PERSONVERN I SKOLE OG BARNEHAGE

Samlerapport, juni 2014

Datatilsynet

Datatilsynet

Gateadresse: Tollbugata 3, Oslo

Postadresse: Pb 8177 Dep, 0034 Oslo

E-post: postkasse@datatilsynet.no

Telefon: 22 39 69 00

Faks: 22 42 23 50

www.datatilsynet.no

Innhold

1 Sammendrag

Datatilsynet har i 2013 og 2014 sett nærmere på opplæringssektoren. Gjennom møter med aktører i skolesektoren og kontroller ved en rekke barnehager, grunnskoler og videregående skoler, har vi kartlagt flyten av opplysninger om elevene i skolen. Vi har blant annet møtt Senter for IKT i utdanningen, Utdanningsforbundet, SSB, Kunnskapsdepartementet og Utdanningsdirektoratet, samt aktører som tilbyr læringsplattformer og skoleadministrative system. Vi har hatt tilsyn på elleve grunnskoler, fire videregående skoler og i fem barnehager – både private og kommunale.

Bakgrunnen for å se på opplæringssektoren er at barnehager og skoler, i likhet med resten av samfunnet, gjennomgår en digitalisering. Barnehager og skoler tar i økende grad i bruk digitale løsninger for praktiske og pedagogiske formål. Vi ser at det stilles større krav til dokumentasjon av elevens læring og utvikling enn hva som var praksis tidligere.

De fleste skoler bruker digitale læringsplattformer (LMS – Learning Management System). Det åpner for kontinuerlig logging av elevens aktivitet, for eksempel når på døgnet eleven leverer oppgaver, hvor lang tid eleven bruker på oppgaveløsning, logg av kommunikasjon med lærer og andre elever, samt hvilke fag eleven har jobbet aktivt med i leksearbeidet.

Mange skoler benytter seg også av andre digitale og nettbaserte læringsressurser[1], som i ulik grad registrerer elevenes aktiviteter. De skoleadministrative systemene registrerer blant annet fravær og karakterer, og noen skoler bruker digitale verktøy til å kartlegge og registrere uønsket atferd[2].

Barnehagene tar i bruk nettbaserte digitale løsninger både for kontakt mellom barnehage/hjem og for pedagogiske formål. Dette dreier seg om alt fra relativt åpne bildearkiv til spesialtilpassede løsninger med innlogging og lagring av taushetsbelagt informasjon om barna.

Samlet utgjør dette et sett med opplysninger som gir et omfattende og detaljert bilde av et barns utvikling og faglig og sosial atferd gjennom et helt utdannelsesløp. Det at flere opplysninger om barna lagres digitalt betyr også at spredningspotensialet blir større. Uten tekniske sperrer og gode rutiner kan uvedkommende få tilgang til opplysninger, og opplysninger om barna kan med få tastetrykk spres til mange.

På bakgrunn av møtene og kontrollene vi har gjennomført, viser vi i denne rapporten til noen hovedutfordringer knyttet til personvern i skole- og barnehagesektoren, og vi kommer med forslag til måter å møte disse utfordringene på.

[1] En oversikt over mange slike tjenester finnes hos Feide (https://www.feide.no/tilgjengelige-tjenester)
[2] Vi har sett på SWIS som er tilgjengelig fra Atferdssenteret (http://www.atferdssenteret.no/)

2 Personvernutfordringer i skoler og barnehager

Personvern handler blant annet om selvbestemmelse. For barn og unge i skole og barnehage, handler det om at foreldre og barn skal ha kontroll med hvordan opplysningene om barna blir brukt. Dette fordrer først og fremst åpenhet fra skolene og barnehagene sin side, med tanke på valg av kommunikasjonsløsninger og lagringsmedier.

Ved at det tas i bruk mange forskjellige kanaler for å kommunisere med foresatte og elever, blir opplysninger om elevene lagt igjen på mange ulike steder, og med ulik grad av sikkerhet. Vi har sett tilfeller hvor skoleeieren ikke har kjennskap til dette og dermed heller ikke har utarbeidet retningslinjer for, eller gitt opplæring i, bruken av dette. Når ingen har vurdert sikkerhetsaspektene ved at opplysninger blir lagret hos en tredjepart, og heller ikke er kjent med at tredjeparten er å anse som en databehandler[3] er sannsynligheten liten for at en databehandleravtale[4] er på plass. En slik avtale er nødvendig for å sikre opplysningene.

Informasjon til foresatte og elever om hvorfor og hvordan opplysningene om barnehagebarn og elever blir behandlet, er en grunnleggende personvernrettighet. Uten informasjon har foresatte og elever ingen mulighet til å si ifra hvis de mener at barnehagen eller skolen ivaretar personvernet på en dårlig måte. Uten informasjon har de heller ingen mulighet til å be om innsyn, retting eller sletting – rettigheter som personopplysningsloven gir.

Gjennom møter og kontroller har vi fått inntrykk av at det gjøres mye bra for å ivareta barnas personvern i barnehagen og i skolen. For eksempel ser vi at det er flere som er bevisste på at bilder av barn på Internett både kan være belastende for barnet selv og gjenstand for misbruk. Dette har gjort at særlig barnehager har laget klare retningslinjer for når bilder kan tas og hva bildene kan brukes til.

Lærere opplever at spill og sosiale medier er forstyrrende faktorer i undervisningen. Enkelte skoler prøver å imøtegå dette ved å overvåke elevenes bruk av PC og nettbrett. Vi har imidlertid også sett at flere skoler bevisst forsøker å unngå et slikt overvåkingsregime, og heller finner andre måter å gjøre undervisningen mer interessant på.

Vi har altså sett eksempler på god praksis, men vår kunnskapsinnhenting avslørte utfordringer for personvernet som virker å være gjeldende for en stor andel barnehager og skoler. Vi vil her beskrive det vi anser som hovedutfordringene.

[3] Databehandler er den som behandler personopplysninger på oppdrag fra den behandlingsansvarlige. Dette er vanligvis en virksomhet.
[4] Databehandleravtale er en avtale mellom en databehandler og den behandlingsansvarlige om hvordan personopplysninger skal behandles (http://www.datatilsynet.no/Sikkerhet-internkontroll/Databehandleravtale/).

Uklarhet omkring hva personopplysninger er

En erkjennelse, og en noe overraskende oppdagelse, har vært at betydningen av begrepet «personopplysning» er uklar for svært mange. Vi opplever at mange misforstår hva personopplysninger omfatter.

Flere forklarer personopplysninger som navn, fødselsnummer, adresse og andre opplysninger som direkte identifiserer oss. Personopplysninger er imidlertid mye mer enn dette. Personopplysninger er **alle** opplysninger som kan knyttes til enkeltpersoner. Dette betyr at ikke bare de opplysningene som tradisjonelt har vært lagret om barna i barnehagen og på skolen er å anse som personopplysninger. I dag er det mye mer som lagres; bilder, kommunikasjon mellom elever, kommunikasjon mellom lærer og elev, kommunikasjon mellom barnehage og hjem, informasjon om allergier, logg fra elevenes bruk av skolens nettverk, logg fra elevenes bruk av pedagogiske verktøy og lignende. Samlet utgjør dette et sett med opplysninger som gir et omfattende og detaljert bilde av et barns utvikling og barnets faglige og sosiale atferd gjennom et helt utdannelsesløp.

