



STYRELSEN FOR
IT OG LÆRING

Vejledning om lovlig brug af kunstig intelligens for uddannelsesinstitutionerne

Indhold

1.	Sammenfatning	4
2.	Indledning, formål og afgrænsning	5
2.1	Indledning og formål	5
2.2	Afgrænsning	6
3.	Hvad er AI og hvordan anvendes det på uddannelsesområdet?	8
3.1	Hvad er AI	8
3.2	Eksempler på anvendelse af AI på uddannelsesområdet	13
4.	Vejledning til uddannelsesinstitutionerne	14
4.1	Overblik	14
4.2	Risikobaseret tilgang	14
4.3	Databeskyttelsesforordningens anvendelsesområde	16
4.3.1	Risikovurdering ift. databeskyttelse som dataansvarlig	19
4.4	Databeskyttelse i et AI-system	21
4.5	De 7 trin	21
4.5.1	Trin 1: Kortlæg jeres AI-løsninger, deres risikoniveau og behandlinger af personoplysninger	22
4.5.2	Trin 2: Kortlæg jeres rolle i forhold til AI-systemerne	24
4.5.3	Trin 3: Vurdér lovligheden af AI-systemerne	25
4.5.4	Trin 4: Vurdér og håndtér risici og sikkerhed	32
4.5.5	Trin 5: Oplys de registrerede om behandlingen af deres personoplysninger og håndtér deres rettigheder	37
4.5.6	Trin 6: Fastsæt centrale politikker og retningslinjer	41
4.5.7	Trin 7: Undervis medarbejderne i AI-færdigheder og jeres politikker og procedurer	44
4.6	Særligt vedrørende egenudvikling af AI-løsninger	49
5.	Hvis I vil vide mere	52
	Bilag A: Ordliste med centrale termer	54
	Bilag B: Kortlægning af AI-løsninger	58

1. Sammenfatning

Denne vejledning har til formål at støtte uddannelsesinstitutioner i en juridisk forsvarlig og ansvarlig anvendelse af kunstig intelligens (AI). Anvendelsen af AI – særligt generativ AI – vinder hastigt indpas i undervisning og administration, men introducerer samtidig komplekse retlige forpligtelser, især i forhold til AI-forordningen og databeskyttelsesforordningen (GDPR).

Vejledningen giver et overblik og en praktisk tilgang til at forstå og navigere i disse regler. Den hjælper uddannelsesinstitutionerne med at kortlægge deres AI-løsninger, identificere deres rolle som idriftsætter eller udbyder, og sikre lovligheden af AI-systemerne, både efter AI-forordningen og databeskyttelsesretten.

Der gives konkrete anbefalinger i form af syv trin, der omfatter alt fra risikovurdering og sikkerhed, til oplysning af de registrerede og uddannelse af medarbejdere. Særligt fokus er lagt på håndtering af personoplysninger, krav om konsekvensanalyser (DPIA), og design af AI-løsninger med indbygget databeskyttelse.

Målgruppen er primært complianceansvarlige, ledelse og undervisere i folkeskoler, ungdomsuddannelser og erhvervsuddannelser. Vejledningen fungerer som både opslagsværk og implementeringsredskab, og støtter institutionerne i at anvende AI på en etisk og juridisk forsvarlig måde.

2. Indledning, formål og afgrænsning

2.1 Indledning og formål

Anvendelsen af kunstig intelligens (AI) på skoleområdet er i hastig vækst og omfatter i stigende grad løsninger som generativ AI, der kan skabe personligt tilpasset undervisningsmateriale, give feedback og understøtte administration. Samtidig er det retlige landskab for AI komplekst og udfordrende at navigere i for mange uddannelsesinstitutioner. AI-forordningen¹ og databeskyttelsesforordningen² stiller omfattende krav til korrekt og sikker anvendelse af AI-løsninger, hvilket skaber behov for en klar og brugervenlig juridisk vejledning.

