

Skytjenester og eksterne IT-tjenester i grunnopplæringen

Rettslige krav i
personopplysningsloven
med forskrift

VEILEDNING



Om Senter for IKT i utdanningen

Senter for IKT i utdanningen er et forvaltningsorgan under Kunnskapsdepartementet. Senterets oppgave er å bidra til at bruken av IKT i skolen styrker kvaliteten på undervisningen, øker elevenes læringsutbytte og utvikler deres læringsstrategier. Målgrupper for senteret er barnehagen, grunnskolen og videregående opplæring, i tillegg til førskolelærer- og lærerutdanningen.

Materialet i denne publikasjonen er omfattet av åndsverklovens bestemmelser. Materialet i denne publikasjonene er videre tilgjengelig under følgende Creative Commons-lisens: Navngivelse-DelPåSammeVilkår 3.0 Norge, jf.: <http://creativecommons.org/licenses/by-sa/3.0/no/>.

Det innebærer at du har lov til å dele, kopiere og spre verket, samt å bearbeide (remikse) verket, så fremt følgende to vilkår er oppfylt:

Navngivelse

Du skal navngi opphavspersonen og/eller lisensgiveren på den måte som disse angir (men ikke på en måte som indikerer at disse har godkjent eller anbefaler din bruk av verket).

Del på samme vilkår

Om du endrer, bearbeider eller bygger videre på verket, kan du kun distribuere resultatet under samme, lignende eller en kompatibel lisens.



Forord

Denne veiledningen gir en oversikt over hvilke krav personopplysningsloven med forskrift stiller når skoleeier setter ut behandlingen av personopplysninger til skytjenesteleverandører eller andre typer eksterne tjenesteleverandører.

Målgruppene for veiledningen er i første rekke skoleledere, skolefaglig ansvarlige hos skoleeier og IT-personell hos skoleeier. Den er også relevant for pedagogiske IKT-koordinatorer og ressurspersoner i skolene på bruk av IKT.

Veiledningen er inndelt i fem hoveddeler:

1. Den første delen drøfter hva som kjennetegner skytjenester og andre eksterne IT-tjenester, og nevner noen konkrete eksempler på slike tjenester i dagens grunnopplæring.
2. Den andre delen gir en kort oversikt over de relevante reglene i personopplysningsloven med forskrift.
3. I den tredje delen drøftes hvilke rettslige krav som stilles til eksternt drift av IT-tjenester hvor personopplysninger behandles.
4. Den fjerde delen drøfter hvilke spesielle rettslige utfordringer som skoleeiers bruk av skytjenesteleverandører reiser.
5. I den femte og siste delen gis en kort gjennomgang av rettslige krav i andre regelverk som har særlig betydning når skoleeier setter ut behandlingen av personopplysninger til skytjenesteleverandører (eller andre typer eksterne IT-leverandører).

Selv om denne veiledningen fokuserer på de reglene i personopplysningslovgivningen som er spesielt relevante når skoleeier anvender skytjenester og andre eksterne IT-tjenester, vil vi likevel understreke at alle de andre reglene i lovgivningen gjelder også her.

Skoleeier plikter derfor å ivareta de øvrige rettighetene og pliktene som gjennomgås i veiledningen "ABC i personvern for skoler og skoleeiere", utgitt av Senter for IKT i utdanningen¹. Her dreier det seg for eksempel om at det må foreligge en saklig grunn for behandlingen av personopplysninger, at det må foreligge et gyldig behandlingsgrunnlag (samtykke, lovhjemmel eller én av nødvendighetsgrunnene som nevnes i personopplysningsloven §§ 8 og 9), at kvaliteten på opplysningene skal være tilstrekkelig, at det ikke skal samles inn unødvendige opplysninger og at opplysningene skal slettes når det ikke lenger er behov for dem. Men fordi disse og andre bestemmelser gjelder ved all elektronisk behandling av personopplysninger og ikke spesielt ved bruk av skytjenester eller andre eksterne IT-tjenester, vil de ikke bli drøftet nærmere i denne veiledningen.

Innhold

Forord	3
01	
Innledning	6
Veiledningens formål	6
02	
Personopplysningsloven med forskrift	8
03	
Generelle rettslige krav ved bruk av skytjenester og eksterne IT-tjenester	10
Risikovurderinger	11
Sanksjoner	11
04	
Spesielle problemstillinger knyttet til skytjenester	12
Hvor personopplysningene lagres	12
Inngåelse av databehandleravtaler	13
Overholdelse av avtalevilkårene	13
05	
Andre lovmessige føringer	15

Del 1

Innledning

De aller fleste skoleeiere og skoler har satt ut driften av visse typer IT-tjenester til eksterne leverandører. Det som kjenne-tegner slike tjenester, er at de ikke driftes av den lokale IT-avdelingen hos skoleeier eller av den enkelte skolen. I stedet er det andre aktører som står for driften, for eksempel nabokommuner eller private og kommersielle selskaper.