Flere læringsplattformer inneholder for eksempel kommunikasjonsverktøy slik som chat, kommentarfelt/diskusjonsforum, e-post og meldingstjenester der private samtaler i noen tilfeller lagres. Videokonferansefunksjon der det er mulig å ta opp både lyd og bilde, er også ofte integrert. Ofte er det dessuten mulig for lærerne å sende SMS fra læringsplattformene til andre lærere, elever og foreldre. Dette er også personopplysninger. Fra et personvernperspektiv er det viktig at skoleeieren[5] har en klar formening om hva personopplysninger er. Det er skoleeierens plikt å ha oversikt over personopplysningene. Skoleeieren skal vite hvorfor de enkelte opplysningene lagres, hvem som skal ha tilgang til dem, hvor lenge de skal lagres og så videre.

Mangelfull internkontroll

Etter 20 tilsyn i barnehager, grunnskoler og videregående skoler, kan vi konstatere at det er et gjennomgående problem at barnehagene og skolene ikke har tilfredsstillende rutiner for å oppfylle personopplysningslovens og personopplysningsforskriftens plikter. Dette gjelder særlig pliktene til:

- å ha oversikt over skolens/barnehagens behandlinger av personopplysninger
- å sørge for innhenting av samtykke når det er nødvendig
- å sørge for at foresatte og barn blir informert om hvordan skolen/barnehagen håndterer opplysningene
- å sørge for at innsyn blir håndtert på riktig måte
- å sørge for å ha slette- og/eller arkivrutiner
- å sørge for risikovurdering ved bruk av digitale verktøy som behandler personopplysninger, og

[5] Skoleeier for de offentlige skolene er kommunen (grunnskolen) og fylkeskommunen (videregående skole), representert ved rådmann/fylkesrådmann/byrådsleder. For privatskoler er det virksomhetens øverste leder.

- å sørge for utarbeidelse av databehandleravtaler.

Listen inneholder de elementene vi forventer er med i internkontrollen for skole- og barnehageeier.

Fylkeskommunen eller kommunen har gjerne overordnede rutiner for internkontroll, men disse er ofte lite kjent i barnehagen og på skolen, og må ofte tilpasses før de kan brukes også der. Det er for eksempel ikke uvanlig at fylkeskommunen/kommunen har en overordnet rutine for innsyn i personopplysninger som gjelder alle kommunens etater. Dette ville vært helt i orden dersom den var dekkende for alle typetilfeller av innsynsbegjæringer som blir rettet mot kommunen. Det som er spesielt for barnehager og skoler er at den som ber om innsyn som oftest ikke er «den registrerte» selv (barnet). Det er enten barnets foresatte eller noen andre som på foresattes fullmakt skal ha opplysningene (advokat, forsikringsselskap eller lignende). Da blir det særlig viktig å forsikre seg om at den som henvender seg har rett til et slikt innsyn.

Slike særskilte situasjoner tilsier at det bør utarbeides egne tilpassede rutiner for barnehagen og skolen. En rutine som er tilpasset disse situasjonene vil i større grad sikre at utleveringen av opplysninger er lovlig og gir samtidig de ansatte en større trygghet for at det de gjør er rett.

Internkontroll

Personopplysningsloven stiller krav til internkontroll i form av etablering og vedlikehold av planlagte og systematiske tiltak for å oppfylle kravene i, eller i medhold av, personopplysningsloven – herunder å sikre personopplysningenes kvalitet. Dette betyr at man må ha:

- rutiner for oppfyllelse av virksomhetens plikter og de registrertes rettigheter
- rutiner og tekniske tiltak for informasjonssikkerhet

Mangelfull informasjonssikkerhet

Av positive funn rundt informasjonssikkerhet kan vi først nevne at vi har inntrykk av at informasjonssikkerheten rundt **sensitive** personopplysninger om barna blir tatt på alvor. Et eksempel på dette er bruken av kartleggingsverktøyet SWIS (School Wide Information System), som også er omtalt lenger bak i rapporten. Opplysningene i dette systemet er avidentifisert. Det vil si at det ikke er registrert direkte identifiserbare opplysninger (navn eller fødselsnummer) knyttet til elevene. Hver elev som registreres i systemet gis en tallkode som skiller vedkommende fra de andre elevene. Skolene har så en kodeliste hvor denne tallkoden, som knyttes mot navn og fødselsnummer, er lagret separat og fysisk innelåst – gjerne på en minnepenn, i papirformat eller begge deler.

Generelt kan vi si at i den grad skolene har skrevne rutiner for behandling av personopplysninger, handler disse gjerne om informasjonssikkerhet. Vi har også et inntrykk av at tradisjonen med papirbasert dokumenthåndtering fortsatt er sterk, og at mange har en oppfatning av at informasjonssikkerhet hovedsakelig handler om å sørge for konfidensialitet.

Det betyr at de to andre viktige elementene i informasjonssikkerhetsbegrepet, tilgjengelighet og integritet, blir glemt.

Et eksempel på dette er at enkelte vi har snakket med har en oppfatning av at når de har lagret et dokument på en minnepenn og låst minnepennen inn i et skap, så er informasjonssikkerheten ivaretatt på en god måte. Opplysningene vil riktignok være vanskelig for en utenforstående å få tak i, men det vil samtidig være tungvint for de som trenger tilgang til opplysningene for å gjøre sin jobb. Når arbeidet blir tungvint er det ikke sikkert opplysningene regelmessig oppdateres, holdes korrekte eller slettes i tide.

Det er varierende bevissthet knyttet til arkivering og sikker lagring av personopplysninger i barnehager og skoler. Det er ikke uvanlig at opplysninger som skal ligge i mapper i et fysisk arkiv, for eksempel blir opprettet og lagret i en skybasert lagringstjeneste eller havner i en perm på lærerens/pedagogens kontorplass.

Denne type praksis springer ut av mangelfull internkontroll og av at rutiner for lagring av personopplysninger enten ikke finnes eller ikke er kjent blant de ansatte. En slik praksis innebærer at verken konfidensialitet eller tilgjengelighet blir ivaretatt.

På tilsyn har vi sett at informasjonssikkerheten gjerne er dokumentert med sikkerhetsmål og sikkerhetsstrategi, og at det er etablert en sikkerhetsorganisasjon. Derimot mangler det ofte dokumentasjon på hvilke sikkerhetstiltak som skal være rundt de spesifikke systemene som inneholder opplysninger om barna.

Mangel på risikovurderinger
Et særlig fremtredende funn som gjelder både skoler og barnehager, er mangel på risikovurdering av informasjonssystemene.

Personopplysningsloven 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 barnehage- og skoleeiere 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
- om opplysningene er sensitive eller ikke.