AI-forordningen trådte i kraft den 1. august 2024, og bestemmelserne heri vil trinvis finde anvendelse som følger:

- 1) Fra den 2. februar 2025 har reglerne om AI-færdigheder og forbudte former for AI-praksis fundet anvendelse.
- 2) Fra den 2. august 2025 vil regler om EU- og nationale organer, AI-modeller til almen brug samt sanktioner finde anvendelse.
- 3) Fra den 2. august 2026 vil øvrige dele af forordningen inkl. transparenskrav og højrisiko-forpligtelser for Bilag III-systemer finde anvendelse.
- 4) Fra den 2. august 2027 vil forpligtelser for Bilag I-systemer finde anvendelse.

Formålet med denne vejledning er at give en overordnet forståelse af reglerne i databeskyttelsesforordningen og AI-forordningen, når uddannelsesinstitutionerne udvikler, anskaffer eller anvender AI-løsninger. Vejledningen sigter mod at skabe en grundlæggende forståelse af reglerne, så uddannelsesinstitutionerne kan implementere AI-løsninger ansvarligt uden unødigt juridisk usikkerhed.

Målgruppen for vejledningen er undervisningssektoren, herunder folkeskoler og grundskoler samt ungdomsuddannelser som gymnasier, erhvervsuddannelser (EUD) og tekniske skoler. Den primære målgruppe er de complianceansvarlige i sektoren, som skal sikre, at uddannelsesinstitutionernes anvendelse af AI-løsninger er i overensstemmelse med gældende regler. Vejledningen kan i øvrigt bruges af undervisere og ledere som en støtte til at forstå de centrale juridiske og tekniske krav samt risici i forbindelse med AI-løsninger.

Med vejledningen er ambitionen at udstyre jer med et konkret redskab, der kan fungere som et opslagsværk i det daglige arbejde med AI. Dette inkluderer en tjekliste for den vurdering, I skal

¹ Europa-Parlamentets og Rådets forordning (EU) 2024/1689 af 13. juni 2024 om harmoniserede regler for kunstig intelligens og om ændring af forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 og (EU) 2019/2144 samt direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (forordningen om kunstig intelligens).

² Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)).

foretage jer i forbindelse med en AI-løsning, så I på en overskuelig måde kan navigere i det komplekse retlige landskab og understøtte en sikker og lovlig anvendelse af AI.

2.2 Afgrænsning

Denne vejledning fokuserer på de retlige og praktiske rammer for anvendelse af AI på uddannelsesområdet, men er ikke en udtømmende fremstilling af alle relevante juridiske aspekter. AI's anvendelse spænder over mange forskellige områder, og de retlige regler, der finder anvendelse, afhænger af den konkrete brugssituation. Det juridiske landskab for AI involverer flere komplekse regler og principper, der bl.a. udspringer af databeskyttelsesret, kontraktret, ophavsret, produktansvarsret og sektorspecifik lovgivning på undervisningsområdet.

Den væsentligste retlige ramme udgøres af databeskyttelsesforordningen, der sætter generelle regler for behandling af personoplysninger, og AI-forordningen, som stiller krav til udvikling, implementering og anvendelse af AI-systemer. Herudover kan nationale regler og sektorspecifik lovgivning på undervisningsområdet også have betydning for uddannelsesinstitutioner, især når AI anvendes i undervisningen eller til administrative formål.

Denne vejledning er afgrænset til primært at omfatte reglerne om behandling af personoplysninger i AI-systemer i henhold til databeskyttelsesforordningen samt reglerne i AI-forordningen. Vejledningen søger at give et overblik over væsentlige retlige forpligtelser og overvejelser, men den favner *ikke* alle retlige problematikker inden for disse retsområder.

Vejledningen omfatter en bred vifte af anvendesscenarier og AI-systemer, der anvendes på uddannelsesområdet. Hovedvægten er lagt på generativ AI, som har særlig relevans i skolesammenhæng. Generativ AI muliggør skabelse af læringsmaterialer, evalueringer og personlig feedback til studerende, hvilket gør det til et centralt værktøj i moderne undervisning.