Mange av disse IT-tjenestene fungerer slik at (1) ansatte og elever (eventuelt også foreldre/foresatte) logger seg på tjenestene over Internett og (2) de informasjonsverdier som produseres eller lagres (undervisningsopplegg, elevbesvarelser, vurderinger, e-poster, klasselister, møtereferater, osv.) overføres til og oppbevares på datamaskiner hos den eksterne tjenesteleverandøren. De fleste digitale læringsplattformer er eksempler på denne typen IT-tjenester, for eksempel Fronter, itslearning og PedIT.

Det samme gjelder for de mest brukte skoleadministrative systemene. I løpet av de senere årene har en ny type eksterne IT-tjenester blitt populære i grunnopplæringen. Dette er tjenester som går under samlebetegnelsen skytjenester (Cloud Computing). Det er etter hvert blitt ganske mange eksempler på skytjenester i grunnopplæringen. Slike tjenester omfatter blant annet Dropbox, YouTube, Moodle, Gmail, Hotmail, Google Apps for Education, Evernote, Microsoft Live@edu, Facebook og Twitter.

Mange av de nevnte skytjenestene er vanlige webtjenester som hver enkelt av oss kan velge å bruke (eller ikke). Men enkelte leverandører av skytjenester tilbyr seg også å drifte IT-tjenester på vegne av skoleeier, for eksempel e-post og andre typer applikasjoner. Dette innebærer at skoleeier overfører informasjonsverdier til tjenesteleverandøren og at leverandøren oppbevarer verdiene på sine datamaskiner. Brukerne (ansatte, elever og i enkelte tilfeller foreldre/foresatte) får tilgang til informasjonsverdiene og applikasjonene over Internett.

Samtidig leveres de mest populære av denne typen skytjenester av multinasjonale selskaper, for eksempel Microsoft eller Google. Dette innebærer at skolens informasjonsverdier (undervisningsopplegg, elevbesvarelser, vurderinger, e-poster, osv.) gjerne lagres på datamaskiner som befinner seg utenfor Norges grenser – maskinene kan i prinsippet befinne seg hvor som helst i verden. Også norske tilbydere av skytjenester kan benytte datamaskiner som befinner seg i utlandet. Som det fremgår av tidligere utgitt veiledning fra Senter for IKT i utdanningen – "Bak skyene er himmelen alltid blå? En innføring i Cloud Computing for skoleeiere"² – kan dette reise enkelte juridiske og personvernmessige utfordringer.

VEILEDNINGENS FORMÅL

Hensikten med denne veiledningen er å gi en oversikt over hvilke regler som gjelder når skoleeier lar eksterne leverandører behandle en bestemt kategori informasjonsverdier: personopplysninger. Personopplysninger er alle former for opplysninger eller vurderinger som kan knyttes til enkeltpersoner, og de kan foreligge som tekst, bilder, lyd- eller videoopptak³. Når skoleeier behandler personopplysninger elektronisk, skal dette skje i henhold til reglene i personopplysningsloven og personopplysningsforskriften⁴.

Personopplysningsloven med forskrift inneholder spesialregler for hva skoleeier må gjøre når den ønsker å overføre og lagre personopplysninger hos leverandører av eksterne IT-tjenester. Reglene gjelder derfor både for digitale læringsplattformer, skoleadministrative systemer, skytjenester og andre IT-tjenester som skoleeier ikke drifter selv. Fokuset vil imidlertid i særlig grad rettes mot skytjenester, fordi det kan oppstå spesielle utfordringer når skoleeier eller skolen ønsker å ta slike tjenester i bruk.

² Veiledningen er tilgjengelig på <http://iktsenteret.no/ressurser/bak-skyene-er-himmelen-alltid-bl-en-innf-ring-i-cloud-computing-skoleeiere>

³ Personopplysningsloven § 2 nr. 1.

⁴ Loven og forskriften er tilgjengelige på www.lovdato.no

Få husstander har et eget kraftverk i kjelleren. Når vi slår på lyset om morgenen, vet vi ikke hvor strømmen er produsert. Kommer den fra et norsk vannkraftverk, en dansk vindkraftfarm eller et svensk kjernekraftverk? Vi vet ikke, og de fleste av oss tenker ikke på det.

Slik ser mange for seg at skytjenester også skal fungere. Når lokale IT-tjenester er satt ut til skytjenesteleverandører, er de tilgjengelige over nettet når vi slår på datamaskinen om morgenen, akkurat som elektrisk kraft. Da trenger vi ikke en egen IT-avdeling for å drifte tjenestene, hevdes det. Og vi skal heller ikke trenge å bry oss om hvor tjenestene leveres fra – Norge eller et hvilket som helst annet land.