Barnehage- og skoleeier 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 barnehage- og skoleeier vurdere risikoen for at det kan skje systemtekniske eller menneskelige feil som påvirker sikkerheten rundt opplysningene, og om det er fare for at opplysningene eksponeres for ytre fysisk påvirkning (brann, vannlekkasje og lignende). Dette vil gi et risikobilde som gir skoleeieren 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.

Autentisering

Skolene vi kontrollerte hadde kun brukernavn og passord for innlogging til læringsplattformene. Det samme gjaldt for barnehagenes innlogging på sine kommunikasjonsplattformer. Dette er det vi kaller svak autentisering.

For foresatte og barns tilgang til læringsplattformer og kommunikasjonsplattformer, anser vi normalt innlogging ved brukernavn og passord som tilstrekkelig sikkert.

Når det gjelder tilgangen for de ansatte vurderer vi det derimot slik at det må kreves en sterkere autentisering – og særlig når tilgang er mulig fra eksterne nett eller elevnett. Kravet om strengere sikkerhet ved ansattes innlogging utenfor skolens/barnehagens nettverk er begrunnet med at en ansatt ved innlogging på en læringsplattform, skoleadministrativt system eller kommunikasjonsplattform får tilgang til personopplysninger om svært mange barn. Dersom uvedkommende klarer å skaffe seg et brukernavn og passord er det mulig, uten flere hindre, å logge seg på systemet fra hvor-som-helst og når-som-helst.

Brukernavn er ofte statisk og lett å gjette seg til. Passord er også mulig å finne ut av. Uten et tiltak i tillegg til brukernavn og passord, er opplysningene om barna ikke godt nok beskyttet. Sterk autentisering hindrer at noen som får tak i brukernavn og passord, klarer å skaffe seg tilgang til systemet.

Autentisering – å bekrefte noe eller noen som autentisk, altså ekte eller sann.

Innenfor informatikk betyr autentisering å verifisere den digitale identiteten til en avsender som forsøker å kommunisere.

Avsenderen kan være en person som bruker en datamaskin, kun en datamaskin eller et program.

Kommunikasjonen kan for eksempel være et forsøk på å logge inn på en datamaskin.

Eksempel på *svak autentisering* er bruk av brukernavn og passord.

Eksempel på *sterk autentisering* er bruk av ytterligere en faktor i tillegg til brukernavn og passord. Dette kan være engangspassord på SMS eller kodekort, eller biometriske parametere.

Det å åpne for hjemmekontorløsning innebærer en risiko i seg selv, fordi pålogging foregår utenfor barnehage- og skoleeiers direkte kontroll. Det må derfor lages gode hjemmekontorløsninger med sterk autentisering, hvor en også har kontroll med utstyret som brukes.

Sikkerhetsrevisjon

Kun én av de kontrollerte skoleeierne hadde gjennomført og dokumentert sikkerhetsrevisjon av sine informasjonssystemer, mens tre av skoleeierne hadde planlagt å gjennomføre revisjon i løpet av 2014. Ingen av barnehagene hadde gjennomført og dokumentert sikkerhetsrevisjon av sine informasjonssystemer.

Uoversiktlig informasjonsflyt og uklare ansvarsforhold

I møter med tilbydere av læringsplattformer har vi fått inntrykk av at det er usikkerhet rundt hvem som er behandlingsansvarlig[6] for personopplysninger i skolen. Kommuner og fylkeskommuner er skoleeiere og behandlingsansvarlige, men disse delegerer i visse tilfeller arbeidet til skolelederne (rektorene). Tilbyderne av læringsplattformer opplyste om at det er varierende kunnskap om personopplysningslovens krav til **hvem** som skal ha rollen som behandlingsansvarlig og **hva** denne rollen innebærer. De opplyste også om at mange skoleeiere ikke etterspør databehandleravtaler.

Vår erfaring fra kontrollene er imidlertid at skoleeiere er bevisste sitt behandlingsansvar etter loven. Det er ikke rolleforståelsen som er problemet, men heller evnen til å sørge for å få implementert kommunens og fylkeskommunens internkontroll ved den enkelte skole.

Skolene har tradisjonelt sett vært nokså autonome og frakoblet sentral kommuneadministrasjon. Det har for eksempel vært vanlig at skolene har hatt egne arkiver og ikke vært tilsluttet kommunens arkivsystem. Den autonome tradisjonen står sterkt og delvis i veien for en vellykket implementering av et internkontrollregime for personopplysninger i skolen.

Et eksempel på dette er bruken av kartleggingsverktøyet SWIS (se tekstboks) som driftes av Atferdssenteret. For å skaffe oss kunnskap om hvordan systemet blir brukt i praksis i skolen, gjennomførte vi to kontroller på skoler som bruker SWIS. Det viste seg at ikke alle kommuner og skoler er like bevisste på hvilke krav som stilles til prosessen **i forkant** av beslutningen om at SWIS skal tas i bruk. Ved en av skolene hadde skoleledelsen selv tatt denne beslutningen uten å involvere skoleeieren, som i dette tilfellet var kommunen som behandlingsansvarlig. Slik vi ser det, er dette et klart brudd på personopplysningsloven. Den fastslår at den behandlingsansvarlige skal ha oversikt over hvilke personopplysninger som innhentes og brukes.

SWIS (School Wide Information System)

SWIS er et databasert informasjonssystem som lagrer rapporter om negative hendelser i skolemiljøet. Opplysningene brukes for å utforme skoleomfattende og individuelle tiltak.

Les mer om SWIS her: http://www.swis.no/

[6] Behandlingsansvarlig er den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Dette er vanligvis en virksomhet.

Det er ikke unaturlig at initiativet til å ta i bruk SWIS kommer fra den enkelte skole. Men, **beslutningen** om å ta i bruk et informasjonssystem som behandler opplysninger om elevene i skolen, må tas på overordnet nivå i kommunen - av den behandlingsansvarlige eller av noen som klart er gitt fullmakt til å ta en slik beslutning.

Deling av personopplysninger med tredjepart

Antall pedagogiske verktøy som tilbys over Internett er økende. Lærere, elever og ansatte i barnehager bruker nettbaserte verktøy og lagringstjenester både i det pedagogiske arbeidet og til administrative formål.

Eksempler på nettbaserte verktøy som lagrer personopplysninger:

Blogspot Cyberbook

Dropbox Lokus

Gyldendal Undervisning Kikora

Vår erfaring fra kontrollene vi har vært på, er at personvernhensyn ikke er del av vurderingen når det skal besluttes om slike verktøy skal tas i bruk, og i tilfelle hvilke. Det er også her et problem at ansatte tar i bruk denne type tjenester uten at barnehage- og skoleeier har besluttet at det skal tas i bruk. Dersom ikke barnehage- og skoleeier som behandlingsansvarlig vet at slike verktøy er tatt i bruk oppstår det følgefeil. Risikovurderinger blir ikke gjort, og ingen vurderer naturlig nok sikkerheten hos leverandøren av verktøyet. Avtalen om bruk av slike verktøy blir heller ikke inngått på riktig måte.