Uddannelsesinstitutionerne kan overordnet påtage sig følgende roller i relation til AI-løsninger, hvilket har betydning for de retlige forpligtelser:

- 1) Udbyder og idriftsætter af egenudviklede eller tilpassede løsninger: Uddannelsesinstitutionerne står her for både udvikling, implementering og drift af AI-systemet. Dette indebærer et øget ansvar for at sikre, at AI-systemet overholder databeskyttelsesforordningen, AI-forordningen og eventuelle andre regler.
- 2) Idriftsætter af købte standardløsninger: Her køber uddannelsesinstitutionerne færdigudviklede AI-løsninger fra leverandører. Ansvarsfokus flytter sig til korrekt anvendelse af AI-systemet efter AI-forordningen. Og efter databeskyttelsesforordningen vil uddannelsesinstitutionen være dataansvarlig og dermed ansvarlig for at sikre, at databehandlingen sker i overensstemmelse med databeskyttelsesforordningen. Uddannelsesinstitutionen skal stadig foretage en grundig vurdering af leverandørens overholdelse af AI-forordningens krav og sikre, at der foreligger klare aftaler.

Det forudsættes, at uddannelsesinstitutionerne som oftest vil have rollen som idriftsættere efter AI-forordningen og dataansvarlige efter databeskyttelsesforordningen. Denne vejledning har

derfor primært fokus på at belyse, hvordan uddannelsesinstitutionerne anvender AI-løsningerne som standardløsninger, dvs. hvor der ikke er foretaget egenudvikling af løsningerne. Derudover vil fokus være på, hvordan uddannelsesinstitutionerne bruger AI-løsningerne korrekt med henblik på at efterleve de retlige krav i AI-forordningen og databeskyttelsesforordningen.

Det er i afsnit 4.6 beskrevet nærmere, hvad man særligt skal være opmærksom på, hvis man egenudvikler AI-løsninger, herunder behandler personoplysninger i forbindelse hermed.

3. Hvad er AI og hvordan anvendes det på uddannelsesområdet?

3.1 Hvad er AI

Kunstig intelligens ("AI") er en samlebetegnelse for computere og andre maskiner, der er i stand til at analysere, lære og tage beslutninger på en måde, som kan sammenlignes med den menneskelige intelligens.³ AI er derfor grundlæggende en simulering af den menneskelige intelligens i computere og andre maskiner, som er beregnet til at udvikle systemer og teknologier, der kan udføre opgaver, som normalt ville kræve menneskelig intelligens.⁴ AI benytter data og algoritmer (dvs. matematiske formler) til at eftergøre menneskers måde at lære, løse problemer på og træffe beslutninger.⁵

Brugen af AI er på EU-niveau reguleret af AI-forordningen, der trådte i kraft den 1. august 2024. Det bemærkes dog, at flere af reglerne i AI-forordningen trinvis vil træde i kraft i løbet af de næste år (frem til august 2027).⁶

AI-forordningen indeholder de første samlede og bindende regler for brugen af AI på tværs af EU/EØS-området, og har grundlæggende til formål at fremme ansvarlig udvikling og udbredelse af AI inden for EU/EØS-området samtidig med, at der sikres et højt beskyttelsesniveau for sundhed, sikkerhed og grundlæggende rettigheder.⁷

I AI-forordningen defineres et "AI-system", som:

"et maskinbaseret system, som er udformet med henblik på at fungere med en varierende grad af autonomi, og som efter idriftsættelsen kan udvise en tilpasningsevne, og som til eksplicite eller implicite mål af det input, det modtager, udleder, hvordan det kan generere output såsom forudsigelser, indhold, anbefalinger eller beslutninger, som kan påvirke fysiske eller virtuelle miljøer".⁸

AI-forordningens definition af et AI-system indeholder også en afgrænsning i forhold til enklere traditionelle softwaresystemer eller programmeringstilgange; definitionen omfatter således ikke systemer, som er baseret på regler, der udelukkende er defineret af fysiske personer til automatisk at udføre operationer.⁹ Nedenfor gives en række eksempler på tilfælde, hvor der ikke er tale om AI-systemer:

- Et traditionelt skema til karakterberegning, hvor en underviser har indtastet faste regler for vægtning af karakterer i forskellige prøver og beregning af en

³ Etiske [retningslinjer](#) for anvendelse af kunstig intelligens (AI) og data inden for undervisning og læring til brug for undervisere, s. 10, 2022, EU-publikationer.

⁴ [Guide til myndigheder \(digst.dk\)](#)

⁵ [National strategi for kunstig intelligens \(digst.dk\)](#)

⁶ Jf. AI-forordningens artikel 113.

⁷ Jf. præambelbetragtning nr. 1 i AI-forordningen.