Del 2

Personopplysningsloven med forskrift

Personopplysningsloven med forskrift trådte i kraft 1. januar 2001, og baserer seg på EUs personverndirektiv fra 1995. Hensikten med reglene i loven og forskriften er å unngå krenkelser av personvernet når opplysninger om den enkelte behandles ved bruk av elektroniske hjelpemidler⁵. Reglene gjelder derfor i nesten alle sektorer, yrker eller bransjer hvor personopplysninger behandles ved hjelp av datamaskiner og programvare, inkludert skoler i grunnopplæringen.

Reglene i personopplysningsloven med forskrift er tidligere drøftet i veiledningen "ABC i personvern for skoler og skoleeiere", utgitt av Senter for IKT i utdanningen⁶. Her er sentrale begreper i regelverket definert og drøftet, og det gis eksempler på hvordan krenkelser av personvernet kan oppstå i en skolesammenheng. For å forstå systematikken i reglene som gjelder når personopplysninger behandles i eksterne IT-tjenester, er det likevel behov for en kort gjentakelse av enkelte av begrepene som drøftes i ABC i personvern-veiledningen:

- Sensitive personopplysninger: alle opplysninger eller vurderinger som kan knyttes til enkeltpersoner og som omhandler helse og helseforhold; etnisk eller rasemessig bakgrunn; politisk, religiøs eller livssynsmessig oppfatning; seksuell legning; strafferettslige forhold eller fagforeningsmedlemskap⁷. Sensitive opplysninger er blant annet informasjon om lærevansker, sosiale ferdigheter, sykefravær, kommunikasjonsevner, tyveri/skadeverk, fagforeningsvirksomhet og rusmisbruk eller alkoholisme i hjemmet.
- Almennelige personopplysninger: alle opplysninger eller vurderinger som kan knyttes til enkeltpersoner og som ikke er definert som sensitive. Informasjon om blant annet underveis- og sluttvurderinger, elevarbeider/innleveringer, faglig utvikling og kontaktinformasjon vil vanligvis være å regne som alminnelige personopplysninger.

- Den registrerte: vedkommende enkeltperson som opplysningene eller vurderingene dreier seg om. I grunnopplæringen er dette ansatte, elever og foreldre/foresatte⁸.
- Den behandlingsansvarlige: den virksomheten som behandler personopplysninger ved bruk av elektroniske hjelpemidler og som bestemmer hva opplysningene skal brukes til. I grunnopplæringen er skoleeier den behandlingsansvarlige⁹.
- Databehandlere: virksomheter som behandler personopplysninger på vegne av skoleeier (den behandlingsansvarlige). Leverandører av eksterne IT-tjenester – enten det dreier seg om nabokommunen som drifter skolens IT-systemer, kommersielle leverandører av læringsplattformer eller internasjonale tilbydere av fjerndriftsløsninger (Microsoft, Google osv.) – er databehandlere for skoleeier¹⁰.

Det er særlig forholdet mellom den behandlingsansvarlige og databehandleren som er avgjørende i denne sammenheng. Databehandleren er leverandøren av eksterne IT-tjenester som den behandlingsansvarlige (skoleeier) har satt ut driften til. Prinsippet er at skoleeier skal ha kontroll med hvordan leverandøren håndterer personopplysninger som skoleeier har et juridisk ansvar for.

Dersom skoleeier ikke forsikrer seg om at leverandøren forvalter personopplysningene på en rettslig forsvarlig og sikker måte, kan den registrerte – ansatte, elever og foreldre/foresatte – utsettes for personvernkrenkelser. Det kan skje hvis skoleeier ikke tydeliggjør hva leverandøren har lov å bruke opplysningene til eller unngår å stille krav til sikring av opplysningene:

⁵ Personopplysningsloven § 1.

⁶ Veiledningen er tilgjengelig på <http://iktsenteret.no/ressurser/abc-i-personvern-skoler-og-skoleeiere>

⁷ Personopplysningsloven § 2 nr. 8.

⁸ Personopplysningsloven § 2 nr. 6.

⁹ Personopplysningsloven § 2 nr. 4.

¹⁰ Personopplysningsloven § 2 nr. 5.

- Dersom skoleeier ikke stiller krav til sikring av personopplysningene, kan opplysningene eksponeres på uheldige måter, for eksempel ved at de tilflyter uvedkommende (personer som ikke har tjenestelige behov for å vite om opplysningene eller personer som den registrerte ikke har samtykket i utlevering til).
- Dersom skoleeier ikke tydeliggjør hva personopplysningene kan brukes til, kan leverandøren benytte dem på måter som den registrerte verken har samtykket til eller vet om (for eksempel til å formidle uønsket reklame til den registrerte, eller til å bygge opp detaljerte personprofiler).