Når må det lages en databehandleravtale?

Databehandleravtale må lages når leverandøren av den nettbaserte tjenesten har tilgang til opplysninger som kan knyttes til en person.

Bruk av nettbaserte pedagogiske verktøy innebærer i noen tilfeller integrering mellom skolens system og tilbyderens applikasjon – noe som igjen betyr at IP-adresser[7] tilflyter en tredjepart (tilbyderen av det pedagogiske verktøyet). I noen tilfeller vil også detaljerte opplysninger om elevenes prestasjoner være tilgjengelige for leverandøren av det nettbaserte verktøyet.

Dette er et faktum som svært få skoler og skoleeiere har reflektert over. Lav bevissthet gjør at overføringen av elevopplysninger ikke

Eksempel på god praksis:

Oslo kommune har gjennomført en undersøkelse i Oslo-skolene for å avdekke omfanget av bruk av nettbaserte tjenester. Undersøkelsen avdekket at omfanget er stort.

Som en følge av dette har Oslo kommune vedtatt en sentral rutine som gjelder for all bruk av eksterne IKT-tjenester. Deres retningslinjer kan lastes ned fra våre nettsider.

[7] IP-adresse (eng: Internet Protocol address) er et nummer som unikt identifiserer en enhet i et nettverk. En IP-adresse er definert som en personopplysning fordi den kan spores tilbake til en bestemt maskinvare og dermed til en enkeltperson. Identifisering av en person gjennom IP-adressen kan også gi mulighet for sammenstilling av personens atferd på nett på tvers av ulike nettsteder.

reguleres i en avtale med leverandøren – slik det er krav til etter personopplysningsloven. Det betyr også at foresatte og elever får lite eller ingen informasjon om hvor elevenes opplysninger havner, eller hva de brukes til.

Leverandørene setter standarden for personvernet

Det er stor variasjon i økonomi, kunnskap og tilgjengelige ressurser hos barnehage- og skoleeiere. Dette påvirker kapasiteten til å ivareta personvernet på systemnivå. Erfaringen viser at store kommuner har kunnskap og kapasitet nok til å sette krav til produkter de kjøper, samt til å gjøre tilpasninger av systemer og bruk, slik at produktet oppfyller kravene til personvern og informasjonssikkerhet. Det samme gjelder kommuner som går sammen om å tilby IKT-tjenester til sine innbyggere. Mindre aktører vil i mange tilfeller kjøpe IKT-produkter som hyllevare og bruke det etter beste evne, uten nødvendigvis å ha et bevisst forhold til personvern. En lokal systemadministrator i en mindre kommune kan typisk være en engasjert lærer/pedagog uten formell bakgrunn eller praksis innen IKT og sikkerhet.

Ofte er det opp til barnehagen eller skolen selv å endre innstillingene i systemet. For eksempel kan den som har administratortilgang bestemme **om** og **hva** foreldrene skal ha tilgang til i læringsplattformen til sitt barn. I andre tilfeller finnes det ingen eller begrensede muligheter for skolen eller barnehagen til selv å endre innstillinger tilpasset deres behov, jf. tekstboksen under. I praksis betyr dette at leverandører av IKT-systemer har stor innflytelse på premissene for hvordan barnehagene og skolene behandler personopplysninger.

Funn fra kontroll – leverandør setter premissene for tilgangsstyring

En av barnehagene vi kontrollerte hadde tatt i bruk et kommunikasjonssystem hvor det kun ble operert med tre roller for tilgang; administrator, ansatt og foresatt. Alle rollene hadde tilgang til å endre opplysninger om barnet, blant annet informasjon om hvem som kunne hente barnet i barnehagen. Det er selvsagt svært viktig at de som har anledning til å endre en slik opplysning gjør det riktig, ettersom feil i hentelisten kan få store konsekvenser. Problemet i dette tilfellet var at leverandøren hadde en egeninteresse av at så mange som mulig hadde tilgang til databasen, fordi de tjente penger på salg av bilder som ble lagt inn. Leverandøren oppfordret derfor til en liberal praksis med hensyn til hvem som kunne få egen pålogging, slik at de foresatte kunne opprette nye brukere, til for eksempel besteforeldre, med samme rettigheter som de foresatte selv.

Tilgangsstyringen i eksempelet over kunne ha vært løst enkelt med en gjesteinnlogging uten rettigheter til å endre opplysninger. Vi ser her et eksempel på at leverandøren ikke har tatt i betraktning hvilke hensyn som er viktige for **barnehagen** å ivareta. Det er derfor det er viktig at barnehagen selv stiller krav om dette.

Det er mye ulik praksis, men det er liten tvil om at det er anbefalingen fra leverandørene av de ulike digitale verktøyene, eller det som er standardinnstillingen, som blir førende for hva som faktisk blir tatt i bruk.

Kommunikasjon mellom skole/barnehage og hjem

Kommunikasjon mellom skole/barnehage og hjem har vært et tilbakevendende tema i dette prosjektet. Måten denne kommunikasjonen foregår på har endret seg markant de siste årene. Før var kommunikasjonen basert på møter og lapper i garderoben og i skolesekken. I dag er mulighetene mange for foresatte til å følge med på en digital plattform. Dette innebærer både fordeler og ulemper sett fra et personvernståsted. En av fordelene er at dette kan være en godt egnet kanal for å gi informasjon om hvorfor og hvordan opplysningene om eleven behandles. Vi har imidlertid sett mange eksempler på mangelfull informasjon til foresatte og elever.

Årsaken til mangelfull informasjon varierer. I noen tilfeller er grunnen rett og slett at skoleeieren ikke kjenner til at elevopplysninger blir lagret, eller at dette i det hele tatt er personopplysninger. I andre tilfeller er skoleeieren bekymret for at informasjon kan skape bekymring hos de foresatte, og velger derfor bevisst ikke å gi informasjon.

Vi har sett eksempler hvor skoleeiere har lagt opp til at kommunikasjon skal foregå i to kanaler; på skolens nettside (hvor det som er «kjekt å vite» kommuniseres), og gjennom læringsplattformen (hvor det som er «viktig å vite» kommuniseres). Praksis blant lærere og elever er en annen. I tillegg til disse to kanalene kan kommunikasjonen foregå også gjennom Mobilskole, e-post, SMS, Facebook, Twitter og den tradisjonelle lappen i sekken.

Ved at det blir brukt mange forskjellige kanaler for å kommunisere med foresatte og elever, blir opplysninger om elevene lagt igjen på mange ulike steder med ulik grad av sikkerhet. Siden skoleeieren ikke vet om dette, er det ikke laget retningslinjer for det. Ingen har gitt opplæring i bruken, og ingen har vurdert den utstrakte bruken og sikkerhetsaspektene ved at opplysninger blir lagt igjen hos en tredjepart. Ingen har heller vurdert hvilke sikkerhetstiltak som må innføres, og dermed har heller ingen vurdert at tredjeparten er en databehandler og at en databehandleravtale må på plass for å sikre opplysningene.