⁸ Jf. AI-forordningens artikel 3, nr. 1.

⁹ Jf. AI-forordningens præambelbetragtning nr. 12.

samlet karakter. Dette system vil ikke være omfattet af AI-forordningens definition, da det ikke anvender maskinlæring eller lignende metoder.

- Et administrativt system, der automatisk genererer kursustilmeldingsoversigter baseret på foruddefinerede regler, som er programmeret direkte af institutionens IT-afdeling, såsom at sortere studerende alfabetisk eller efter studieretning. Dette system vil ikke være omfattet af AI-forordningens definition, da der er tale om simple automatiske beregninger uden brug af læring. Systemet udfører opgaverne baseret på faste regler uden at anvende maskinlæring, statistisk modellering eller logikbaseret inferens. Det betyder, at systemet ikke 'lærer' af tidligere data, ikke tilpasser sine metoder over tid og ikke genererer nye regler eller mønstre baseret på erfaring. Systemet udfører alene en mekanisk sorteringsproces, uden at træffe egne beslutninger.
- Et bibliotekssystem, der udløser påmindelser til studerende baseret på faste regler for udlånsperioder og bødeberegning. Dette system vil ikke være omfattet af AI-forordningens definition, da der er tale om simple automatiske beregninger uden brug af læring. Systemet fungerer efter enkle, eksplicit programmerede regler, såsom at sende en påmindelse et bestemt antal dage før en afleveringsfrist eller beregne en bøde baseret på en fast takst. Der sker ingen form for læring, tilpasning eller optimering af reglerne over tid. Bibliotekssystemet analyserer ikke data for at forbedre sine forudsigelser eller beslutninger – det følger blot faste regler uden nogen form for 'intelligens'.
- Et Excel-ark, hvor en uddannelsesinstitution foretager statistiske beregninger.

AI-forordningen omfatter de almindelige, gængse former for AI, herunder "machine learning" ("maskinlæring"), "neural network" ("neurale netværk"), "generativ AI" m.fl. Fælles for disse begreber er, at det er afgørende, at I kender og forstår definitionen af disse begreber, hvis I skal være ordentligt klædt på til at forstå, hvordan I kan anvende AI-systemer i praksis, herunder hvilke muligheder og begrænsninger der medfølger.

En række centrale begreber relateret til kunstig intelligens er derfor defineret i nedenstående tabel 1:

Centralt begreb	Definition
Algoritme	En algoritme kan defineres som en proces eller et sæt af regler, der udføres af en computer, til at løse et problem i et antal trin. Algoritmer kan eksempelvis afdække mønstre i elevernes/de studerendes præstationer og kan hjælpe underviserne med at optimere deres undervisningsstrategier/metoder til at personalisere læring og forbedre resultaterne.¹⁰
(Kunstigt) neuralt netværk	Kunstige neurale netværk (ANN) er computersystemer med indbyrdes forbundne knudepunkter, der fungerer ligesom neuroner i den menneskelige hjerne.¹¹ Ved hjælp af algoritmer kan de genkende skjulte mønstre og sammenhænge i data, og dermed gruppere og klassificere dem og – over tid – løbende lære og forbedre sig.¹² Neurale netværk er bl.a. gode til opgaver, som omhandler billedgenkendelse og sprogforståelse.¹³
Maskinlæring	Maskinlæring er en gren af kunstig intelligens, som har til formål at sætte en computer i stand til at lære af et datasæt uden at blive direkte programmeret hertil.¹⁴ Algoritmerne trænes således til at finde mønstre og korrelationer i store datasæt og, baseret på denne analyse, selv at kunne træffe de bedste beslutninger og forudsigelser. Denne form for kunstig intelligens anvendes hyppigt til at lave AI-systemer.¹⁵ Et eksempel på maskinlæring i praksis er Googles søgemaskinealgoritmer.¹⁶ Maskinlæring kan anvendes til at give den studerende en individuel uddannelsesoplevelse, ved at analysere den studerendes præstationer og f.eks. skræddersy forklaringer efter specifikke fejl.¹⁷

¹⁰ Etiske [retningslinjer](#) for anvendelse af kunstig intelligens (AI) og data inden for undervisning og læring til brug for undervisere, s. 32, 2022, EU-publikationer.

