



STYRELSEN FOR
IT OG LÆRING

Børne- og Undervisningsministeriet, Styrelsen for It og Læring

Tillæg til "Vejledning om lovlig brug af kunstig
intelligens for uddannelsesinstitutionerne"

Indholdsfortegnelse

Indledning	3	
Ledelsesansvar	4	Case 2 - brug af AI-værktøj til at opdage snyd ved skriftlige hjemmeopgaver 18
Oversigt over skolens trin-for-trin-afklaringer ved brug af AI-løsninger efter GDPR og AI-forordningen.	5	Case 3 - brug af AI-ansigtsgenkendelse til registrering af elevfravær 20
Trin 1: Kortlæg jeres AI-løsninger, deres risikoniveau og behandling af personoplysninger	6	
Trin 2: Kortlæg jeres rolle i forhold til AI-systemerne	8	
Trin 3: Vurdér lovligheden af AI-systemerne	8	
Trin 4: Vurdér risikoniveauet for jeres AI-systemer	10	
Trin 5: Oplys de registrerede om behandlingen af deres personoplysninger og håndter deres rettigheder	11	
Trin 6: Fastsæt centrale politikker og retningslinjer	12	
Trin 7: Undervis medarbejderne i AI-færdigheder og jeres politikker og procedurer	14	
Case 1 - brugen af AI til feedback på elevers opgaver	16	

Indledning

Den 28. maj 2025 udkom *Vejledning om lovlig brug af kunstig intelligens for uddannelsesinstitutionerne*. Det var allerede forinden planen, at der skulle udgives en miniguide, der vil skulle fungere som en praktisk og lettilgængelig guide for bl.a. institutionerne i deres daglige arbejde.

Efter udgivelsen har Styrelsen for It og Læring modtaget respons og input fra en bred skare af institutioner, organisationer m.fl. Her efterspørges bl.a. en operationalisering af vejledningen med flere konkrete eksempler, en grafisk oversigt samt at det præciseres tydeligere, hvor ansvaret for at ibrugtage en AI-løsning ligger.

Formålet med denne miniguide samt tilhørende bilag er således primært at:

1. Klarlægge hvem der har ansvaret ved ibrugtagning af AI-løsninger.
2. Udtrække de vigtigste pointer fra vejledningen og de 7 trin samt udarbejde en grafisk oversigt, som kan hjælpe en bredere skare af medarbejdere på uddannelsesinstitutionerne, når de skal forholde sig til, hvad de skal være opmærksomme på, når de ibrugtager en AI-løsning.
3. Give konkrete og brugbare eksempler på brugen af vejledningen og førnævnte grafiske oversigt i relevante cases fra uddannelsesinstitutionerne.

4. At stille en skabelon til rådighed som skal anses som et understøttende rådgivningsværktøj for uddannelsesinstitutionerne, som de kan hente inspiration fra og tage udgangspunkt i, når de skal risikovurdere et AI-system.

Hvor vejledningen henvendte sig mest til jurister og complianceansvarlige i sektoren, så er det meningen, at denne miniguide skal henvende sig til et bredere publikum og være et brugbart redskab for særligt fagfolk, blandt andet lærere, skoleledelse, rektor samt øvrige medarbejdere, der kan betragte denne guide som et operationelt redskab (tjekliste) i vurderingen af, om en konkret AI-løsning (f.eks. en ny app) er lovlig - inden de tager den i brug i klasserummet.

Som responsen på vejledningen også bevidner, så er området omkring kunstig intelligens både nyt, svært og i rivende udvikling. Det er svært at give klare ja/nej svar på særlig meget. Derfor tages der også generelt et forbehold for, at der skal foretages konkrete vurderinger - en juridisk vurdering (f.eks. lovgiggørelse efter GDPR), en risikovurdering (jf. trin 4) samt en etisk/pædagogisk vurdering af systemets formål. Det er med andre ord et komplekst område, og der er grænser for hvor meget det kan koges ned og simplificeres. Men med fælles hjælp og åben dialog kommer vi et godt stykke.

Derudover kan man også læse STUKs anbefalinger for brug af generativ kunstig intelligens i undervisningen på landets ungdomsuddannelser på nedenstående link: [Nu kommer anbefalinger for brug af generativ kunstig intelligens i undervisningen på landets ungdomsuddannelser | Børne- og Undervisningsministeriet](#).

Ledelsesansvar

Det er det klare udgangspunkt, at det er uddannelsesinstitutionernes eget ansvar, såfremt de vil tage en AI-løsning i brug. Børne- og Undervisningsministeriet (BUVM) har en generel vejledningsforpligtelse, hvilket også er baggrunden for både vejledning om lovlig brug af kunstig intelligens for uddannelsesinstitutionerne og nærværende miniguide.

AI-forordningen træder i kraft trinvist og der indføres med forordningen et nyt risikobaseret system (udover GDPR), hvor institutionen skal vurdere om en AI-løsning er forbudt eller har en minimal- eller høj risiko (f.eks. evaluering af læringsudbytte). Dette medfører mere omfangsrige forpligtelser for institutionen.

Når en uddannelsesinstitution vælger at tage en AI-løsning i brug, skal ibrugtagning ske inden for rammerne af GDPR samt AI-forordningen. Ibrugtagning vil derudover falde inden for institutionens ansvar for den daglige drift og forvaltning, som institutionens ledelse overordnet set har ansvaret for.

En sådan beslutning om ibrugtagning har i øvrigt et vist omfang og tyngde, som en ledelse bør være involveret i, således at det ikke er en enkelt medarbejder, der står i et klasselokale og skal træffe beslutning om, hvorvidt og hvordan en AI-løsning kan tages i brug.

Derfor er det vigtigt, at ledelsen hjælper medarbejderne ved at opstille klare og tydelige retningslinjer for ibrugtagning af nye IT-løsninger. Det er også vigtigt, at ledelsen tager ansvar for deres medarbejderes kendskab hertil, så den enkelte medarbejder ude i klasselokalet altid er bekendt med skolens retningslinjer og i øvrigt søger sparring hos ledelsen, hvis der opstår usikkerhed i en given situation.