Informasjon til foresatte og elever om hvorfor og hvordan opplysningene om elevene blir behandlet, er en grunnleggende personvernrettighet. Uten informasjon har foresatte og elever ingen mulighet til å si i fra hvis de mener skolen ivaretar personvernet på en dårlig måte. Uten informasjon har de heller ingen mulighet til å be om innsyn, retting eller sletting – som er rettigheter personopplysningsloven gir den enkelte.

Noe av bakgrunnen for at vi gjennomførte kontrollene for å se på bruken av SWIS (se faktaboks s. 10), var blant annet klager fra foresatte om mangelfull informasjon om SWIS fra skoler som hadde tatt i bruk systemet. Vi så derfor spesielt på den informasjonen som blir gitt foresatte og elever om SWIS.

Inntrykket vi sitter igjen med er at det er Atferdsenteret, som selger systemet, som setter premissene for hvilken informasjon som gis. De har laget en brosjyre om SWIS som deles ut til foresatte. Ellers er det for det meste muntlig informasjon som blir gitt på foreldremøter. Vi mener at hver enkelt skole bør utarbeide sin egen informasjon om systemet, og beskrive

de særskilte forholdene ved egen skole som begrunner at de tar i bruk SWIS.

Bruk av kartleggingsverktøy i barnehagen

Datatilsynet får jevnlig spørsmål om bruk av kartleggingsverktøy, slik som TRAS, ALLE MED, MIO og ASQ i barnehagene. Spørsmålene kommer både fra foresatte og ansatte, og dreier seg i stor grad om hvorvidt det kreves samtykke for å ta i bruk et slikt verktøy, samt hvilken informasjon som skal gis.

TRAS (Tidlig Registrering Av Språkutvikling)

TRAS er observasjonsmateriell for registrering av språkutvikling hos barn mellom 2-5 år. Verktøyet brukes i hele 90 prosent av alle landets barnehager.

Et av hovedtemaene under kontrollene vi gjennomførte i barnehagene var derfor bruk av slike kartleggingsverktøy. Vi ønsket å undersøke om barnehageeiere baserer bruken av disse verktøyene på samtykke, og hvilken informasjon som blir gitt de foresatte om metodene de bruker.

Det er særlig to funn som utmerker seg fra kontrollene:

Samtykke eller ikke?

Det er ulik oppfatning blant barnehageeiere om hvorvidt det skal være opp til de foresatte å bestemme om barnas språklige, motoriske og sosiale atferd skal kartlegges ved hjelp av standardiserte kartleggingsverktøy.

De barnehageeierne som mener at kartlegging ikke kan være frivillig, begrunner dette med at kartleggingen er en nødvendig del av avtalen om barnehageplass, og at det ikke er mulig å tilby en forsvarlig tjeneste uten å gjøre slik kartlegging.

De barnehageeierne som mener at kartlegging av barnas utvikling skal skje etter samtykke fra de foresatte, innhenter skriftlig samtykke fra de foresatte til dette. Vi ser imidlertid at metodene de bruker i liten grad er beskrevet, og gir dermed de foresatte liten mulighet til å sette seg inn i hva kartleggingen faktisk innebærer.

Kartlegge alle? Eller bare de med behov?

Det er også ulik oppfatning blant barnehageeierne om hvorvidt kartlegging skal være obligatorisk for alle barn, eller om bruken skal baseres på at man ser et behov hos enkeltbarn.

Våre funn viser at de barnehageeierne som mener at kartleggingen ikke kan være frivillig, er de samme som mener at det er nødvendig å kartlegge alle barn.

Logging av elevenes bruk av IKT

Et av hovedtemaene under kontrollene på skoler var overvåking av elever. Vi ønsket å se på skoleeierens håndtering av opplysninger som elever legger igjen når de bruker skoleeierens IKT-utstyr og -ressurser.

Det som er positivt er at det er lite overvåking av elevene ved skolene, bortsett fra under eksamen og ved gjennomføring av prøver for å forhindre fusk. Men ved én av de videregående skolene ble det benyttet et klassestyringsverktøy, samt en omfattende registrering av trafikken på nettverket ved bruk av et nettfilter.

Funn fra kontroll – overvåking ved bruk av klassestyringsverktøy og nettfilter

Ved en videregående skole hadde de et **klassestyringsverktøy** som kunne brukes i timene og som ble styrt av læreren. Verktøyet kunne bare brukes når PC-en var koblet til skolens nettverk. Læreren kunne aktivere/deaktivere verktøyet og fikk da opp en oversikt over elevenes skjermer. Slik kunne læreren se om elevene benyttet PC-en til annet enn det de skulle den aktuelle timen. Elevene fikk opp et lite ikon som ga dem beskjed om at verktøyet var aktivert. Den eneste muligheten en elev selv hadde til å unngå overvåkingen, var å koble fra det trådløse nettet eller låse/logge av maskinen.

Nettfilteret ble hovedsakelig brukt for å kunne se og finne sikkerhetstrusler i nettverket, slik som virusinfiserte datamaskiner og tilgang til nettsteder. I rapportene som så ble generert, ble elevenes bruk av nettet avidentifisert. En vanlig administrator vil se et nummer i stedet for elevens navn, hvilke nettsteder hver elev er inne på, og så få en grafisk fremstilling av hvilke kategorier av nettsider en elev har vært inne på i løpet av dagen. Hver kategori blir fremvist som et ikon med en fargekode. Fargene viser ulike nivåer av risiko fra svært lav risiko til svært høy risiko.

Vi mener at skolens i eksempelet over går ut over sitt formål i sin bruk av klassestyringsverktøy. Slik det er i bruk i dag, er det flere hendelser som burde vært vurdert til å gi høy risiko for urettmessig overvåking, slik som for eksempel:

- Dersom en elev har gyldig fravær fra en time for å drive med elevrådsarbeid, kan læreren likevel overvåke denne elevens PC fra klasserommet.
- Det er mulig for en lærer å aktivere overvåking når elevene har friminutt.

Formålet med å bruke et nettfilter skal være å administrere systemet og ivareta sikkerheten. Vi mener dette verktøyet ikke skal brukes til å overvåke og kontrollere hver enkelt elev. Vi stilte spørsmål til skoleeieren om hvorfor det er nødvendig å overvåke de «snille» elevene som kun er på nettsider kategorisert til lav risiko. Skoleeieren svarte at siden elevene er avidentifisert i rapportene, blir de ikke overvåket før de har gjort noe galt som gjør at de må identifiseres. Skoleeieren ga oss et eksempel på at dersom ledelsen fikk vite at noen hadde trakassert en medelev på en nettside, kunne de finne ut hvem som hadde vært inne på denne nettsiden på det gitte tidspunktet.

Vi mener derimot at ved å bruke verktøyet slik **blir** hver enkelt elev overvåket, utover det som er regulert av personopplysningsforskriften § 7-11. Denne bestemmelsen dreier seg om aktivitetslogg i edb-system eller datanett, der formålet er å administrere systemet eller å avdekke/oppklare brudd på sikkerheten i datasystemet. I det konkrete eksempelet som skoleeieren ga oss, er det også en risiko for identifisering av feil person dersom flere elever har vært inne på samme nettside i samme tidsrom.

