Elevdokumentasjon og tilgangsstyring i VGS

Kontrollutvalget i Innlandet fylkeskommune

10.03.2022

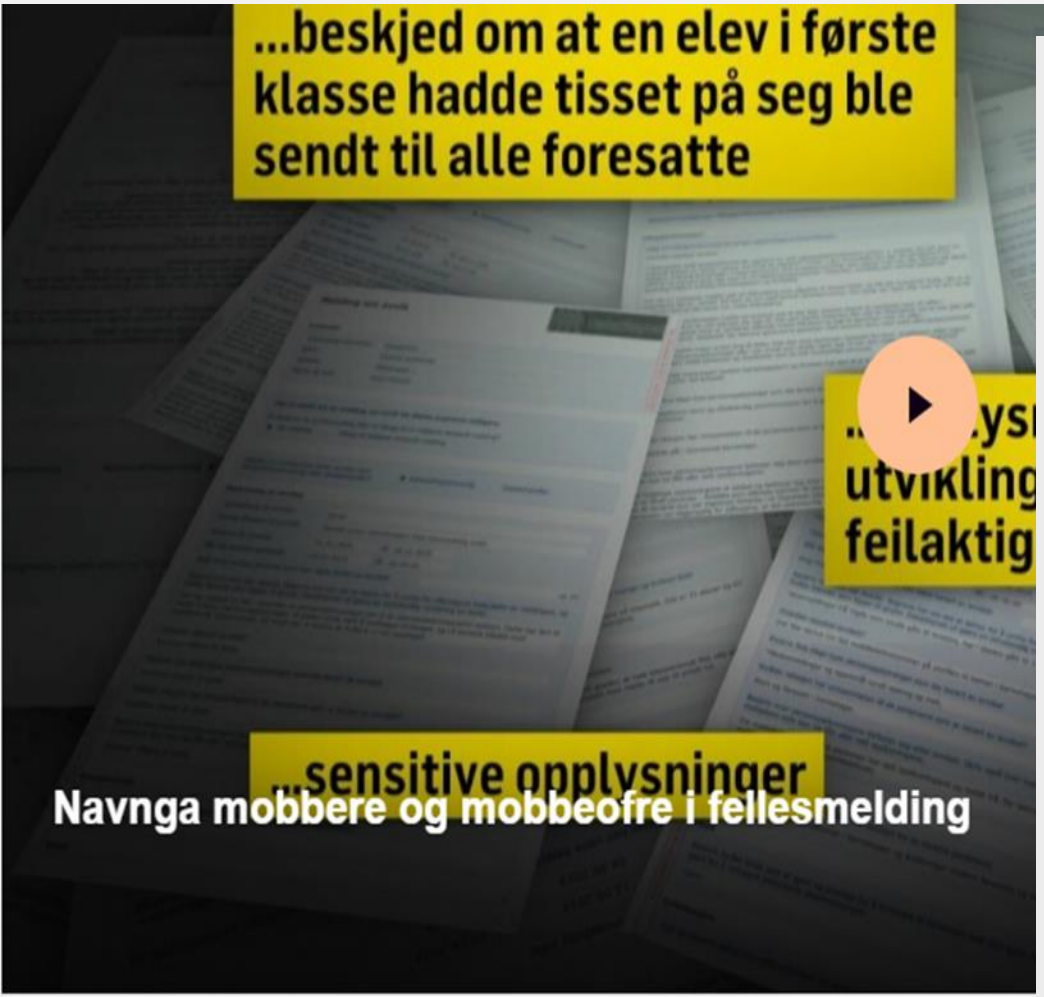
Anette Karenstuen

INNLANDET REVISJON IKS

Kontrollutvalgets bestilling

Forvaltningsrevisjon om:

- *Elevdokumentasjon og tilgangskontroller hvor formålet skal være å sette fokus på tilgangskontroller i sentrale IKT-systemer i de videregående skolene.*



Norske kommuner har s personvernet til flere tu

– Dette er bare toppen av isfjellet, sier direktør i Datatilsynet.

