Utdannings-
direktoratet

Ta hensyn til personvernet ved bruk av KI

Dersom skolen tar i bruk KI i undervisningen, må løsningene være godkjent og personvernvurdert av skoleeier. Her følger råd om sikre KI-løsninger.

ARTIKKEL | SIST ENDRET: 08.11.2024

Selv om ikke all bruk av KI tilsynelatende innebærer bruk av personopplysninger, skal det imidlertid mye til for at personopplysninger ikke behandles overhodet. Bruken av KI i opplæringen må derfor være innenfor de rammer skoleeier har satt, slik at elevenes og ansattes personvern og informasjonssikkerhet er ivaretatt.

Selv om skolen ønsker å bruke løsninger som skoleeier har godkjent, må skolen vurdere om den pedagogiske fordelen med å bruke det aktuelle KI-verktøyet i det konkrete tilfellet veier opp for eventuelle personvernkonsekvenser. Det henger sammen med at bruk av personopplysninger alltid skal begrenses til det som er nødvendig for formålene med bruken.

Språkmodeller er ett eksempel på bruk av KI som flere skoleeiere/skoler har tatt i bruk. Det en elev legger inn i en språkmodell kan fort identifisere eleven selv eller andre, særlig når språkmodellen setter denne informasjonen sammen med andre opplysninger språkmodellen kan få tak i.

Tips til skoleeiere som ønsker å benytte språkmodeller

Ikke bruk språkmodeller som trener på informasjonen den får

Ikke bruk språkmodeller som trener på informasjon den mottar av elever eller ansatte. Hvis man lar språkmodellen trene på informasjonen elever eller ansatte legger inn, deler man personopplysninger uten å ha rettslig grunnlag for det. Da har dere ikke lenger kontroll på personopplysningene.

Dersom skoleeier tar i bruk språkmodeller som bruker opplysningene til å trene seg opp, må både skoleeier

og leverandør av språkmodellen ha behandlingsgrunnlag for hver sin bruk av opplysningene. Skoleeier må ha behandlingsgrunnlag for å dele opplysningene med leverandøren av språkmodellen til et slikt formål, og leverandøren av språkmodellen blir behandlingsansvarlig for sin bruk av personopplysningene og må derfor også ha et behandlingsgrunnlag.

Unngå gratisverktøyene

Det kan være fristende å ta i bruk språkmodeller som er gratis, men disse innebærer ofte svakt personvern og forbehold om viderebruk av personopplysningene, og må derfor unngås.

Benytt modeller som lagrer minst mulig informasjon

Skolen bør i størst mulig grad benytte språkmodeller/leverandører som ikke lagrer informasjon som legges inn i språkmodellen. Hvis noe lagres, for eksempel i forbindelse med innlogging, bør det som skrives inn i språkmodellen ikke enkelt kunne kobles med hvem som har skrevet det inn.

Snakk med elevene om hva de kan skrive og ikke

Vær oppmerksom på at det som legges inn i språkmodellen kan være personopplysninger, selv om leverandøren ikke kjenner elevens identitet. Snakk med elevene om hva man kan skrive i språkmodellen og ikke – det er ikke bare navn som identifiserer personer når det som skrives kan kobles med opplysninger som kan hentes andre steder.

Sørg for tilstrekkelig opplæring

Sørg for tilstrekkelig opplæring av lærere og elever – om muligheter språkmodellen gir, om personvernrisiko ved bruk av språkmodellen og skoleeiers føringer for bruk av språkmodeller.

Skoleeier skal ha full oversikt over personvernopplysninger

Skoleeier skal ha full oversikt over sin og leverandørers behandling av personopplysninger og iverksette tekniske og organisatoriske tiltak som gjør at personvernregelverket følges. Dette betyr at skoleeier må gjøre mange viktige vurderinger – før dere samler inn og bruker personopplysninger i f.eks. språkmodeller. Skoleeier har også ansvar for å dokumentere at de selv og skolene deres følger loven. Skoleeier må blant annet huske på at:

- Skolen må ha klart angitte formål med bruk av en språkmodell, siden det er stor sannsynlighet for at den bruker personopplysninger. Formålet med behandling av personopplysninger i språkmodeller i opplæringen, vil vanligvis måtte knyttes til kompetansemål i Læreplanverket.
- Skoleeier må gjennomføre en personvernkonsekvensvurdering (DPIA) før dere tar i bruk en

språkmodell.