3 Råd for et bedre personvern i skoler og barnehager

Datatilsynet har et mål om at personvernet for barn og unge i barnehager og skoler skal forbedres. Vi kommer i dette kapittelet med en del råd som hjelp på veien. Vi har også lagt ved en lenkesamling over eksempler til etterfølgelse og tips til hvor det finnes veiledningsmateriell.

Lag rutiner for internkontroll for hver enkelt skole og barnehage

Skole- og barnehageeiere må ta ansvar for internkontroll og informasjonssikkerhet. De må få orden på rutiner og dokumentasjon, kommunisere det ut til skolen/barnehagen, samt sørge for tilstrekkelig opplæring av de ansatte. De må sørge for at hver enkelt lærer, førskolelærer, pedagog og assistent vet hva som er greit og ikke.

Foresatte og barn har krav på å vite hvilke personopplysninger som blir behandlet, hvordan opplysningene er beskyttet og hvilke rettigheter de har til informasjon, innsyn, retting, sletting. Skole- og barnehageeierne må sørge for at internkontrollen inkluderer skolens/barnehagens behandlinger. De må også ta ansvar for å heve kompetansen om personvern i den enkelte skole/barnehage. Praktisk kan internkontrollen opprettes etter de samme fremgangsmåtene som benyttes i HMS-arbeidet.

Eksempel på god praksis:

Ved Ajer ungdomsskole i Hamar kommune har de gjort et godt grunnarbeid for å skaffe seg oversikt over de ulike behandlingene. På våre nettsider kan et eksempel på en slik oversikt – basert på Ajer ungdomsskole sin modell – lastes ned (se også lenkesamling bakerst).

Vi har utarbeidet en veileder for internkontroll og informasjonssikkerhet som kan lastes ned fra våre nettsider (se også lenkesamling bakerst).

Gjennomfør regelmessige risikovurderinger

Barnehage- og skoleeiere må ha oversikt over hva slags personopplysninger som behandles, og de må selv fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger. Det er skoleeier som er ansvarlig for at risikovurderinger blir gjennomført og at de blir gjentatt ved endringer som har betydning for informasjonssikkerheten. Vi mener at risikovurderinger skal gjøres ved innføring av nye systemer, ved endringer av eksisterende systemer og at de gjentas årlig.

Risikovurderinger kan gjøres som et gruppearbeid. På denne måten sikrer man at flest mulig scenarioer blir drøftet. For en skole kan en slik gruppe bestå av rektor, IKT-ansvarlig (fylkeskommunen/kommunen), sikkerhetsansvarlig (fylkeskommunen/kommunen), system-/fagansvarlig og lærere/pedagoger. Ved videregående skoler kan også elever delta i et slikt

arbeid, siden de kan være litt mer kreative og kanskje kan tenke ut andre mulige uønskede hendelser enn de ansatte.

I en barnehage kan gruppen bestå av daglig leder/styrer, IKT-ansvarlig, representant for de ansatte og representant for de foresatte.

Vi mener også at det er en fordel å være konkrete når det gjelder hendelsene, men ikke så spesifikke at det vil være usannsynlig at de vil inntreffe. Vi oppfordrer dessuten til å beskrive **årsaker** i tillegg til hendelser. Det er viktig å vurdere både konsekvens og sannsynlighet. En hendelse kan være vurdert til lite sannsynlig, men ha stor konsekvens dersom den inntreffer.

I lenkesamlingen bakerst viser vi til veiledere for risikovurderinger som kan lastes ned fra våre og andres nettsider.

Forhandle frem gode databehandleravtaler

Skole- og barnehageeierne **må** vite hvem som behandler opplysninger på deres vegne og etablere databehandleravtaler. De **skal** være kjent med sikkerhetsarbeidet hos leverandørene gjennom kunnskap om sikkerhetsstrategien til slike virksomheter. Videre skal de forsikre seg om at informasjonssikkerheten hos leverandøren er tilfredsstillende. Dette kan oppnås ved at skole- og barnehageeier innhenter resultater fra ledelsesgjennomganger, sikkerhetsrevisjoner og avviksbehandlinger hos leverandøren.

Gjennom våre skolekontroller har vi sett at skoleeiere som har tatt i bruk FEIDE (Felles Elektronisk Identitet), er av den oppfatningen at ved å være «FEIDE-klar», så trenger de ikke å vurdere leverandørene som blir tilgjengelige gjennom FEIDE eller inngå databehandleravtaler med disse. Det stemmer ikke. Skoleeieren må vurdere hvilke personopplysninger som blir overført til leverandørene, om det er nødvendig at opplysningene blir overført, eller om det hadde vært mulig å anonymisere opplysningene i stedet.

På våre nettsider har vi en veileder med tilhørende maler. Veilederen skisserer hovedmomentene i databehandleravtaler (se også lenkesamlingen bakerst).

FEIDE (Felles Elektronisk IDEntitet)

«*Feide er et rammeverk for håndtering av personvernet til elever og lærere i skolen. Som Felles Elektronisk Identitet (Feide)-bruker registrerer du deg bare én gang; på ditt universitet, høgskole, kommune, fylkeskommune eller private skole. Basert på kommunens opplysninger om elever og ansatte i skolen lages en elektronisk identitet - en Feide-identitet. Denne identiteten kan elever og ansatte bruke til å legitimere seg overfor ulike digitale tjenester, nettsteder, portaler, bibliotek og andre tjenester som er beregnet for utdanningssektoren.*»

https://iktsenteret.no/prosjekter/feide-i-skolen

Bruk sterk autentisering ved behov

De skolene og barnehagene vi har vært på kontroll hos, og som bruker informasjonssystem som inneholder opplysninger om mange barn, har vi pålagt at må etablere sterk autentisering for de ansatte ved innlogging dersom løsningen er tilgjengelig fra eksterne nett.

Med sterk autentisering mener vi for eksempel bruk av kodebrikke eller sikkerhetskode tilsendt på SMS. Dette kan også realiseres i en fjernarbeidsløsning med sterk autentisering, og påfølgende tilgang til for eksempel læringsplattform, skoleadministrative system eller annet pedagogisk verktøy på nett. Dette hindrer at noen som får tak i brukernavn og passord klarer å skaffe seg tilgang til systemet.

Begrens overvåking og gi god informasjon

Skoleeieren har plikt til å etablere sikkerhetstiltak for å hindre uautorisert bruk av informasjonssystemet og for å gjøre det mulig å oppdage forsøk på slik bruk. Derfor må for eksempel nettrafikk logges i brannmur og nettfilter, men det er viktig at loggene brukes kun for å administrere systemet og for å avdekke/oppklare brudd på sikkerheten i systemet. Verktøyene skal ikke brukes til andre formål som å overvåke og kontrollere elevene på en skole. Dette betyr for eksempel at logger i utgangspunktet ikke kan brukes for å håndtere mobbing.