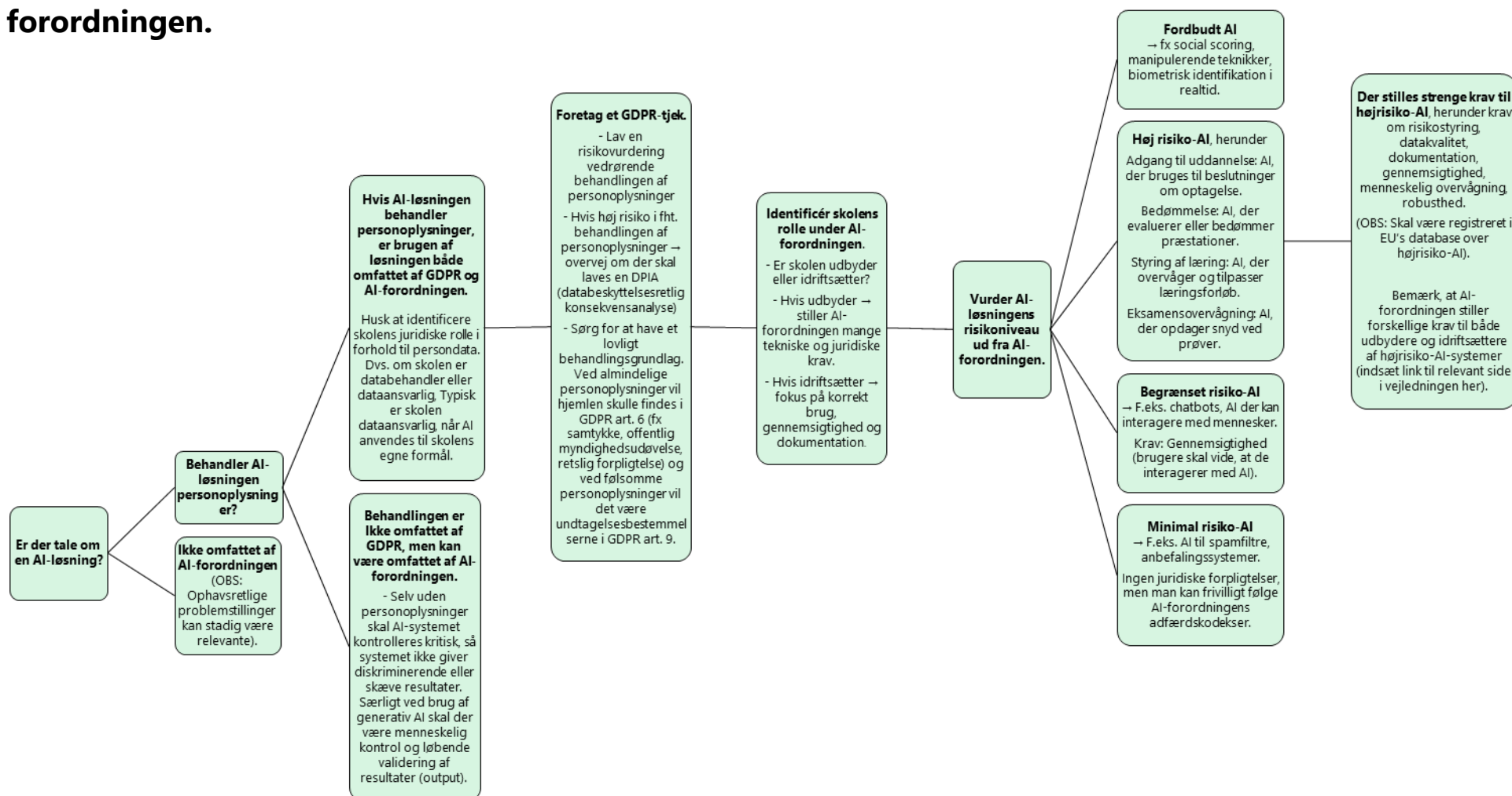
Undersøgelse fra Microsoft Danmark

I en undersøgelse¹ som Microsoft Danmark har fået udarbejdet, svarer 7 ud af 10 af de adspurgte medarbejdere på danske arbejdspladser, at de bruger AI-værktøjer, som ikke officielt er stillet til rådighed af deres arbejdsgiver.

Det fremgår endvidere af undersøgelsen, at blot 30 procent af virksomhederne i undersøgelsen har klare retningslinjer for brug af kunstig intelligens.

I praksis kendes det som "Skygge AI", hvor løsningen bliver at fastsætte en klar "AI-politik" (trin 6) og en liste over godkendte AI-værktøjer for at undgå uautoriseret og potentielt ulovlig brug. Dette sikrer, at ansvaret ikke falder tilbage på den enkelte underviser.

Oversigt over skolens trin-for-trin-afklaringer ved brug af AI-løsninger efter GDPR og AI-forordningen.



Bemærk: Dette er en forenklet oversigt og ikke en udtømmende gennemgang af de krav, som en dataansvarlig skal overholde i medfør af GDPR og AI-forordningen.

Den dataansvarlige skal altid sikre efterlevelse af de grundlæggende principper i GDPR, herunder bl.a. artikel 5 (lovlighed, rimelighed, gennemsigtighed, formålsbegrænsning, dataminimering, rigtighed, opbevaringsbegrænsning, integritet og fortrolighed, samt ansvarlighed). Hertil kommer krav om bl.a. fortegnelse over behandlingsaktiviteter, oplysningstekster til de registrerede samt indgåelse af databehandlaftertaler mm.

1.1 Trin 1: Kortlæg jeres AI-løsninger, deres risikoniveau og behandling af personoplysninger

Identificér hvilke AI-systemer I bruger

Første skridt er at skabe overblik over, hvilke AI-systemer I bruger, og hvilke løsninger der blot er software uden AI. Ifølge AI-forordningen forstås et AI-system som en løsning, der er bygget på en AI-model og stilles til rådighed i en bestemt anvendelseskontekst. AI adskiller sig fra traditionel software ved at kunne lære, ræsonnere eller modellere på baggrund af data og i et vist omfang tilpasse sig efter idriftsættelsen.

Et AI-system kan levere forudsigelser, anbefalinger, beslutninger eller indhold ud fra det input, det modtager. Bag teknologien kan der ligge maskinlæring, hvor systemet lærer af data, eller logik- og vidensbaserede metoder.

Lav en samlet oversigt over alle AI-systemer, der bruges på f.eks. jeres skole – både store og små. Det giver jer et klart billede af, hvor AI er i spil, og hvordan det bruges.