Logikken er altså at når skoleeier overlater driften av IT-tjenester til eksterne leverandører, kan risikoen for krenkelseser av personvernet øke. På den annen side kan det tenkes at eksterne leverandører er mer ressurssterke og profesjonelle enn skoleeier, for eksempel når det gjelder å ivareta personvernet og informasjonssikkerheten. Men den usikkerheten som uansett oppstår når skoleeier overlater personopplysninger i en annen aktørs varetekt, gjør at bruk av fjerndriftede løsninger bare er lovlig dersom skoleeier har ivaretatt de relevante rettslige kravene i personopplysningsloven og personopplysningsforskriften. Skoleeiere som setter ut behandlingen av sensitive personopplysninger, bør være særlig nøye med at dette skjer på en rettslig forsvarlig måte¹¹. Men de samme rettslige kravene gjelder også når eksterne leverandører behandler alminnelige personopplysninger på vegne av skoleeier.

Hvilke rettslige krav som personopplysningsloven med forskrift inneholder, drøftes i del 3.

Mange skytjenester som brukes i grunnopplæringen, baserer seg ikke på at skoleeier inngår avtaler med leverandøren om drift av tjenesten. Dette er skytjenester av typen YouTube, Dropbox, Facebook eller Twitter, det vil si webtjenester hvor hver enkelt av oss (og ikke skoleeier) avgjør om vi ønsker å bruke dem. Her er det skytjenesteleverandøren som er den behandlingsansvarlige – leverandøren behandler ikke personopplysninger på vegne av skoleeier, men bestemmer selv hva opplysningene skal brukes til. Derfor kan det være lurt å lese leverandørens personvernerklæring før tjenestene tas i bruk for å sjekke hvordan opplysningene vil bli brukt.

Hvis skolen ønsker at elevene benytter denne typen skytjenester i undervisningen, er det ekstra viktig at ledere og lærere studerer personvernerklæringen kritisk. Dessuten bør elevene (eventuelt deres foreldre/foresatte) bes om samtykke før skytjenestene tas i bruk på skolen. Det kan også være hensiktsmessig om skoleeier har retningslinjer som sier noe om det er greit at lærere og ansatte bruker slike tjenester i det pedagogiske og administrative arbeidet.

¹¹ Slike opplysninger vil også være taushetsbelagte etter opplæringsloven § 15-1.

Del 3

Generelle rettslige krav ved bruk av skytjenester og eksterne IT-tjenester

Bestemmelsene som drøftes i denne delen, gjelder for all utsettelse av IT-drift hvor personopplysninger behandles, det vil si uavhengig av om det dreier seg om pedagogiske eller administrative tjenester og uavhengig av om tjenestene leveres av nabokommunen, en lokal IT-bedrift eller et multinasjonalt selskap. Kravene i personopplysningsloven med forskrift er altså i utgangspunktet de samme uansett hvilke IT-tjenester som settes ut og hvem tjenestene settes ut til.

I personopplysningsloven § 15 heter det at en databehandler (leverandør av eksterne IT-tjenester) ikke kan behandle personopplysninger på annen måte enn det som er skriftlig avtalt i en databehandleravtale med den behandlingsansvarlige (skoleeier). Leverandøren kan heller ikke overlate personopplysningene til andre selskaper/aktører (for lagring eller bearbeidelse) uten at dette fremgår av databehandleravtalen. Til slutt heter det at databehandleravtalen skal spesifisere at leverandøren plikter å overholde reglene om informasjonssikkerhet som følger av personopplysningsloven § 13 og personopplysningsforskriften kapittel to.

Disse bestemmelsene innebærer følgende:

1. Skoleeier plikter å inngå databehandleravtaler med leverandører av eksterne IT-tjenester dersom leverandørene behandler personopplysninger på vegne av skoleeier.
2. Databehandleravtalen skal inngås før skoleeier overfører personopplysninger til leverandøren av eksterne IT-tjenester.
3. Det skal fremgå av avtalen om leverandøren kan overføre personopplysninger til eventuelle underleverandører (eller andre aktører), for eksempel selskaper som leverandøren leier serverkapasitet av.
4. I databehandleravtalen skal skoleeier kreve at leverandøren iverksetter nødvendige tiltak for å ivareta informasjonssikkerheten til skoleeiers personopplys-

ninger. Dette er tiltak rettet mot å unngå brudd på opplysningenes konfidensialitet (hindre at opplysningene kommer uvedkommende i hende), integritet (hindre at opplysningene endres/manipuleres på uautoriserte måter) og tilgjengelighet (sikre at opplysningene er tilgjengelig for de som har rettmessig behov for dem).

Punkt 4 betyr at risikoen for brudd på personopplysningenes konfidensialitet, integritet og tilgjengelighet ikke skal være større enn hva skoleeier kan godta. Det er den daglige ledelsen hos skoleeier som har ansvaret for at informasjonssikkerheten ivaretas når eksterne leverandører behandler personopplysninger på vegne av skoleeier¹². Hos offentlige skoleeiere vil dette være rådmann/fylkesrådmann, mens i privateide skoler vil det være rektor/daglig leder ved hver utdanningsinstitusjon.