Gi informasjon om logging

Vi ser imidlertid at det er hensiktsmessig å overvåke og begrense nettilgang for elever ved eksamensgjennomføring. I de tilfellene er det da viktig å gi god informasjon i forkant av eksamen om hva som gjøres fra skolens side, hva elevene må gjøre og hvor lenge loggene lagres.

Skolen må informere om hva de logger i nettverket, nettfilter og brannmur. Det må også informeres om hva formålet med loggingen er, hva loggingen brukes til, om det er identifiserende eller avidentifiserte opplysninger, hvem som har tilgang til loggene, hvor lenge loggene lagres, samt begrunne lengden på lagringstid. Det vil også være positivt om skolen forteller hva de **ikke** bruker loggene til.

Informasjon om logging kan stå i en personvernerklæring på skolens nettsider, i IKT-avtaler og i IKT-reglement.

Riktig bruk av klassestyringsverktøy

Vi mener at et klassestyringsverktøy ikke er galt å bruke, så lenge det ikke misbrukes, og så lenge elevene selv har tillit til at de ikke blir unødvendig overvåket. Bruken av klassestyringsverktøyet kan for eksempel foregå slik:

- Når timen begynner skal læreren opplyse elevene om at verktøyet vil bli benyttet i undervisningen.
- Læreren aktiverer gjeldende klasse.

- Elevene aktiverer pålogging fra sin PC. Dersom en elev er til stede i klasserommet, men ikke pålogget klassestyringsverktøyet, kan lærer muntlig henvende seg til eleven og anmode eleven om å logge seg på. På denne måten unngår man å overvåke elever som ikke er til stede.
- Ved timeslutt avsluttes overvåkingen ved at læreren kobler fra. Det kan også være tidsinnstilling slik at det er satt til automatisk frakobling når det er friminutt og slutt for dagen/timen.

Riktig bruk av nettfilter

Vi mener at fylkeskommunen og skolen kun skal bruke nettfilteret for å administrere systemet og ivareta sikkerheten i systemet. Rapportene som genereres bør kun inneholde kategorier som er til trussel for sikkerheten, slik som å stoppe skadelig kode eller trafikk som tar stor båndbredde. Videre må det være retningslinjer for en superadministrator som tilsier at utlevering av identiteter ikke skal kunne gis ut til enhver lærer eller rektor som spør om det.

Still krav til leverandører

Det må bygges en bedre bestillerkompetanse hos skole- og barnehageeiere når det gjelder innkjøp av digitale verktøy. På våre kontroller har vi sett at skoler og barnehager i altfor stor grad kjøper hyllevare eller ikke får nettbaserte tjenester tilpasset sitt behov.

I en barnehage vi var hos hadde de gjort jobben med å ta stilling til hva de hadde behov for og hvilken grad av sikkerhet de kunne akseptere. Resultatet ble mye bedre enn ved de barnehagene som ikke hadde gjort denne jobben.

Et eksempel på det motsatte er bruken av fødselsnummer for pålogging på læringsplattform når dette ikke er nødvendig. Når skoleeieren selv sier at dette ikke er nødvendig, må de stille krav til leverandør om å endre dette.

Er det nødvendig med fødselsnummer i læringsplattformen?

Skoleeieren ved en av de kontrollerte skolene hadde behov for å vite hvem som logget seg på læringsplattformen og knyttet dette til fødselsnummer. Vi fikk også vite at fødselsnummeret ble overført til leverandøren av læringsplattform og har stilt spørsmålstegn ved denne praksisen.

Bruken av fødselsnummer skal være nødvendig. Når skoleeieren har en annen bruker-ID ved å bruke FEIDE, mener vi at leverandøren av læringsplattformen ikke har behov for å vite fødselsnummer. Det er tilstrekkelig unikt at det finnes en entydig bruker-ID kombinert med navn og skole.

Vi ser det som svært uheldig at en leverandør lager en løsning som forutsetter fødselsnummer som identifikator når skoleeier vurderer det til ikke å være nødvendig.

4 Konklusjon og utfordringer i årene som kommer

Mange av problemstillingene vi har sett på knytter seg til bruken av elektroniske systemer for å løse administrative oppgaver og som støtte i læringsarbeidet. Teknologien gjør det mulig å produsere, lagre, sende og dele informasjon i en helt annen skala enn tidligere. Dette setter større krav til et bevisst og ryddig forhold til behandling av personopplysninger.

Bruken av elektroniske og nettbaserte tjenester i skoler og barnehager vil bare øke ytterligere i årene som kommer. Noen av disse tjenestene vil i økende grad tilby læringsanalyse som kartlegger og sammenstiller informasjon om barnas aktivitet på detaljnivå. Et eksempel er det norskutviklede matteprogrammet Kikora. Dette programmet logger elevens tastetrykk ned til hvert ledd i regnestykket og tilbyr læreren et «dashboard» med detaljert oversikt over **hva** hver enkelt elev har gjort, **når** og **hvordan** det gikk. Dette verktøyet er tatt i bruk ved et flertall av de grunnskolene vi har vært på kontroll hos.

Tilgjengelighet er et stikkord i dagens og morgendagens skole. Mange ser nytten av å ta i bruk mobil, nettbrett og lignende i skolehverdagen. Flere av aktørene vi har vært i kontakt med påpeker imidlertid at nettbaserte løsninger er sårbare, og at det er behov for veiledning knyttet til hva som er akseptable sikkerhetsløsninger.

Disse utfordringene, og behovet for veiledning, er felles for alle skole- og barnehageeiere. Vi mener derfor det er viktig at det tas et samlet og koordinert tak i hele sektoren. Dette kan oppnås ved at sentrale aktører i skole- og barnehagesektoren blir enige om en ensartet praksis som i alle fall oppfyller minimumskravene etter lovverket.

Oppsummering av de største utfordringene

Uklarhet omkring hva personopplysninger er. Mange misforstår hva personopplysninger omfatter, og vet ikke at det er alle opplysninger som kan knyttes til enkeltpersoner, som for eksempel: bilder, kommunikasjon mellom elever/lærere/barnehage/hjem, informasjon om allergi, logg fra elevers bruk av skolens nettverk, verktøy og liknende.

Mangelfull internkontroll. Skoler og barnehager mangler rutiner:

- for å gi innsyn,
- for å innhente samtykke,
- for retting og sletting, og
- for å gi ut informasjon om deres behandlinger av personopplysninger

Mangelfull informasjonssikkerhet. Det er ofte tatt hensyn til konfidensialitet rundt personopplysningene, men man mangler integritetsaspektet og tilgjengelighetsaspektet. Det er få som har gjennomført risikovurderinger og sikkerhetsrevisjoner.

Uoversiktlig informasjonsflyt og uklare ansvarsforhold. Det er ofte uklart hvem som er ansvarlig for behandling av personopplysninger i skole og barnehage, og hvilket ansvar som følger med.

Deling av personopplysninger med tredjepart. Det hender at skolens ansatte tar i bruk digitale verktøy uten at det er klarert med skoleeier, og det er liten bevissthet rundt mengden personopplysninger som deles med tredjeparter.