Vær opmærksom på personoplysninger

Databeskyttelsesforordningen gælder for al elektronisk behandling af personoplysninger. Det betyder, at reglerne også gælder, når I udvikler, træner, bruger, opdaterer eller vedligeholder AI, hvis personoplysninger indgår. Personoplysninger kan findes både i de data, I lægger ind i AI (fx prompts) og i det output, systemet genererer (fx svar). Begge dele skal håndteres efter databeskyttelsesreglerne.

Dokumentér og opdater løbende

Brug gerne en skabelon eller tabel (fx Bilag B i vejledning om lovlig brug af kunstig intelligens for uddannelsesinstitutionerne) til at strukturere kortlægningen. Sørg for at opdatere oversigten jævnligt, så I kan dokumentere over for myndigheder som Datatilsynet og Digitaliseringsstyrelsen, at I overholder kravene i både AI-forordningen og databeskyttelseslovgivningen.

Faktaboks: Kortlæg AI

Find ud af: Hvilke systemer der anvender AI

Tjek op på: Kontroller, at både de data, der bruges, og de resultater, systemet leverer, følger GDPR

Dokumentér: Lav en oversigt og hold den regelmæssigt opdateret

Sådan skelner du AI-software fra software uden AI

Software uden AI	Software med AI
Følger faste regler og instruktioner, som udvikleren har defineret.	Kan lære af data, erfaring eller brugermønstre og tilpasse sine handlinger.
Reagerer altid ens på de samme input.	Kan give forskellige resultater ved samme input, afhængigt af kontekst eller tidligere læring.
Udfører opgaver trin-for-trin efter en forudbestemt logik.	Anvender modeller til at analysere, forudsige, generere eller beslutte på egen hånd.
Eksempler: Tekstbehandlingsprogram som Microsoft Word, PowerPoint, regneark, kalendersystemer og planlægningsværktøjer som fx Outlook og Google kalender.	Eksempler: Chatbots, billedgenkendelse, tekstgeneratorer, billedgenerator, anbefalingssystemer.

Det centrale juridiske kendetegn ved et AI-system er, at det kan tilpasse sig og skabe output på baggrund af mønstre i inputdata. Det adskiller sig fra traditionel software, som blot udfører faste, forudbestemte regler (som f.eks. et regneark).

Det vil sige, at hvis systemet "forstår", "anbefaler", "genkender" eller "forudsiger" noget baseret på data og på denne baggrund levere et output, så bruger det sandsynligvis AI.

Trin 2: Kortlæg jeres rolle i forhold til AI-systemerne

Rolle efter databeskyttelsesforordningen

Det er vigtigt at afklare, om I er dataansvarlige eller databehandler, da kravene i databeskyttelsesforordningen er forskellige.

Den dataansvarlige bestemmer formålet med databehandlingen og hvilke hjælpemidler, der bruges. En databehandler behandler oplysninger på den dataansvarliges vegne og efter instruks.

Uddannelsesinstitutionens typiske rolle

I langt de fleste tilfælde er skolen dataansvarlig, når personoplysninger behandles til skolens egne formål – fx klassedeling eller eksamensplanlægning. IT-leverandører, der driver skolens systemer, vil typisk være databehandler.

Hvis en elev og/eller lærlinge (i det følgende refererer 'elev' til elever og/eller lærlinge) på eget initiativ downloader og bruger en AI-app på privat udstyr uden skolens anvisning, er skolen hverken dataansvarlig eller databehandler.

Hvis skolen har instrueret, opfordret eller udstyret eleverne til at bruge en bestemt AI-løsning, vil skolen normalt være dataansvarlig for behandlingen af personoplysninger i den bestemte AI-løsning, samt for instruktioner i sikkerhedsmæssig korrekt anvendelse.

Rolle efter AI-forordningen

Under AI-forordningen skal I også afklare, om I er idriftsætter eller udbyder af AI-systemer. Skoler vil oftest købe færdigudviklede AI-løsninger fra en leverandør og derfor vil skolerne ud fra AI-forordningen betragtes som "idriftsættere". Men hvis I ændrer formålet, foretager større ændringer eller markedsfører systemet under eget navn, kan I blive betragtet som udbydere hvorefter dette vil medføre et større ansvar.

Faktaboks: Kend jeres rolle

Afklar: Er I dataansvarlige eller databehandler?

Typisk: Skolen er dataansvarlig, mens IT-leverandører er databehandler.

AI-forordningen: Skoler er oftest idriftsættere – men kan blive udbydere ved større ændringer.

Når jeres rolle er kortlagt, er det vigtigt at få kommunikeret dette tydeligt til ansatte samt eleverne i forhold til deres ansvar.

Trin 3: Vurdér lovligheden af AI-systemerne

Forbudte AI-praksisser

AI-forordningen forbyder visse typer af AI-systemer, især dem der kan manipulere menneskers underbevidsthed eller udnytte sårbare grupper på en måde, der kan forvolde fysisk eller psykisk skade. Det gælder fx systemer med skjulte beskeder, der kan påvirke elevers valg uden deres viden. Et særligt eksempel i undervisningssektoren er AI, der aflæser følelser hos elever ved hjælp af kamera, stemmeanalyse eller biometriske data for at tilpasse undervisningen – dette vil være omfattet af forbuddet i artikel 5 i AI-forordningen, da det indebærer en høj risiko for indgreb i privatlivets fred og menneskelig værdighed.

Højrisiko systemer

Hvis I anvender et højrisiko-AI-system, skal det bruges i overensstemmelse med brugsanvisningen, og overvågning skal udføres af kompetente personer. Inputdata skal være relevante og repræsentative for formålet. Systemets drift skal løbende overvåges, logfiler skal gemmes i mindst seks måneder, og eventuelle risici skal rapporteres til leverandør og myndigheder. Systemet skal registreres i EU's database (når denne åbner), og der skal i de fleste tilfælde laves en konsekvensanalyse af påvirkningen af grundlæggende rettigheder. På uddannelsesområdet betragtes AI-systemer som højrisiko, hvis de fx kan overvåge elevernes computere for at opdage snyd, vurdere læringsudbytte, træffe beslutninger om adgang til uddannelse eller styre elevers læringsprocesser.