Flere av sakene handler nemlig om at foreldre uten foreldreansvar har fått tilgang til informasjon om barnet sitt. Foreldre som er voldsdømte og ikke skal vite hvor barnet bor, eller aldri har hatt noe med barnet å gjøre.

Direktør i Datatilsynet, Bjørn Erik Thon, er bekymret:

– Digitaliseringen av skolen går altfor fort. Lærerne, skoleledelsen og kommunene sitter ikke på kompetansen til å gjøre dette på en trygg og sikker måte, sier han.

BEKYMRET: Direktør i Datatilsynet Bjørn Erik Thon, sier det er vanskelig å vite hvor mange som er rammet, men at dette kun er toppen av isfjellet. Foto: Mariam Butt/NTB

Gjennomføring

- Eksternt fagmiljø for å kvalitetssikre problemstillinger, revisjonskriterier, metode og vurderinger.
- Gjennomføring 2021.
- Rapport desember 2021.
- God dialog med sentraladministrasjonen og videregående skoler.
- 800 timer.

Elevdokumentasjon

Fylkeskommunen og de videregående skolene oppbevarer og behandler store mengder personopplysninger på vegne av elever:

- Opplysninger om hvilke elever som har gått på hvilken skole, fravær, undervisningsvurderinger, sluttvurderinger, karakterer og elevbesvarelser.
- Særlige kategorier personopplysninger som enkeltvedtak, opplysninger om sykdom og helseforhold, vurderinger, referater fra samarbeid med BUP, PPT og helsevesen.
- Bilder, kommunikasjon, logg fra elevens bruk av skolens nettverk etc.

Samlet utgjør dette et sett med opplysninger som gir et omfattende og detaljert bilde av elevens utvikling og dens faglige og sosiale atferd gjennom et helt utdannelsesløp.

Tilgangsstyring

- Tilgangsstyring er et sikkerhetstiltak som skal bidra til å oppfylle målene om *konfidensialitet*, *integritet* og *tilgjengelighet* for virksomhetens informasjon.
- Tilgangsstyring innebærer å bare tildele godkjent personell, brukere eller maskiner tilgang til et system, et domene eller et konkret sett med opplysninger.
- Dersom personer har tilgang til systemer, tjenester og dokumentasjon de ikke har tjenstlig behov for kan dette føre til brudd på målene for IKT-sikkerhet om integritet og konfidensialitet
- Viktig for å redusere skadene ved en eventuell uautorisert tilgang.

Organisering og ansvar

- Fylkeskommunen eier og drifter 23 videregående skoler.
- Seksjonssjef for Koordinering og lederstøtte i avdeling for Kompetanse og tannhelse har personalansvar for rektorene ved de videregående skolene.
- Store forskjeller på skolestørrelser i fylkeskommunen, fra Storsteigen VGS med 120 elever til Hamar Katedralskole med 1156 elever.

Organisering og ansvar forts.

- Fylkeskommunedirektøren det overordnede ansvaret for personvern og informasjonssikkerhet i organisasjonen.
- Når det gjelder ansvar for IKT-systemer fordeles ansvaret mellom tjenesteeier og tjenesteansvarlig i sentraladministrasjonen i fylkeskommunen.
- Lokale skoleadministratorer er organisatorisk plassert på skolene.

Problemstillinger

Problemstilling 1:

Hvilke IKT-systemer behandler personopplysninger om elever i videregående opplæring, og hvilke personopplysninger behandles i de ulike IKT- systemene?

Problemstilling 2:

I hvilken grad er det etablert grunnleggende retningslinjer og rutiner for tilgangsstyring i IKT-systemer som behandler elevdokumentasjon?