Leverandørene setter standarden for personvernet. Det er mange skole- og barnehageeiere som mangler kunnskap og kapasitet til å sette krav til produkter de kjøper, og de mangler kompetanse til å gjøre tilpasninger til systemet og bruken. Det mangler ofte databehandleravtaler.

Kommunikasjon mellom skole/barnehage og hjem. Det er mangelfull informasjon til foresatte og elever om hvordan opplysningene om barn og unge blir behandlet. Det blir ofte brukt mange flere kommunikasjonskanaler enn det skoleeieren har lagt opp til. Informasjon om bruk av ulike digitale system blir ikke tilpasset etter skolens/barnehagens bruk.

Bruk av kartleggingsverktøy i barnehagen. Det er ulik oppfatning blant barnehageeierne om hvorvidt det skal være opp til de foresatte å bestemme om barnas atferd skal kartlegges ved hjelp av standardiserte kartleggingsverktøy – og om **alle** barna skal kartlegges, eller bare de med behov.

Logging av elevers bruk av IKT. Det er generelt lite overvåking av elevene, men det forekommer overvåking ved noen skoler. Det er lagt opp til liten grad av selvbestemmelse i denne overvåkingen, og det blir gitt for lite informasjon om hvordan det foregår, om når logger slettes, hva de brukes til og liknende.

5 Lenkesamling

Internkontroll og informasjonssikkerhet
Datatilsynets veileder om internkontroll og informasjonssikkerhet:
http://www.datatilsynet.no/Sikkerhet-internkontroll/internkontroll_informasjonssikkerhet/

Risikovurdering
Datatilsynets veileder for risikovurdering informasjonssystem: http://www.datatilsynet.no/Sikkerhet-internkontroll/Risikovurdering/

Senter for IKT i utdanningen har laget en veileder for risikovurdering spesifikt for personopplysninger i skolen med flere tilhørende faktafoldere:

- Sikker håndtering av personopplysninger i skolen (hovedveileder): http://iktsenteret.no/sites/iktsenteret.no/files/attachments/veiledning_personopplysninger_web.pdf
- Sikker håndtering av personopplysninger i det skoleadministrative system (faktafolder): http://iktsenteret.no/sites/iktsenteret.no/files/attachments/faktafolder_skoleadm.pdf
- Sikker håndtering av personopplysninger i den digitale læringsplattformen (faktafolder): http://iktsenteret.no/sites/iktsenteret.no/files/attachments/faktafolder_digplattform.pdf
- Sikker håndtering av personopplysninger ved bruk av skolens lagringsområder (faktafolder): http://iktsenteret.no/sites/iktsenteret.no/files/attachments/faktafolder_lagring.pdf
- Informasjonssikkerhet i barnehagen (faktafolder): http://iktsenteret.no/sites/iktsenteret.no/files/attachments/informasjonssikkerhet_i_barnehagen_bm_0.pdf

Databehandleravtaler
Datatilsynets veiledning om databehandleravtale med tilhørende maler:
http://www.datatilsynet.no/Sikkerhet-internkontroll/Databehandleravtale/

Senter for IKT i utdanningen sin mal for databehandleravtaler ved bruk av tjenester i skolen:
https://feide.iktsenteret.no/node/234

Annet relevant
I beste mening – en veiledning om bilder av barn på nett:
http://www.datatilsynet.no/Sektor/Skole-barn-unge/Bilder-av-barn-pa-nett/

Tips til hva et samtykkeskjema for publisering av bilder av barn på nett bør inneholde:
http://www.datatilsynet.no/Sektor/Skole-barn-unge/Innhold-i-et-samtykkeskjema/

Eksempler på retningslinjer og sjekkliste for skolenes bruk av eksterne IKT-tjenester laget av Utdanningsetaten i Oslo kommune, eksempler på risikovurderinger med uønskede hendelser og tiltak, samt et eksempel på hvordan en oversikt over behandlinger i skolen kan se ut, ligger på våre nettsider: http://www.datatilsynet.no/Nyheter/2014/Personvern-i-skole-og-barnehage---samlerapport/

Sjekkliste for skole- og barnehageeiere

- ☐ Vi har utarbeidet en oversikt over alle behandlinger som inneholder personopplysninger om barn i skole/barnehage. Det inkluderer alle digitale system med følgende informasjon:
    - Systemnavn, Formål, Behandlingsgrunnlag, Melding/konsesjon, Klassifikasjon, Sikringstiltak, Lagring og kommunikasjon, Opplysningenes omfang, Avdeling, System-/dataeier

- ☐ Vi har utarbeidet skriftlige rutiner for internkontroll som inkluderer:
    - Samtykke (når trenger vi å innhente samtykke)
    - Innsyn (når skal vi gi innsyn og til hvem)
    - Retting (hvor ofte og når skal vi kontrollere at personopplysningene er korrekt)
    - Sletting (hvor ofte og når skal vi slette personopplysninger)
    - Informasjon (hvor ofte/når/til hvem/om hva/hvordan, skal vi gi ut informasjon)

- ☐ Vi har etablert rutine for, og gjennomført risikovurdering. Vi har vurdert konsekvens og sannsynlighet for hendelsesbrudd på konfidensialitet, integritet og tilgjengelighet, for:
    - hele informasjonssystemet (PC, nettverk, servere)
        - årlig og ved endringer
    - hvert enkelt system som inneholder personopplysninger (for eksempel læringsplattform, kommunikasjonsplattform, skoleadministrativt system, digitale nettressurser)
        - ved innføring av nye system, årlig og ved endringer

- ☐ Vi har innført sikkerhetstiltak som kom frem under risikovurderingen. Sikkerhetstiltakene er:
    - tekniske tiltak (for eksempel sterk autentisering av læringsplattform)
    - organisatoriske tiltak (rutiner, opplæring osv.)
    - fysiske tiltak

- ☐ Vi begrenser overvåking av våre elever og lærere, og gir ut informasjon om hva vi logger og når vi sletter loggene.

- ☐ Vi har rutine for sikkerhetsrevisjon og skal gjennomføre sikkerhetsrevisjon årlig for hvert enkelt system som inneholder personopplysninger.

- ☐ Vi har inngått databehandleravtale med alle leverandører av system som inneholder personopplysninger. Vi har også vurdert avtalene nøye og vet at avtalene som minimum inneholder informasjon om:
    - formål og type personopplysninger som blir lagret/overført
    - rett til tilgang til sikkerhetsdokumentasjon og sikkerhetsrevisjoner
    - hvem som har tilgang hos databehandler
    - tilfredsstillende sikkerhetstiltak etter personopplysningsloven med forskrift
    - avvikshåndtering
    - eventuelle underleverandører
    - lagringssted for personopplysningene
    - at personopplysningene er forsvarlig adskilt fra andre kunders personopplysninger
    - sletting av data (ved avtalens utløp, når brukere slutter eller er inaktive)

- ☐ Vi har gjennomført opplæring av alle ansatte i skolen/barnehagen i:
    - rutiner for internkontroll
    - informasjonssikkerhet