Begrænset risiko

Hvis I anvender et AI-system med begrænset risiko, skal det overholde specifikke gennemsigtighedskrav fra AI-forordningen. Det betyder blandt andet, at det tydeligt skal fremgå for elever, studerende og undervisere, at de interagerer med en AI og ikke et menneske. Det gælder f.eks. chatbots, generative værktøjer eller virtuelle undervisningsassistenter.

AI-genereret indhold, såsom tekster, billeder eller videoer, skal markeres som skabt af en AI, så brugerne kan forholde sig kritisk til materialet. Systemet må ikke give indtryk af at være en menneskelig underviser uden klar oplysning herom. Der er ingen krav om registrering i EU's database eller konsekvensanalyse.

Minimal risiko

Hvis I anvender AI-systemer med minimal risiko, kan de frit bruges da der ikke stilles krav om gennemsigtighed, registrering eller konsekvensanalyse. Disse systemer fungerer typisk som hjælpemidler, f.eks. stave- og grammatikkontrol, automatisk oversættelse, anbefaling af læringsmateriale eller spilbaserede læringsværktøjer.

Overhold principperne for personoplysninger

Som dataansvarlig skal I sikre, at AI-systemet følger reglerne for behandling af personoplysninger fra starten. Der skal være et klart og lovligt behandlingsgrundlag (jf. GDPR art. 6 og/eller art. 9 ved føl-

somme oplysninger), behandlingen skal være rimelig, og de personer, hvis data bruges, skal have tydelig information om formål, opbevaring og videregivelse.

Forebyg urimelige eller diskriminerende udfald

AI-systemer må ikke give skæve resultater pga. forkerte eller skævt fordelte træningsdata, eller fordi systemet lægger vægt på irrelevante faktorer. Det kan fx være et optagelsessystem, der favoriserer bestemte skoler, eller et støttesystem, der diskriminerer pga. fornavne. Oplysninger må kun bruges til klart definerede formål. Output skal være korrekt, og især ved generativ AI skal man være opmærksom på risikoen for forkerte eller opdigtede svar.

Krav til behandlingsgrundlag

Hver form for databehandling i AI-systemet (indsamling, analyse, videregivelse, opbevaring) skal have sit eget lovlige grundlag. For skoler er dette ofte artikel 6, stk. 1, litra e i databeskyttelsesforordningen (offentlig myndighedsudøvelse), men ved følsomme oplysninger kræves også hjemmel efter artikel 9. Jo mere indgribende behandlingen er, desto klarere skal hjemlen være i lovgivningen. "Harmløse" behandlinger med lav risiko kan ofte ske med den generelle hjemmel, mens mere indgribende analyser kræver særskilt lovhjemmel.

Tjek leverandørernes brug af data

AI-løsninger leveres ofte af store, internationale cloududbydere. Læs altid betingelserne grundigt, især for at sikre, at leverandøren ikke

bruger elevernes data til egne formål som produktudvikling eller markedsføring.

Faktaboks: Krav til AI i undervisningssektoren

Forbudt: AI, der manipulerer, udnytter sårbare grupper eller aflæser følelser (fx via kamera, stemme eller biometriske data).

Høj risiko: Skal overvåges af kompetente personer, have relevante inputdata, logfiler i mindst 6 mdr., risici rapporteres, registreres i EU's database og ofte ledsages af en konsekvensanalyse.

Begrænset risiko: Brugere skal altid informeres om, at de interagerer med AI (fx chatbots, generative værktøjer). AI-genereret indhold skal markeres tydeligt.

Minimal risiko: Frit brug uden registrering eller konsekvensanalyse (fx stavekontrol, oversættelse, læringsspil).

Persondata: Alle AI-systemer skal overholde GDPR med lovligt grundlag, gennemsigtighed og korrekt information til de registrerede.

Saglighed: AI må ikke diskriminere eller give skæve resultater pga. skæve data. Output skal være korrekt, og generativ AI kræver kritisk kontrol.

Leverandører: Tjek altid kontraktvilkår – elevernes data må ikke bruges til andres formål.

Trin 4: Vurdér risikoniveauet for jeres AI-systemer

Vurdering af risici ved AI-brugen

Når en institution beslutter at bruge kunstig intelligens, er det afgørende at identificere de risici, som AI-systemet kan medføre. Det inkluderer både risici for elever og for medarbejdere. Potentielle problemer kan være diskrimination, hvor algoritmen utilsigtet favoriserer nogle elever frem for andre, eller bias i de data, systemet trænes på, som kan skabe uretfærdige resultater. Der kan også opstå fejlinformation, hvis systemet genererer svar eller anbefalinger, der er forkerte eller misledende, hvilket kan påvirke undervisningens kvalitet. Derudover kan manglende gennemsigtighed i beslutningsprocesser også være en risiko, da det kan være uklart, hvordan og hvorfor AI'en træffer bestemte valg, hvilket kan skabe usikkerhed blandt både medarbejdere og elever.

Konsekvensanalyse og DPIA

Når I bruger AI, vil der som udgangspunkt næsten altid være krav om at gennemføre en systematisk analyse af de risici, AI-systemet kan medføre, samt hvordan disse risici kan forebygges. Denne analyse kaldes ofte en konsekvensanalyse eller en DPIA (Data Protection Impact Assessment). Analysen bør blandt andet beskrive formålet med systemet, hvordan persondata behandles, og om brugen af data er nødvendig og proportional i forhold til formålet. Det er også vigtigt at identificere konkrete risici og beskrive, hvilke foranstaltninger der implementeres for at minimere dem. Systemer der fx bruges til karaktergivning eller til at opdage snyd ved prøver udløser omfattende krav for højrisiko-AI, herunder krav om DIPA.

Implementering af sikkerhedsforanstaltninger

Efter risikovurderingen er det centralt at implementere konkrete sikkerhedsforanstaltninger. AI-systemet skal beskyttes mod uautoriseret adgang, hvilket kan indebære brug af kryptering, adgangskontrol og andre it-sikkerhedsforanstaltninger. Systemet skal også opdateres løbende for at lukke eventuelle sårbarheder og forblive i overensstemmelse med f.eks. skolens it-politikker. Det er vigtigt, at alle medarbejdere, som anvender AI, har kendskab til de sikkerhedsprocedurer.