Skoleeier plikter videre å forsikre seg om leverandøren faktisk iverksetter de sikringstiltak som er nødvendige for å oppnå den graden av informasjonssikkerhet som skoleeier har bestemt. Skoleeier må derfor ha kunnskap om leverandørens sikkerhetsstrategi og sikkerhetsarbeid, og jevnlig påse at strategien følges opp av leverandøren. Dette fremgår også av personopplysningsforskriften § 2-15, 5. ledd. Vær også oppmerksom på at Datatilsynet krever kryptering av sensitive personopplysninger som overføres mellom skoleeier og leverandør ved bruk av usikre kommunikasjonsnettverk (for eksempel Internett)¹³.

Skoleeier bør også stille krav til hvordan tilbakeføringen av personopplysninger skal skje dersom samarbeidet med den eksterne leverandøren avvikes. Her kan det for eksempel avtales at opplysningene tilbakeføres på måter og i et format som er enkelt for skoleeier å håndtere, og at leverandøren forplikter seg til å slette alle kopier av personopplysningene.

Datatilsynet har laget en egen veileder om databehandleravtaler. Her forklares hva en databehandleravtale som minimum bør inneholde. Veilederen inneholder også en

¹² Personopplysningsforskriften § 2-3.

¹³ Se bl.a. Datatilsynets veileder i sikkerhetsarkitektur. Den er tilgjengelig på http://www.datatilsynet.no/templates/article_____3966.aspx.

skisse til hvordan en databehandleravtale som oppfyller kravene i personopplysningsloven med forskrift kan se ut¹⁴. Databehandleravtalen trenger ikke å foreligge som en egen avtale, men kan tas inn som en del av det generelle avtaleverket mellom skoleeier og leverandøren. Det er viktig å være oppmerksom på at leverandøren ikke kan endre databehandlerdelen av avtalen uten at skoleeier er blitt informert om og har godkjent endringene. Skoleeier må derfor undersøke om avtaleverket inneholder klausuler hvor leverandøren forbeholder seg retten til ensidig å endre avtalevilkårene. Hvis dette er tilfelle, må skoleeier sørge for at databehandlerdelen ikke omfattes av slike klausuler.

RISIKOVURDERINGER

Personopplysningsloven med forskrift krever at skoleeier gjennomfører en risikovurdering før driften av IT-tjenesten settes ut. Tilsvarende risikovurderinger skal gjentas med jevne mellomrom (for eksempel årlig) så lenge skoleeier benytter seg av tjenesten, og risikovurderingene skal dokumenteres¹⁵.

Det er informasjonssikkerheten som skal risikovurderes, det vil si om leverandørens IT-tjeneste og skoleeiers egen bruk av tjenesten oppfyller de kravene som skoleeier stiller til sikring av personopplysningenes konfidensialitet, integritet og tilgjengelighet. Risikovurderingen skal derfor ikke bare fokusere på sikkerhetsutfordringer som kan oppstå hos skoleeier, men bør omfatte hele driftsløsningen. Hvis risikovurderingen viser at sikringen av personopplysningene ikke er tilfredsstillende, kan ikke skoleeier ta tjenesten i bruk (eller fortsette å anvende tjenesten) uten at dette er i strid med reglene i personopplysningsloven med forskrift. I veiledningen "Sikker håndtering av personopplysninger i skolen", utgitt av Senter for IKT i utdanningen, forklares det hva risikovurderinger er og hvordan de kan gjennomføres¹⁶.

SANKSJONER

Det er skoleeier som er hovedansvarlig for at det gjennomføres risikovurderinger og at det foreligger en skriftlig avtale med leverandøren av IT-tjenester som oppfyller kravene skisert ovenfor. Leverandøren har samtidig et selvstendig ansvar for at kravene som skoleeier stiller i databehandleravtalen, spesielt når det gjelder sikring av opplysningenes konfidensialitet, integritet og tilgjengelighet, blir ivaretatt. Dette fremgår av personopplysningsloven § 13, 1. ledd.

Dersom Datatilsynet gjennomfører tilsyn hos skoleeier og oppdager manglende overholdelse av reglene om informasjonssikkerhet, risikovurderinger og databehandleravtaler, vil Datatilsynet fatte vedtak om at avvikene fra regelverket må rettes.

Ved alvorlige brudd på reglene kan Datatilsynet ilegge følgende sanksjoner¹⁷:

- For det første kan skoleeier straffes med bøter (overtredelsesgebyr) av Datatilsynet hvis personopplysninger overføres til leverandører uten at det er inngått en skriftlig avtale som oppfyller vilkårene i personopplysningsloven med forskrift.
- For det andre kan skoleeier straffes med bøter av Datatilsynet hvis det foreligger en databehandleravtale med leverandøren, men uten at skoleeier har sikret seg muligheter til å kontrollere at leverandøren overholder vilkårene i avtalen.
- For det tredje kan leverandøren straffes med bøter av Datatilsynet hvis vilkårene i databehandleravtalen ikke følges opp i praksis¹⁸.

