunen et særskilt ansvar for elevenes personopplysninger som følge av at de administrerer de digitale enhetene. Det stilles krav i personvernregelverket om at all behandling av personopplysninger må ha et rettslig grunnlag i personvernforordningen og opplæringslova, se nærmere redegjørelse under punkt 10.2.

Hva er en informasjonskapsel (cookie)?

En informasjonskapsel, ofte kalt cookie, er en liten tekstfil som lastes ned og lagres på datamaskinen når brukeren åpner en nettside. Informasjonskapselen brukes for eksempel til å lagre innloggingsdetaljer, huske handlekurv i nettbutikken eller registrere hvor brukeren beveger seg rundt på nettstedet.[1]

En tredjeparts informasjonskapsel settes av en annen enn den som driver nettstedet som brukeren besøker. Eksempel på dette er annonser og reklamebannere på nettaviser.[1]

IP-adresse

*En **IP-adresse** (Internet Protocol address) er en unik identifikator eller adresse som blir tildelt en enhet, for eksempel en PC eller nettbrett, for at de skal kunne skilles fra hverandre på internett.[1] Dette regnes normalt som en personopplysning fordi informasjonen ofte kan knyttes til en enkeltperson, jf. personvernforordningen artikkel 4 nr. 1.*

13.3.1 Kommunenes besvarelser

Det var 41 av 50 kommuner som besvarte dette frivillige spørsmålet.

Annonseblokkeringsverktøy

Et annonseblokkeringsverktøy er en programvare som fjerner reklame på en nettside eller inne i en applikasjon. Ut ifra besvarelsene er det kun fem kommuner som har installert annonseblokkeringsverktøy på elevenes enheter. Disse bruker blant annet tjenesten Adblock og Trend Micro Web security som er filterløsninger som stenger for reklame.

Annonseblokkeringsverktøy

Annonseblokkeringsverktøy kan blokkere forespørsler (requests) fra domener som har til hensikt å vise annonser. Ved blokkering av disse forespørslene vil ikke annonsøren kunne sette informasjonskapsler i brukerens nettleser. Dette forutsetter at IP-adressen eller domenet som sender en forespørsel allerede er registrert i filterlisten til annonseblokkeringsverktøyet. Annonseblokkeringsverktøyet har altså ikke blokkering av selve informasjonskapsler som funksjon.

Hvitlisting/svartelisting av nettsider

Det er flere kommuner som har innført alderstilpassede filter av nettsider i henhold til Utdanningsdirektoratet (Udir) sine anbefalinger fra høsten 2024.[27] Udir anbefaler filter som kun tillater tilgang til forhåndsdefinert innhold (hvitliste) for barneskolen, og filter som blokkerer tilgang til skadelig innhold (svarteliste) for ungdomsskolen. Av de 41 kommunene som svarte er det 23 som har innført svartelisting og 7 kommuner som har innført hvitelisting av nettsider. Dette er

[27] Utdanningsdirektoratet, Hvordan beskytte elever mot skadelig innhold på nett, udir.no/kvalitet-og-kompetanse/sikkerhet-og-beredskap/veileder-hvordan-beskytte-barn-mot-skadelig-innhold-pa-nett/?depth=0

gjennomført primært med tanke på å forhindre eksponering av skadelig innhold, men vil samtidig kunne redusere sporing av elevene på nett gjennom at kommunene har større kontroll på nettsidene elevene kan besøke, særlig ved hvitlisting.

Kripos sitt blokkeringsfilter

Det var videre 27 kommuner som opplyste om at de benyttet Kripos sitt blokkeringsfilter.
Kripos har laget en liste over nettsider som benyttes av voksne for å lokke til seg barn, sider for dating og seksuelle tjenester, som kan sperres. I april 2024 uttalte Stortinget at de sterkt anbefaler at alle kommuner installerer Kripos sitt blokkeringsfilter på elevenes digitale enheter. Kommunene kan få tilgang til listen ved å rette en forespørsel til kommunenes politikontakt som koordinerer med Kripos.