Løbende overvågning og evaluering

Selv efter implementering er arbejdet med AI ikke afsluttet. Det er vigtigt at overvåge systemets præstation og de risici, der kan opstå over tid. Løbende evaluering kan ske gennem feedback fra brugere – både lærere og elever – samt gennem analyser af eventuelle fejl eller utilsigtede konsekvenser, som systemet måtte producere. Overvågningen hjælper desuden med at sikre, at AI-brugen fortsat lever op til lovgivningens krav og f.eks. skolens interne standarder, samtidig med at elevernes trivsel og datasikkerhed prioriteres højt.

Trin 5: Oplys de registrerede om behandlingen af deres personoplysninger og håndter deres rettigheder

Oplys de registrerede om behandlingen af deres personoplysninger og håndter deres rettigheder

Når en skole eller uddannelsesinstitution anvender personoplysninger i et AI-system, er det vigtigt at informere de registrerede – det vil sige elever, forældre og medarbejdere – om, hvordan deres data anvendes. Dette er en central forpligtelse i henhold til GDPR. Oplysningspligten skal være klar, forståelig og tilgængelig, og den skal beskrive formålet med databehandlingen, hvilke data der indsamles, og hvordan de behandles. Det er også nødvendigt at informere om, hvordan de registrerede kan udnytte deres rettigheder, såsom retten til indsigt, berigtigelse, sletning og indsigelse mod behandling. Skolen skal sikre, at disse informationer er let tilgængelige og præsenteret på en måde, der er forståelig for målgruppen, herunder elever i forskellige aldre og med forskellige forudsætninger.¹

Ud over oplysningspligten skal skolen også håndtere de registreredes rettigheder effektivt. Dette indebærer at have klare procedurer for, hvordan

anmodninger om indsigt, rettelse, sletning eller begrænsning af behandling håndteres. Skolen skal sikre, at disse anmodninger behandles inden for de tidsfrister, der er fastsat i GDPR, og at der er en ansvarlig person eller enhed, der koordinerer og følger op på disse anmodninger. Det er også vigtigt at dokumentere alle anmodninger og de truffe foranstaltninger, så der er sporbarhed og gennemsigtighed i processen. Skolen skal være opmærksom på, at visse rettigheder kan være begrænsede i specifikke situationer, f.eks. hvis opfyldelsen af en anmodning vil skade andre rettigheder eller interesser, men disse undtagelser skal være velbegrundede og dokumenterede.

Eksempler på, hvor oplysninger kan gives til de registrerede

- Privatlivspolitik på skolens hjemmeside
- Elevhåndbog eller personalehåndbog
- Intranet eller læringsplatforme (fx Aula)
- Digitale pop-ups/notifikationer i de systemer, hvor personoplysninger behandles

¹ Se skabelon vedr. oplysningspligten fra Datatilsynet:
<https://www.datatilsynet.dk/regler-og-vejledning/blanketter-og-skabeloner>

Trin 6: Fastsæt centrale politikker og retningslinjer

Når uddannelsesinstitutioner bruger AI og samtidig behandler personoplysninger, skal der være klare politikker og procedurer på plads. Det er både et krav i databeskyttelsesforordningen (GDPR) og i AI-forordningen, men det handler også om at skabe tryghed og gennemsigtighed for elever, forældre og medarbejdere. Det betyder blandt andet, at institutionen aktivt skal oplyse om, hvordan de behandler data, samt at denne information skal gives direkte til de registrerede, hvorfor det ikke er nok, blot at lægge dette på en hjemmeside.

Tydelige politikker om data

En vigtig del er udarbejdelsen af en persondatapolitik eller privatlivspolitik. Her skal det tydeligt fremgå, hvem der er dataansvarlig, hvilke oplysninger der behandles, hvad formålet er, hvor længe oplysningerne opbevares, og om de deles med andre. Politikken skal også forklare hvilke rettigheder de registrerede har, for eksempel retten til indsigt og retten til at klage til Datatilsynet. På den måde bliver både elever, forældre og ansatte klar over, hvordan deres oplysninger anvendes, også når der bruges AI-systemer.

Klare retningslinjer for brug af AI

Institutionen bør også have klare og konkrete retningslinjer for brugen af AI. Retningslinjerne skal være rettet mod medarbejderne og tydeligt fastlægge:

1. Godkendte værktøjer: Ledelsen bør opliste, hvilke AI-løsninger der er godkendt til brug, eksempelvis med en henvisning til databehandleraftaler og vurdering af datasikkerhed. Dette sikrer, at medarbejdere kun bruger værktøjer, hvor fortrolige oplysninger håndteres korrekt.

2. Korrekt anvendelse: Retningslinjerne skal instruere i, hvordan de godkendte værktøjer bruges korrekt. Det kan eksempelvis omfatte:

- 2.1. Undgå at indtaste fortrolige oplysninger, såsom persondata, eksamensbesvarelser, karakterer eller andre følsomme oplysninger.
- 2.2. Anvende AI som støtteværktøj frem for at erstatte faglige vurderinger.
- 2.3. Sikre, at output fra AI vurderes kritisk og ikke anvendes ukritisk i beslutninger.

3. Begrænsninger og risici: Medarbejderne skal være opmærksomme på AI's begrænsninger, herunder risiko for fejl, bias eller misfortolkning af data. Retningslinjerne bør fremhæve situationer, hvor AI ikke bør anvendes, og hvilke procedurer der gælder for kvalitetskontrol af AI-genereret materiale.

Eksempel på praksis:

Ledelsen kan i praksis lave en liste over godkendte værktøjer med korte instrukser:

- Værktøj A – kun til generel tekstgenerering, ingen persondata.
- Værktøj B – til analyse af anonymiserede data, med databehandleraftale.
- Værktøj C – må ikke anvendes til elevmateriale eller karakterer.

Derudover kan man tilføje simple "dos and don'ts" for prompting: f.eks. aldrig indtaste fortrolige oplysninger, altid gennemgå output kritisk, og kun bruge AI som et supplement til faglig vurdering

Ansvar og procedurer

Endelig er det vigtigt at have procedurer for at håndtere rettighedsanmodninger, som når elever eller forældre beder om indsigt i deres oplysninger. Procedurerne skal beskrive, hvem der er ansvarlig for at svare, hvordan anmodninger behandles, og hvordan tidsfrister overholdes. Hvis institutionen har en databeskyttelsesrådgiver (DPO), skal denne inddrages i relevante situationer, som ved sikkerhedsbrud eller konsekvensanalyser. Ved at fordele ansvar tydeligt og give de rette personer de nødvendige ressourcer, sikres det, at institutionen kan leve op til reglerne og samtidig beskytte alle involverede parter bedst muligt.