Ved spesielt alvorlige regelbrudd kan Datatilsynet anmelde forholdet til politiet. I tillegg kan den registrerte (ansatte, elever eller foreldre/foresatte) kreve erstatning fra skoleeier og leverandøren hvis bruken av eksterne IT-tjenester fører til krenkelser av hans eller hennes personvern¹⁹.

¹⁴ Datatilsynets veileder og avtaleskisse er tilgjengelig på http://www.datatilsynet.no/templates/Page_____2747.aspx

¹⁵ Personopplysningsloven § 13, jf personopplysningsforskriften § 2-4 og §§ 2-11 til 2-13.

¹⁶ Veiledningen er tilgjengelig på <http://iktsenteret.no/ressurser/sikker-handtering-av-personopplysninger-i-skolen>

¹⁷ Datatilsynets vedtak om sanksjoner kan klages inn for Personvernemnda (se www.personvernemnda.no).

¹⁸ Sanksjonsbestemmelsene finnes i personopplysningsloven §§ 46-48.

¹⁹ Personopplysningsloven § 49.

Del 4

Spesielle problemstillinger knyttet til skytjenester

Selv om reglene drøftet i del 3, i utgangspunktet er de samme også ved utsetting av driften til skytjenesteleverandører, kan det oppstå spesielle utfordringer når skoleeier bruker skytjenester. Det skyldes at mange (men slett ikke alle) av disse tjenestene tilbys av selskaper som overfører personopplysninger til og lagrer opplysninger på datamaskiner i utlandet. Utfordringene for skoleeier blir derfor annerledes enn hvis behandlingen av personopplysninger settes ut til en nabokommune eller til et lokalt IT-selskap:

- For det første kan det være vanskelig for skoleeier å skaffe seg informasjon om i hvilket (eller hvilke) land leverandøren oppbevarer personopplysningene.
- For det andre kan det være vanskelig for skoleeier å få leverandøren til å godta de kravene som personopplysningsloven med forskrift stiller til databehandleravtaler.
- For det tredje kan det være vanskelig for skoleeier å kontrollere at vilkårene i databehandleravtalen overholdes av leverandøren.

Nedenfor gjennomgås hver enkelt av disse utfordringene.

HVOR PERSONOPPLYSNINGENE

LAGRES

Den første utfordringen har fått særlig stor oppmerksomhet i diskusjonen om skytjenester og personvern. Dette skyldes at kapittel fem i personopplysningsloven og kapittel seks i personopplysningsforskriften inneholder regler om overføring og lagring av personopplysninger i land utenfor EU/EØS-området. Hovedregelen er at skoleeier ikke kan overføre personopplysninger til skytjenesteleverandører i land som ikke har tilsvarende personverngarantier som de vi finner i EU/EØS-land. Derfor må skoleeier ha informasjon om hvor

personopplysningene havner, inkludert om skytjenesteleverandøren benytter seg av underleverandører som befinner seg utenfor EU/EØS-området.

Kravet til kontroll med hvor personopplysningene fysisk befinner seg gjelder også når skytjenesteleverandøren er et selskap etablert i Norge. Årsaken til dette er at det kan tenkes at selskapet overfører og lagrer personopplysninger på datamaskiner utenfor EU/EØS-området, for eksempel dersom selskapet benytter seg av utenlandske underleverandører.

Det betyr likevel ikke at det er et generelt forbud mot overføring av personopplysninger til land utenfor EU/EØS-området. Overføring og lagring av personopplysninger til land utenfor dette området kan skje på visse vilkår:

- Skoleeier kan overføre personopplysninger til land som EU-kommisjonen eller Datatilsynet mener har gode nok personverngarantier²⁰.
- Safe Harbor-avtalen mellom USA og EU gjør at norske skoleeiere kan overføre personopplysninger til amerikanske selskaper som behandler personopplysninger i henhold til prinsippene i avtalen²¹.
- Skoleeier kan overføre personopplysninger etter unntaksbestemmelsene i personopplysningsloven § 30. Overføring kan blant annet skje hvis den registrerte (ansatte, elever og foreldre/foresatte) samtykker²² til at dette skjer eller hvis overføring er nødvendig for å oppfylle en avtale med den registrerte²³.
- Datatilsynet kan tillate overføring dersom skoleeier gir tilstrekkelige garantier for at den registrertes personvernrettigheter blir ivaretatt av skytjenesteleverandøren (for eksempel ved at leverandøren har et bedriftsinternt personvernregelverk som gir garantier for at personopplysningene håndteres på en forsvarlig måte)²⁴.

²⁰ Hvilke land det her dreier seg om, kan man få informasjon om ved henvendelse til Datatilsynet.