Øvrige filterløsninger

Kommunene har også innført andre typer filterløsninger som er tilpasset ulike aldersgrupper. Dette er eksempelvis å bruke Youtube i begrenset modus, Google safe Browsing som hindrer brukere i å besøke nettsider med uønsket innhold, eller Google safe search som forhindrer visning av søkeresultater av upassende innhold. Et annet eksempel er filteret «Safe Site URL» eller Microsoft Defender som tar vekk nettadresser som kategoriseres som pornografiske. Apple har også et innholdsfilter mot vold og pornografisk innhold som benyttes av enkelte kommuner. Andre kommuner informerer om at de har blokkert sosiale medier for barneskolen og delvis for ungdomsskolen.

Del 4 – Avslutning og veien videre

Hovedmålet med denne rapporten har vært å presentere våre vurderinger av kommunenes besvarelser, sammen med praktisk veiledning til hvordan kommuner skal ivareta kravene til personvern og personopplysningssikkerhet ved bruk av digitale læringsverktøy til opplæringsformål. De digitale læringsverktøyene som benyttes i undervisningen i dag muliggjør innsamling, behandling og deling av personopplysninger i en helt annen skala enn tidligere. Dette medfører behov for at skolene og kommunene har høy bevissthet om personvernet til elevene.

Datatilsynet anbefaler at arbeidet med personvern i skolen samordnes og effektiviseres i fremtiden. Det er ikke hensiktsmessig at hver kommune skal gjennomføre de samme vurderingene hver for seg for hvert enkelt læringsverktøy som skal tas i bruk.

Utdanningsdirektoratet (Udir) har på oppdrag fra Kunnskapsdepartementet (KD) startet et utredningsarbeid for hvordan en støttetjeneste for personvern, informasjonssikkerhet og universell utforming for digitale læremidler i skolen og barnehagen kan se ut. I digitaliseringsstrategien for skolene fra 2023 er et av tiltakene å etablere en offentlig forvaltet nasjonal tjenestekatalog for digitale læremidler.[28] Formålet med en slik tjenestekatalog er å gi kommuner og skoler bedre oversikt i markedet, samtidig som den skal sikre valgfrihet og et rikt tilbud. Katalogen kan blant annet inneholde en oversikt over og en beskrivelse av digitale læremidler, informasjon om tilgjengelige lisenser, statistikk og analyse av bruk og dessuten vurderinger opp mot krav til personvern, universell utforming og målform.[29]

En nasjonal støttetjeneste vil kunne bistå kommunene med delvurderinger knyttet til personvern, kompetanseheving, erfaringsutveksling, informasjonsinnhenting og systematisering samt rådgivning i konkrete spørsmål. Dette mener Datatilsynet kan bidra til å løse mange av de personvernrettslige utfordringene kommunene står ovenfor i dag. Vi mener at kommunenes redegjørelser for hva de anser som utfordrende og trenger bistand til, under del 3 av samlerapporten, kan gi noen føringer for hva en støttetjeneste bør fokusere på.

Datatilsynet erfarer at tilsyn har stor oppdragende effekt ute i sektoren. Vi planlegger å gjennomføre ytterligere stedlige tilsyn med skolesektoren i kommuner i nærmeste fremtid. Vi ønsker også å sende ut et selvevalueringsskjema som gir kommunene en mulighet til å evaluere egen etterlevelse av personvernregelverket, basert på tema i brevkontrollen.

Vi håper at andre veiledningsaktører kan nyttiggjøre seg av funnene vi har presentert i denne rapporten og at dette arbeidet vil bidra til utviklingen av veiledningen de gir.

[28] Kunnskapsdepartementet, Strategi for digital kompetanse og infrastruktur i barnehage og skole, 2023, https://www.regjeringen.no/no/dokumenter/nou-2023-19/id2982722/?ch=5

[29] Læring, hvor ble det av deg i alt mylderet?, NOU 2023: 19, punkt 13.5.2, https://www.regjeringen.no/no/dokumenter/nou-2023-19/id2982722/?ch=5

Besøksadresse:
Trelastgata 3, Oslo

Postadresse:
Postboks 458 Sentrum,
0105 Oslo

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no