Trin 7: Undervis medarbejderne i AI-færdigheder og jeres politikker og procedurer

For at sikre en ansvarlig og lovlig anvendelse af AI i undervisningen er det essentielt, at alle medarbejdere modtager grundig oplæring i både AI-teknologi og de interne politikker og procedurer, der gælder for brugen af AI-systemer. Oplæringen bør give forståelse for, hvordan AI fungerer, hvilke data der behandles, og hvordan systemerne bruges korrekt og etisk i undervisningen. Målet er at sikre, at både ansatte og elever anvender AI sikkert, bevidst og ansvarligt – fx gennem konkrete eksempler og inspiration til gode prompts.

Undervisningen bør også inkludere kendskab til institutionens retningslinjer for datasikkerhed, beskyttelse af personoplysninger og håndtering af de registreredes rettigheder. Det er vigtigt, at medarbejderne forstår deres ansvar i forhold til at beskytte elevernes data og sikre, at AI-systemerne anvendes på en måde, der er i overensstemmelse med gældende lovgivning og institutionens politikker.

Desuden skal medarbejderne være opmærksomme på de potentielle risici ved AI-brugen, såsom diskrimination, bias og manglende gennemsigtighed i beslutningsprocesser. De skal være i stand til at identificere og håndtere sådanne risici samt vide, hvordan de skal reagere, hvis de opdager problemer eller fejl i AI-systemerne.

Uddannelsen bør være løbende og opdateres regelmæssigt for at følge med i udviklingen af AI-teknologi og ændringer i lovgivningen. Det er også vigtigt at skabe en kultur, hvor medarbejderne føler sig trygge ved

at stille spørgsmål, rapportere bekymringer og bidrage til en ansvarlig anvendelse af AI i undervisningen.

Ved at investere i medarbejdernes AI-kompetencer og sikre, at de er velinformeret om institutionens politikker og procedurer, kan skolen fremme en etisk og lovlig brug af AI, der gavner både elever og ansatte. AI-kompetencer for underviser bør differentieres og blandt andet omfatte følgende tre hovedområder:

1. Teknologisk forståelse (hvordan virker Gen. AI?)
2. Praktisk forståelse (god prompting, AI-pædagogik/didaktik, kildekritik osv.)
3. Etisk/juridisk forståelse (risici ved personoplysninger og bias osv.)

Faktaboks: Eksempler på handlingsplan

- Udpeg en ansvarlig
- Indfør lokale retningslinjer for databeskyttelse
- Afhold kursus/undervisning for medarbejdere
 - Kurset/undervisningen kunne fx indeholde:
 - Interne politikker og procedurer
 - Diskrimination og bias ved anvendelse
 - AI's virkemåde
 - Prompting

Case 1 - brugen af AI til feedback på elevers opgaver

En lærer overvejer at bruge et AI-værktøj til at give feedback på elevers skriftlige opgaver. AI-værktøjet kan analysere teksten og komme med forslag til forbedringer i forhold til struktur, sprog og indhold. Læreren ser det som en mulighed for at give hurtigere og mere individualiseret feedback.

Hvordan kan skolen sikre, at dette sker på en lovlig og ansvarlig måde?

Trin 1: Kortlæg AI-løsningen

Skolen skal først have overblik over værktøjet:

Skolen identificerer, at der er tale om et AI-værktøj, som behandler elevers opgaver (tekstdata). Det skal afklares:

- Hvilke data der behandles: Elevernes opgaver kan indeholde personoplysninger (fx navn, brugernavn og evt. følsomme oplysninger, hvis emnerne i opgaverne berører helbred, religion, politisk overbevisning m.m.).

Værktøjet skal kortlægges: Er det et eksternt cloud-baseret system, eller hostes det lokalt på skolens serverer?

Trin 2: Kortlæg jeres rolle i forhold til AI-systemet

Skolen er dataansvarlig da skolen beslutter, hvorfor og hvordan elevernes data (opgaver) behandles.

Skolen har ansvar for at sikre, at behandlingen sker lovligt og forsvarligt.

Leverandøren af AI-værktøjet er databehandler. Leverandøren behandler data på skolens vegne, fx til at generere feedback.

Skoler vil typisk i dette tilfælde være idriftsættere af AI-systemet: skolen vælger og bruger AI-værktøjet, men udvikler det ikke selv. Skolen kan blive udbyder (leverandør) af AI, hvis skolen foretager større ændringer af systemet, fx ændrer koden eller træner modellen med egne data til andre formål.

Trin 3: Vurdér lovligheden af AI-systemet

Skolen undersøger, om leverandøren af AI-værktøjet lever op til GDPR.

Er der indgået en databehandleraftale, der sikrer, at opgaverne kun bruges til feedback og ikke til modeltræning eller deles med tredjepart? Hvis der ikke foreligger en databehandleraftale eller licensaftale, er det vanskeligt at risikovurdere selve løsningen.

Trin 4: Vurdér risikoniveauet

Potentielle risici:

Uautoriseret deling af elevernes opgaver.

Bias i vurderingerne (fx at AI'en bedømmer sprogligt stærke elever anderledes end andre).

Elever mister tillid, hvis de oplever, at deres arbejde behandles af en "maskine". Derudover skal man være opmærksom på, at der kan være en overtrædelse af databeskyttelsesforordningens artikel 22 hvis læreren ikke kan dokumentere egen afsluttende vurdering og personlige feedback.

Mulige tiltag:

1. Begrænse hvilke data der indtastes (fx ingen følsomme personoplysninger).
2. Test af systemets feedbackkvalitet.
3. Supplere AI-feedback med lærervurdering så AI-systemet ikke er afgørende for bedømmelsen.

Trin 5: Oplysning og håndtering af rettigheder

1. Elever og forældre skal informeres om, at elevernes opgaver behandles af AI, og hvad formålet er.
2. De skal have viden om deres rettigheder: indsigt, mulighed for indsigelse, og sletning af data.
3. Information kan gives i skolens privatlivspolitik samt ved introduktion af værktøjet i undervisningen.