²¹ For mer informasjon om denne avtalen, se http://www.datatilsynet.no/templates/article_2626.aspx.

²² Et samtykke er en frivillig, uttrykkelig og informert erklæring fra den registrerte (elever, ansatte eller foreldre/foresatte) om at vedkommende godtar at skoleeier overfører opplysninger om han/henne til land som ikke har like strenge regler for personvern som land innenfor EU/EØS-området (se personopplysningsloven § 2 nr. 7).

²³ For øvrige unntak, se § 30, 1. ledd.

Dersom skoleeier overfører personopplysninger til skytjenesteleverandører utenfor EU/EØS-området uten at ett av vilkårene ovenfor er oppfylt, vil dette være i strid med reglene i personopplysningsloven med forskrift.

Lovmessig overføring av personopplysninger til leverandører utenfor EU/EØS-området trenger som hovedregel ikke forhåndsgodkjenning av Datatilsynet.

INNGÅELSE AV DATABEHANDLERAVTALER

Den andre utfordringen – om det er mulig å inngå en databehandleravtale med leverandøren – har ikke fått særlig oppmerksomhet i debatten om skytjenester og personvern. Vi har imidlertid sett at lovverket krever at det skal foreligge en slik avtale og at databehandleravtalen skal inngås før skoleeier overfører personopplysninger til skytjenesteleverandøren. Men spesielt hvis leverandøren er et utenlandsk selskap etablert utenfor EU/EØS-området, er det ikke sikkert at leverandøren uten videre kjenner til eller har rutiner for å følge opp reglene i norsk og europeisk personvernlovgivning.

Det er derfor viktig at skoleeier leser avtaletilbudet som mottas fra skytjenesteleverandøren (for eksempel vilkår for bruk) og forvisser seg om at kravene som stilles til databehandleravtaler, er ivarettatt. Her kan det være hensiktsmessig at skoleeier setter seg inn i minimumskravene som Datatilsynet stiller til databehandleravtaler²⁴, og sjekker minimumskravene opp mot vilkårene i avtalen som tilbys av leverandøren. Dette gjelder uavhengig av om det dreier seg om gratis tjenester eller betalingstjenester. Det spiller altså ingen rolle om skoleeier betaler for skytjenestene eller ikke – det avgjørende er at tjenestene behandler personopplysninger.

Vær imidlertid oppmerksom på at avtalen som leverandøren tilbyr, kan være vanskelig å sette seg inn i og forstå. Da blir

det desto viktigere at skoleeier gjør en nøye sammenlikning av avtalen og kravene til databehandleravtaler for å sjekke at avtalen dekker de kravene som stilles.

Dersom avtalevilkårene som tilbys av leverandøren ikke oppfyller lovverkets krav til databehandleravtaler (eller hvis leverandøren ikke ønsker å endre avtalen slik at den blir i tråd med de kravene som stilles), vil skoleeiers aksept av avtalen være i strid med reglene i personopplysningsloven med forskrift.

OVERHOLDELSE AV AVTALEVILKÅRENE

Den tredje utfordringen – kontroll med at leverandøren overholder vilkårene i databehandleravtalen – er kanskje den vanskeligste for skoleeier å ivareta på en god måte. I Datatilsynets veileder for skytjenester, "Cloud Computing – en veileder i bruk av nettskytjenester"²⁵, understrekes det at skoleeier må ha god kunnskap om hvordan leverandøren ivaretar informasjonssikkerheten til personopplysningene. Datatilsynet stiller derfor følgende krav til skoleeiers kontroll med informasjonssikkerheten til leverandører av skytjenester:

- at skoleeier har tilgang til informasjon om hvordan leverandørens datasystemer er oppbygd (konfigurasjonskart) og hvilke sikkerhetsløsninger som leverandøren har implementert.
- at skoleeier informeres om og godkjenner eventuelle endringer av de sikkerhetsløsningene som leverandøren har implementert.
- at skoleeier sikrer seg adgang til å gjennomføre sikkerhetsrevisjoner hos skytjenesteleverandøren.

²⁴ Les mer om reglene for overføring av personopplysninger til land utenfor EU/EØS-området på http://www.datatilsynet.no/templates/article____2620.aspx. For en gjennomgang av den registrertes personvernrettigheter, se "ABC i personvern for skoler og skoleeiere", tilgjengelig på <http://iktsenteret.no/ressurser/abc-i-personvern-skoler-og-skoleeiere>.

²⁵ Se http://www.datatilsynet.no/templates/Page____2747.aspx.

²⁶ Se http://www.datatilsynet.no/templates/article____3829.aspx.

