

Personvern i skytjenester

Leverandører av skytjenester må fylle de samme sikkerhetskravene som alle andre leverandører som skal behandle personopplysninger på deres vegne.

VEILEDNING | SIST ENDRET: 09.12.2021

De fleste barnehage- og skoleeiere tar i bruk skytjenester, og lar dermed eksterne leverandører behandle personopplysninger. Skytjenester kan være alt fra dataprosessering og datalagring, til programvare på servere som er eksternt tilgjengelig. De fleste av disse tjenestene behandler data utenfor Norge, og mange utenfor EU/EØS.

For å ta i bruk skytjenester må dere gjennomføre en risikovurdering av skytjenesten, og gjøre gode vurderinger rundt både personopplysningene leverandøren skal behandle og databehandleravtalen dere inngår.

[Veiledere om sikkerhetskrav som kan være aktuelle ved innkjøp av skytjenester \(SkoleSec/KS\)](#)

Personopplysninger i skyen

Når barnehagen eller skolen velger å ta i bruk skytjenester fra en ekstern leverandør, er normalt barnehage- eller skoleeier behandlingsansvarlig. Hvis leverandøren av skytjenesten behandler personopplysninger på vegne av barnehagen eller skolen, regnes leverandøren som en databehandler.

[Les mer om behandlingsansvarlig og databehandler \(Datatilsynet\)](#)

Oversikt over behandlingene

Barnehage- eller skoleeier skal ha oversikt over hvilke behandlinger av personopplysninger som foretas i skyen. [Dette kaller vi internkontroll.](#) Oversikten er nødvendig for at dere skal kunne ivareta pliktene deres.

Oversikten danner også grunnlag for risikovurderingene dere må gjøre.

Oversikten bør inneholde:

- hvilke opplysninger leverandøren av skytjenesten vil behandle og hvorfor de vil bli behandlet
- hvilket behandlingsgrunnlag som ligger til grunn for den behandlingen leverandøren skal gjøre
- om personopplysningene er særlig kategori
- sikkerhetstiltak
- hvor leverandøren lagrer opplysningene og om de overfører opplysningene til andre land
- personopplysningenes omfang
- hvem som behandler personopplysningene, og om leverandøren overfører opplysningene til andre

Risikovurdering og informasjonssikkerhet

Barnehage- og skoleeier skal gjennomføre en risikovurdering både før dere tar i bruk en skytjeneste, og ved endringer som kan påvirke risikobildet for personvern eller informasjonssikkerheten. Slike endringer kan være at skytjenesten endrer vilkår for lagring av personopplysninger, engasjerer nye underleverandører, nedgraderer sikkerhetsnivået eller endrer andre vilkår.

Ikke alle skytjenester er utformet slik at de ivaretar personopplysningene i tråd med personvernregelverket og retningslinjer dere har for behandling av personopplysninger. Når barnehagen eller skolen skal ta i bruk eksterne tjenester, har dere ansvaret for å kvalitetssikre og dermed også foreta en risikovurdering av tjenesten.

Dere må være sikre på at skytjenesten møter sikkerhetskravene dere har.

Viktige punkter til risikovurderingen

Når dere risikovurderer en skytjeneste er det mange punkter dere bør tenke på. De samme tingene må dere også vurdere når dere skal utforme databehandleravtalen med leverandøren.

- Vil barnehagen- eller skolens personopplysninger bli blandet sammen med opplysninger fra andre kunder? Hvordan håndterer leverandøren dette?
- Hvem hos leverandøren har tilgang på deres informasjon? Sikrer leverandøren god nok tilgangsstyring?
- Logger skytjenesten autorisert og uautorisert bruk?
- Lagrer eller overfører leverandøren personopplysningene til land utenfor EU/EØS? Dersom dere for eksempel gir en russisk underleverandør tilgang til å logge seg inn og se dataene deres, regnes dette som en overføring selv om

dataene kun er lagret på en server i Norge.

- Hvor lagrer leverandøren sikkerhetskopier og hvem har tilgang til disse? Hvis de lagrer sikkerhetskopien i utlandet må de følge reglene for lagring av personopplysninger i utlandet.
- Krypterer leverandøren opplysningene før de lagres i skyen? Er kommunikasjonen mellom dere og leverandøren kryptert? Er kommunikasjonen mellom leverandøren og underleverandører/datasenter kryptert? Hvem sitter på krypteringsnøkklene?
- Blir informasjonen slettet, og i så fall når? Leverandøren har ikke rett til å behandle personopplysninger etter at barnehagen eller skolen har bedt om sletting, eller å lagre personopplysninger lenger enn det som er regulert i databehandleravtalen.
- Har leverandøren et punkt i avtalen om at de kan bruke personopplysninger (eller eventuelt anonymiserte data) til egne formål, som for å forbedre egne tjenester? Dere behandler personopplysninger om barn og elever for allerede angitte formål. Hvis skolen registrerer karakterer i en skytjeneste, skal karakterene brukes til det opplæringsloven og forskriften sier at skolen kan bruke karakterer til. Skyleverandøren skal ikke ha mulighet til å bruke karakterene til andre ting, som til å lage en profil over «flinke» og «mindre flinke» elever som de kan selge videre til andre selskaper.
- Bruker leverandøren underleverandører? Alle disse skal fremgå av databehandleravtalen.

Det vil variere fra tjeneste til tjeneste hvor viktige de ulike punktene er. Dere må for eksempel stille andre krav til en tjeneste som behandler særlige kategorier av personopplysninger, som helseopplysninger, enn til en kalenderfunksjon som deler aktiviteter på skolen med foreldrene.

Sjekkliste

Før dere tar i bruk en skytjeneste bør dere gjennomgå disse stegene.

Gjennomfør en risikovurdering

[Se veiledning om risikovurdering](#)

Sørg for å ha en databehandleravtale med leverandøren

Dere må inngå en databehandleravtale med leverandøren av skytjenestene.

Vi anbefaler at dere bruker statens mal for databehandleravtale. Noen leverandører ønsker å bruke sin egen databehandleravtale. Da må dere lese avtalen nøye, gå gjennom punktene over og gjennomføre en risikovurdering. Vurder om databehandleravtalen og leverandøren sikrer personopplysningene dere er ansvarlige for på en god nok måte til at dere kan ta tjenesten i bruk. Er risikoen for stor, og databehandleravtalen ikke god nok, anbefaler vi at dere ikke tar i bruk tjenesten.

Få på plass nødvendig dokumentasjon

Sørg for at løsningen er tilstrekkelig dokumentert slik at du eller offentlige myndigheter kan gjennomføre en kontroll.

Eksempler på dokumentasjon du trenger er:

- en gjennomført risikovurdering av tjenesten
- databehandleravtale som er inngått med leverandøren
- dokumentasjon på eventuell løpende oppfølging av leverandøren.
- dokumentasjon fra egne revisjoner eller revisjoner dere ber andre om å gjøre på deres vegne