Trin 6: Centrale politikker og retningslinjer

1. Skolen fastsætter klare regler:
 - a. AI må kun bruges som støtteværktøj, ikke som erstatning for lærerens faglige vurdering.
 - b. Eleverne må ikke indtaste følsomme persondata i AI-systemet.

- c. Skolen definerer, hvilke fag og opgavetyper AI-værktøjet kan bruges til, og hvordan feedbacken skal præsenteres for eleverne.

Trin 7: Undervisning og kompetenceudvikling

1. Lærere skal uddannes i korrekt brug af værktøjet, inkl. datasikkerhed og pædagogisk integration.
2. Eleverne skal undervises i at forstå AI-feedback som et værktøj til læring – ikke som en endelig dom.
3. Skolen kan afholde workshops, hvor både lærere og elever diskuterer styrker og begrænsninger ved AI-feedback.

Opsummering:

Casen viser, at brugen af AI til feedback rummer databeskyttelses- og pædagogiske samt etiske udfordringer. For at sikre lovlig og ansvarlig anvendelse skal skolen både have styr på databehandlaftaler, risikovurdering, oplysning til elever og klare retningslinjer. AI kan være et nyttigt supplement, men må aldrig stå alene i den endelige vurdering.

Bemærkning om prøvebesvarelser:

En skriftlig prøvebesvarelse skal bedømmes udelukkende af de allokerede censorer. Det betyder, at kun censorernes faglige vurdering må danne grundlag for karakteren. AI, som f.eks. automatiserede analyseværktøjer, sprogvurderingssystemer eller generative modeller (som ChatGPT), må ikke anvendes i bedømmelsesprocessen.

Case 2 - brug af AI-værktøj til at opdage snyd ved skriftlige hjemmeopgaver

En skole indkøber et AI-system, der scanner elevernes skriftlige besvarelser af hjemmeopgaver i undervisningen for mistænkelige mønstre og indikationer på snyd (fx plagiat eller AI-genereret tekst). Systemet bruges til at understøtte underviseren i at identificere besvarelser, der kræver manuel gennemgang af læreren for at kvalificere en eventuel snydeformodning.²

Hvordan kan skolen vurdere, om dette værktøj er både lovligt og forsvarligt?

Trin 1: Kortlæg AI-løsningen

Skolen identificerer, at der er tale om et AI-værktøj, som behandler elevers opgavebesvarelser (tekstdata).

Data: Elevernes besvarelser af skriftlige hjemmeopgaver, metadata samt personoplysninger som fremgår af besvarelserne (fx navn, brugernavn, initialer og evt. følsomme oplysninger, hvis emnerne berører helbred, religion, politisk overbevisning m.m.).

Værktøjet skal kortlægges: Er det et eksternt cloud-baseret system eller en løsning hostet lokalt? Er der menneskelig kontrol i loop (foretager læreren en manuel kontrol, hvis AI-systemet registrerer en opgave som mulig snyd)?

² Det skal bemærkes, at der i visse sammenhænge også kan opstå ophavsretlige spørgsmål, som kan have betydning for den konkrete vurdering. Dette eksempel er dog alene udarbejdet med henblik på at belyse problemstillinger inden for AI-området og skal derfor ikke betragtes som en udtømmende behandling af eventuelle ophavsretlige aspekter.

Trin 2: Kortlæg risikoniveau og personoplysninger GDPR

Skolen skal afklare sin juridiske rolle i forhold til persondata.

I denne situation vil skolen typisk være dataansvarlig, da skolen bestemmer formålet samt midlerne til behandlingen af elevernes personoplysninger (kontrol af besvarelser af skriftlige hjemmeopgaver). Leverandøren af AI-systemet fungerer som databehandler, fordi systemet alene anvendes til brug for skolens formål.

AI-forordningen

Skolen betragtes som idriftsætter (bruger) af AI-systemet, da den tager løsningen i brug i egen drift og til egne formål. Leverandøren af systemet er derimod udbyder, idet det er dem, der har udviklet og markedsført AI-løsningen.

Trin 3: Vurdér lovligheden af AI-systemet

Skolen skal sikre, at systemet anvendes i overensstemmelse med GDPR.

Det indebærer et lovligt grundlag for behandlingen af elevernes persondata og en databehandleraftale med leverandøren, der klart fastlægger, at data kun må bruges til skolens formål og ikke til fx modeltræning eller tredjepartsdeling.

Som idriftsætter under AI-forordningen skal skolen sikre, at systemet opfylder kravene om transparens, menneskelig kontrol og ansvarlig anvendelse. AI må aldrig træffe automatiske afgørelser uden lærerens indblanding, og elever og forældre skal informeres åbent om systemets brug.

Skolen bør desuden vurdere, om databehandlingens omfang og karakter kræver en konsekvensanalyse (DPIA) efter GDPR.

Trin 4: Vurdér risikoniveauet

Potentielle risici:

- Kan have konsekvenser for elevens standpunktskarakterer.
- Fejlagtige flag (false positives) - systemet kan udpege elever som mistænkt for snyd uden grund.

Mulige tiltag:

- Dataminimering – skolen bør kun dele oplysninger (tekstdata), der er nødvendige for at kontrollere besvarelser af skriftlige hjemmeopgaver for mistænkelig aktivitet/snyd.
- Det skal dokumenteres, at der altid er en lærer, som følger op på systemets output, og at AI'en aldrig "står alene" i vurderingen.

NB: Hvis systemet klassificeres som et højrisikosystem under AI-forordningen, skal skolen desuden være opmærksom på ekstra krav: fx at kunne dokumentere, hvordan systemet bruges, og at der løbende følges op på, om det fungerer korrekt og på en fair måde.

Trin 5: Oplysning og håndtering af rettigheder

Elever (og forældre) skal informeres klart og tydeligt om, at elevernes besvarelser af skriftlige hjemmeopgaver bliver analyseret af AI, formål, databehandlingens grundlag, opbevaringstid, og hvordan de kan udøve deres rettigheder (indsigt, ret til rettelse, klage mv.).

Skolen skal også have procedurer for håndtering af klager og fejl, og mulighed for manuel revurdering.