- Databehandleren har ikke lov til å bruke personopplysninger fra dere videre til egne formål, med mindre dette er avtalt med dere og formålet er forenelig med formålet om å gi opplæring.
- Skoleeier skal ha en behandlingsprotokoll. I protokollen skal det blant annet stå hvilke personopplysninger som blir behandlet i språkmodellen, hvilke behandlinger som skjer, hva som er det rettslige grunnlaget for de ulike behandlingene, hvor opplysningene behandles og ev. hjemmel hvis opplysningene behandles utenfor EØS.
- Hvis dere tar i bruk en språkmodell, vil leverandøren behandle personopplysninger på vegne av skoleeier. Skoleeier må da ha en databehandleravtale med leverandøren om behandlingsaktivitetene. Det er viktig at blant annet tilgangskontroll reguleres i databehandleravtalen.
- Dere må kunne ivareta de registrertes rettigheter. Det betyr blant annet at dere må informere ansatte, elever og foreldre om bruken av personopplysninger, og gi innsyn hvis de ber om det. Databehandleren må kunne hjelpe dere med innsyn i de personopplysningene de har. Dere kan lese mer om de registrertes rettigheter på Datatilsynets nettside.
- Skoleeier må ha rutiner for å kontrollere om det gjøres endringer i språkmodellen, og gjør nye vurderinger av personvernet og informasjonssikkerheten der endringer påvirker vurderingen som er gjort.

> Bruk av KI innebærer ofte behandling av personopplysninger, og slik bruk av KI i opplæringen innebærer at skolen/skoleeier må ha et behandlingsgrunnlag. Hvis bruk av språkmodeller i opplæringen er egnet for at elevene tilegner seg kunnskap i henhold til læreplanverket, vil behandlingsgrunnlaget være personvernforordningen art. 6 nr. 1 bokstav e, sammen med relevant bestemmelse i opplæringsloven og læreplanverket.

Tips ved anskaffelse av en språkmodell

For at skoleeiere, elever og ansatte på skolene skal kunne benytte seg av sikre språkmodeller, må skoleeier som hovedregel kjøpe tilgang til en språkmodell.

Offentlige skoler/skoleeiere må huske på å overholde anskaffelsesregelverket. I forkant av og i anskaffelsesprosessen kan det være nyttig å tenke på følgende:

- Personene som skal gjennomføre anskaffelsen hos skoleeieren bør ha riktig bestillerkompetanse for det aktuelle innkjøpet. Dette vil ofte være bl.a. juridisk kompetanse innen personvern og informasjonssikkerhet, pedagogisk kompetanse og teknisk kompetanse innen bl.a.

informasjonssikkerhet.

- Sett krav til personvern og informasjonssikkerhet i kravspesifikasjonen, da dere ikke kan bruke digitale løsninger som vil bryter med personvernregelverket.
    - Hvis dere kjøper et system, sørg for at systemet har innebygd personvern, herunder overholder prinsippet om dataminimering.
    - Hvis dere kjøper funksjonalitet som dere selv skal sette sammen til en løsning, sørg for å vurdere personvern og informasjonssikkerhet i både funksjonaliteten dere anskaffer og den planlagte løsningen deres.
- Bruk kun leverandører som dere får en tilfredsstillende databehandleravtale med. Da har dere mer kontroll på hvordan personopplysninger benyttes, og dere skal varsles ved endringer i språkmodellen.
- Vi anbefaler avtalevilkår som gjør at skoleeier enkelt kan tre ut av avtalen dersom personvernet og informasjonssikkerheten ikke lenger er tilfredsstillende.
- Skoleeiere bør kreve at språkmodellene kan "pre-promptes" (instrueres) av både skoleeier og den aktuelle læreren, slik at det kun er mulig å stille spørsmål innenfor klart angitte rammer.
- Undersøk språkmodellens muligheter for å ivareta de registrertes rettigheter, eksempelvis innsyn og sletting.
- Kartlegg alle steder hvor personopplysningene vil, eller kan, sette spor etter seg, slik at dere har fullstendig oversikt over dataflyten før dere anskaffer språkmodellen. Vær ekstra forsiktig dersom personopplysninger behandles utenfor EØS. Eksempelvis gjennomføres supporttjenester gjerne ulike steder i verden, avhengig av tiden på døgnet. Behandler supporttjenesten personopplysninger, vil det skje en overføring av personopplysninger til det landet supporten gjennomføres fra. Undersøk derfor om det er mulig å avtale at support kan gjennomføres uten at supporttjenesten får tilgang til personopplysninger.

Informasjon og veiledning om KI andre steder:

- Digdirs veileder for kunstig intelligens
- KiNS – policy for kunstig intelligens (pdf laget 28. juni 2024)
- KS – hva må jeg gjøre før jeg kan ta i bruk en ny digital tjeneste?
- KS – nasjonal DPIA for Google
- Datatilsynet - Secure Practice, sluttrapport
- Datatilsynet – Sluttrapport i AVT-prosjektet