I tillegg krever Datatilsynet at skoleeier har god oversikt over og kontroll med følgende forhold hos skytjenesteleverandøren:

- at sikkerhetskopier av skoleeiers personopplysninger ikke befinner seg på datamaskiner i land som mangler tilstrekkelige personverngarantier.
- at leverandøren ikke lagrer skoleeiers personopplysninger slik at de blandes sammen med personopplysninger som tilhører andre behandlingsansvarlige²⁷.
- at skoleeier forsikrer seg om at leverandøren har klare rutiner for hvilke ansatte hos leverandøren som har tilgang til personopplysningene.
- at skoleeier forsikrer seg om at leverandøren registrerer uautorisert bruk (og forsøk på slik bruk) av leverandørens datasystemer.
- at skoleeier må kunne dokumentere at det foreligger skriftlige rutiner for bruken av personopplysninger som behandles av skytjenester²⁸.

Internasjonale studier av e-forvaltning i offentlig sektor indikerer at når drift av IT-tjenester settes ut til eksterne leverandører, oppstår det en fare for svekkelse av IT-kompetansen i den virksomheten som setter ut driften²⁹. Dermed kan det bli vanskelig å ta driften tilbake igjen fordi kompetansen og kapasiteten til å drifte tjenestene selv blir bygd ned.

Dette er en utfordring som skoleeier bør tenke igjennom før eksterne driftsløsninger tas i bruk. Skoleeier bør stille seg følgende spørsmål:

- Hvor viktig vil det være for oss å sikre oss muligheten til å ta tilbake driftsansvaret? Har vi kompetanse og kapasitet til å ta tilbake driften hvis det skulle vise seg ønskelig/nødvendig, eller blir vi låst fast i et ensidig avhengighetsforhold til leverandøren?
- Hvilken administrativ kompetanse trenger vi å ha (eller er det behov for å opparbeide) dersom driftsansvaret settes ut til en ekstern leverandør, spesielt når det gjelder lover og regler som direkte eller indirekte regulerer bruken av fjerdriftsløsninger?

Når det gjelder det siste punktet, er det ikke bare kompetanse om de relevante reglene i personopplysningslovgivningen som vil være viktig. Det finnes også andre lovmessige føringer som det kan være nødvendig å ha kompetanse på.

²⁷ Datatilsynet krever at personopplysninger tilhørende ulike behandlingsansvarlige skilles fra hverandre ved hjelp av to uavhengige sikkerhetsbarrierer (se Veileder i sikkerhetsarkitektur, s.29, tilgjengelig på http://www.datatilsynet.no/templates/article____3966.aspx).

²⁸ Se også personopplysningsforskriften § 2-16.

²⁹ Se for eksempel Patrick Dunleavy, Helen Margetts, Simon Bastow og Jane Tinkler (2006): *Digital Era Governance. IT Corporations, the State and E-government* (Oxford University Press, Oxford).

Del 5

Andre lovmessige føringer

Det er altså ikke bare personopplysningsloven med forskrift som inneholder bestemmelser som skoleeier bør være oppmerksom på dersom driften av IT-tjenester og behandling av personopplysninger settes ut til eksterne leverandører. For skoleeiere er det særlig to andre regelsett som det kan være viktig å kjenne til:

- *Opplæringsloven § 9-6*

Her er det et forbud mot reklame i grunnopplæringen. Forbudet er ikke absolutt; begrensede former for reklame kan godtas³⁰. Skoleeier bør derfor være oppmerksom på om avtaler om bruk av skytjenester (eller andre eksterne IT-tjenester) inneholder klausuler hvor skoleeier forplikter seg til å motta reklame fra leverandøren eller fra leverandørens samarbeidspartnere. Det er skoleeier som må vurdere om eventuelle forpliktelser til å motta reklame er såpass omfattende eller er av en slik art at det er i strid med opplæringsloven.

- *Godkjente arkivløsninger*

Hvis skoleeier benytter skytjenester (eller andre eksterne IT-tjenester) til langvarig lagring av arkivverdig materiale, skal tjenestene inneholde en arkivmodul som er godkjent av riksarkivaren. Dette fremgår av reglene i arkivloven med forskrifter³¹. Dersom leverandøren ikke kan tilby en slik arkivmodul, må skoleeier enten skrive ut arkivverdig dokumentasjon og lagre den i sitt papirbaserte arkiv, eller overføre dokumentasjonen til et godkjent elektronisk arkivsystem. Hvis skytjenestene i tillegg anvendes til utsendelse eller mottak av saksdokumenter, må skoleeier/skolen påse at det finnes løsninger for journalføring av dokumentene.

³⁰ Se Utdanningsdirektoratets veileder til § 9-6 på <http://www.udir.no/Regelverk/Tolkning-av-regelverket/Skoleeiers-ansvar/Reklame-i-skolen-paragraf9-6-veileder/>.

³¹ For en gjennomgang av kravene til arkivering av elektronisk materiale, se Ivar Fornes (2010): *Arkivhåndboken for offentlig forvaltning* (Kommuneforlaget, Oslo)

**SENTER
FOR IKT I
UTDANNINGEN**

www.ihtsenteret.no
post@ihtsenteret.no