Trin 6: Centrale politikker og retningslinjer

Skolen fastsætter klare regler for brug af AI til at opdage snyd:

1. AI må kun bruges som støtteværktøj til læreren og må ikke erstatte den faglige vurdering.
2. Skolen fastlægger, hvilke fag og opgavetyper AI-værktøjet må anvendes på, så det udelukkende bruges til at identificere mistanke om snyd.
3. Læreren skal altid gennemgå og vurdere output fra AI-løsningen (både opgavebesvarelser som mistænkes for snyd, og opgavebesvarelser som ikke mistænkes).

Trin 7: Undervisning og kompetenceudvikling

Lærere og administrativt personale skal have målrettet undervisning og kompetenceudvikling, så de forstår, hvordan AI-systemet fungerer, kan anvende det korrekt, vurdere dets output kritisk og sikre, at det bruges ansvarligt og i overensstemmelse med skolens retningslinjer og gældende lovgivning.

Opsummering

Denne case viser, at selvom AI kan understøtte identifikation af snyd, må en sådan løsning aldrig erstatte lærerens faglige vurdering. Desuden skal skolen til enhver tid sikre, at AI-løsningen ikke trænes på elevernes opgaver, indgå en klar databehandleraftale med leverandøren og løbende vurdere risiko og proportionalitet for at sikre, at der ikke kan anvendes mindre indgribende midler til at opdage snyd.

Bemærkning vedr. formålet med indkøbet af AI-systemet

Hvis en skole i stedet for at indkøbe et AI-system, der scanner elevernes skriftlige hjemmeopgaver i undervisningen for mistænkelige mønstre og indikationer på snyd, indkøber et AI-system der skal kunne scanne elevernes skriftlige opgaver for fx stavfejl, vil man fortsat skulle iagttage ovenstående trin, men risikoen og konsekvensen for eleven vil være meget mindre, hvorfor selve systemet, med al sandsynlighed vil blive betragtet som et lav-risiko system.

Case 3 - brug af AI-ansigtsgenkendelse til registrering af elevfravær

Casen om brug af AI til ansigtsgenkendelse ved fraværsregistrering er tænkt som et ekstremt eksempel, der illustrerer nogle af de juridiske og etiske problemstillinger, der kan opstå ved behandling af følsomme data i et AI-system. Casen afspejler ikke de mest almindelige dilemmaer, som uddannelsesinstitutioner aktuelt står overfor i arbejdet med AI. Formålet er derfor primært at give et klart billede af risici og lovgivningsmæssige krav, der gælder, og ikke at anbefale en bestemt praksis, som institutionerne skal følge.

En administrativ medarbejder foreslår at indføre et AI-system med ansigtsgenkendelse, som automatisk registrerer, når elever møder op i klassen. Formålet er at lette arbejdet med fraværsregistrering og sikre mere præcise data.

Hvordan kan skolen vurdere, om dette er lovligt og forsvarligt?

Trin 1: Kortlæg AI-løsningen

Skolen identificerer, at systemet indsamler og behandler biometriske data (ansigtsbilleder), hvilket er en særlig kategori af personoplysninger (følsomme data).

- Formål: dokumentation af fremmøde/fravær.
- Dataflow: billeder/ansigtsdata lagres og analyseres af AI-systemet.
- Leverandør: ekstern udbyder eller internt system?

Trin 2: Kortlæg jeres rolle i forhold til AI-systemet

GDPR

Skolen skal først afklare sin juridiske rolle i forhold til persondata.

Skolen vil typisk være dataansvarlig, da det er skolen, der beslutter, at elevernes ansigter skal registreres for at holde styr på fremmøde.

Hvis AI-systemet leveres af en ekstern udbyder, vil udbyderen normalt være databehandler, da de kun behandler billederne på skolens vegne.

AI-forordningen

Skolen er typisk idriftsætter af AI-systemet, dvs. den aktør, der tager systemet i brug og beslutter, hvordan det skal anvendes i praksis.

Skolen kan blive udbyder, hvis den ændrer systemet betydeligt og tilbyder AI-løsningen til andre.

Trin 3: Vurdér lovligheden af AI-systemet

Biometriske data er særlige kategorier af personoplysninger, jf. GDPR art. 9, og behandling kræver et klart retsgrundlag i både artikel 6 og artikel 9.

Som udgangspunkt er det ulovligt at anvende biometriske data til kontrol eller overvågning, medmindre der foreligger et specifikt undtagelsesgrundlag, fx udtrykkeligt samtykke eller anden lovhjemmel.

Skolen skal vurdere, om der findes hjemmel i lovgivningen.

Trin 4: Vurdér risikoniveauet

Risici:

- Databrud, hvor elevers biometriske data kompromitteres.
- Elever føler sig overvåget og mister tillid til skolen.
- Risiko for fejlregistrering (fx tekniske fejl, bias mod bestemte hudtoner eller ansigtstræk).

Selv ved stærke sikkerhedsforanstaltninger vil risikoen være høj.

Trin 5: Oplysning og håndtering af rettigheder

Hvis systemet mod forventning kan lovliggøres skal elever og forældre informeres detaljeret om formål, dataopbevaring, og rettigheder.

Trin 6: Centrale politikker og retningslinjer

Hvis systemet mod forventning kan lovliggøres, skal skolen udarbejde centrale politikker og retningslinjer for systemet.

Skolen kan, hvis ikke systemet kan lovliggøres, fastsætte retningslinjer for alternative løsninger (fx digital registrering via elevens login eller QR-koder).

Trin 7: Undervisning og kompetenceudvikling

Medarbejdere skal have viden om, hvorfor biometriske data er særligt beskyttede og hvilke begrænsninger der gælder for behandling af sådanne data.

Kompetenceudvikling bør blandt andet inkludere:

- Hvordan AI-løsninger kan håndtere biometriske data, og hvilke risici det medfører (fx overvågning, profilering, sikkerhedsbrud).
- Eksempler på ulovlig brug af biometriske data i AI-systemer
- Praktiske retningslinjer for at undgå utilsigtet behandling af biometriske data, fx hvordan billeder eller videoer håndteres, og hvordan data anonymiseres.

Opsummering:

Denne case viser, at AI-løsninger med ansigtsgenkendelse til fraværsregistrering indebærer meget høje risici og sandsynligvis ikke kan indføres lovligt i en uddannelsesinstitution. Skolen bør i stedet vælge løsninger, der ikke involverer følsomme biometriske data.