Problemstilling 3:

I hvilken grad er det etablert rutiner og praksis for kontroll av tilgangsstyringen i utvalgte IKT-systemer som behandler personopplysninger om elever i videregående opplæring?

Metode

- Intervjuer.
- Gjennomgang av tilganger i utvalgte IKT-systemer.
- Dokumentanalyse av relevante dokumenter og rutiner fra fylkeskommunene.
- Verifisering av intervjureferater, fakta-kapittelet ble sendt fylkeskommunen for gjennomgang, og innhenting av uttalelse fra fylkeskommunedirektøren på utkast til rapport.

Kilder til revisjonskriterier

- Personopplysningsloven og personvernforordningen (GDPR)
- Kommuneloven kap. 25 om internkontroll
- Fylkeskommunens egne styringsdokumenter som omhandler tilgangsstyring og ivaretagelse av personvern
- Datatilsynets veiledning om virksomheters plikter etter personvernregelverket
- Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet versjon 2.0
- ISO/IEC 27001 - Ledelsessystem for IKT-sikkerhet

Konklusjoner

Problemstilling 1- IKT-systemer

- IKT-systemer der elevdokumentasjon registreres og behandles er VIGO, Visma InSchool, Engage, Oppfølgingsloggen, Elements, Microsoft Office 365 og LAO.
- Disse IKT-systemene lagrer og behandler store menger av personopplysninger om elever.

Problemstilling 2 – grunnleggende retningslinjer

- Revisjonens hovedkonklusjon er at fylkeskommunen i mindre grad har etablert grunnleggende retningslinjer og rutiner for tilgangsstyring som bør være på plass for at tilgangsstyringen skal fungere best mulig.
- Fylkeskommunen har på tidspunktet for revisjonen ingen overordnet retningslinje for tilgangsstyring, selv om de har på plass enkelte deler av hva en overordnet rutine bør inneholde.

Problemstilling 3 –tiltak for tilgangsstyring

- Revisjonens hovedkonklusjon er at fylkeskommunen i mindre grad har etablert tilfredsstillende tiltak for tilgangsstyring i utvalgte IKT-systemer som behandler personopplysninger om elever.
- Av IKT-systemene som ble undersøkt er det kun Visma InSchool som har dokumentert hvordan arbeidet med tilgangsstyring skal gjennomføres.

Anbefalinger

1. **Fylkeskommunen bør utarbeide og implementere overordnet retningslinje for tilgangskontroll basert på en overordnet informasjonsklassifisering. Retningslinjen bør inneholde følgende punkter:**
    a) Tilgang tildeles i samsvar med tjenstlig behov, herunder vurdering av hvilken tilgang som er nødvendig.
    b) Rutiner for tildeling, endring, sletting og kontroll av tilganger. Rutiner for autentisering basert på graden av sensitivitet i personopplysningene og hvilken enhet pålogging skjer fra.
    c) Tildeling av rettighet til tilgang (autorisasjon) skal registreres i et register.
    d) Ansvarsfordeling innen tilgangskontrollen.

Anbefalinger forts.

2. For å sikre personopplysninger om elever i IKT-systemer som behandler sensitive personopplysninger og/eller store mengder personopplysninger, bør fylkeskommunen iverksette to-faktor autentisering i Feide.
3. Fylkeskommunen bør iverksette sikkerhetsovervåking for å oppdage sikkerhetshendelser knyttet til tilgangskontrollen.
4. Administratorprivilegier bør ha separate brukerkontoer dersom det er teknisk gjennomførbart. Som minimum bør administratorkontoer være beskyttet av to-faktor autentisering.

Anbefalinger forts.

5. Fylkeskommunen bør sørge for jevnlig kontroll av tilganger i IKT-systemer som behandler elevdokumentasjon, spesielt tilganger med utvidete rettigheter (administratortilganger).

6. Fylkeskommunen bør innrette tilgangsstyringen i IKT-systemene i henhold til risikovurdering av informasjonsverdiene i systemet.