¹¹ [neurale netværk – Lex](#)

¹² [Neurale netværk: Hvad de er & og hvorfor de er vigtige | SAS DK](#), og [Maskinindlæring | Definition, typer og eksempler | SAP og Etiske retningslinjer](#) for anvendelse af kunstig intelligens (AI) og data inden for undervisning og læring til brug for undervisere, s. 35, 2022, EU-publikationer.

¹³ [9 begreber, du bør kende om AI - Aros Business Academy](#)

¹⁴ Etiske [retningslinjer](#) for anvendelse af kunstig intelligens (AI) og data inden for undervisning og læring til brug for undervisere, s. 34, 2022, EU-publikationer.

¹⁵ [Maskinindlæring | Definition, typer og eksempler | SAP](#)

¹⁶ [Fem gloser der er værd at kende om kunstig intelligens - Teknologisk Institut](#)

¹⁷ Etiske [retningslinjer](#) for anvendelse af kunstig intelligens (AI) og data inden for undervisning og læring til brug for undervisere, s. 34, 2022, EU-publikationer.

Centralt begreb	Definition
Dyb læring	Dyb læring er en gren af maskinlæring, som er "dyb", fordi den består af mange lag af det neurale netværk og meget store mængder af komplekse og uensartede data. Systemet er designet til at engagere sig i flere lag i netværket og dermed finde mønstre i den komplekse data og på den baggrund udvikle højere niveauer af outputs. Eksempler på dybe læringsapplikationer er talegenkendelse, billedklassifikation m.m.¹⁸ AI-systemer med dyb læring har bl.a. potentiale til at forudsige små aspekter af uddannelsesmæssige præstationer, hvilket kan bidrage til at udvikle strategier for personaliseret læring.¹⁹ Google har eksempelvis tidligere bygget et kunstigt neuralt netværk, som kan gennemgå videoer på YouTube og identificere katte uden menneskelig instruktion i, hvordan en kat defineres.²⁰
Superviseret læring (overvåget læring)	Superviseret læring er en læringsmetode, der er en gren af maskinlæring. Ved superviseret læring bliver algoritmen trænet med dataeksempler (input), som på forhånd er markeret med et korrekt output. Formålet er, at modellen efterfølgende kan bruge det tidligere markeret data til at genkende nye lignende datasæt. Algoritmen trænes således i at generalisere og finde ligheder i nye datasæt på baggrund af det gamle datasæt.²¹ I praksis kan nævnes e-mail spamfiltre, hvor algoritmen er blevet trænet i et stort datasæt, som har illustreret, hvordan en spammail typisk vil se ud. Systemet lærer herefter at genkende fremtidige spammails.²²

¹⁸ [Maskinindlæring | Definition, typer og eksempler | SAP](#)

¹⁹ Etiske [retningslinjer](#) for anvendelse af kunstig intelligens (AI) og data inden for undervisning og læring til brug for undervisere, s. 34, 2022, EU-publikationer.

²⁰ [Google's Artificial Brain Learns to Find Cat Videos | WIRED](#)

²¹ Etiske [retningslinjer](#) for anvendelse af kunstig intelligens (AI) og data inden for undervisning og læring til brug for undervisere, s. 36, 2022, EU-publikationer.

²² [Fem gloser der er værd at kende om kunstig intelligens - Teknologisk Institut](#)

Centralt begreb	Definition
Ikke-overvåget læring	Ikke-overvåget læring er en læringsmetode, der også er en gren af maskinlæring. I disse tilfælde arbejder en model med inputdata, som ikke på forhånd er markeret med et korrekt output. Formålet er at modellen selvstændigt skal identificere mønstre i datasættet, eksempelvis i form af gruppering af lignende eksempler.²³ Disse mønstre er værdifulde for forudsigelsen af de studerendes præstationer ved at analysere en række kontekstuelle oplysninger som f.eks. demografi samt disses sammenhæng med de samlede resultater.
Generativ AI	Generativ AI er en type kunstig intelligens, og udgør værktøjer, der udnytter en meget stor datamængde til at producere nyt indhold, herunder billeder, lyd, video eller tekst, baseret på input (prompts) fra brugerne. Der er ikke tale om intelligens i menneskelig forstand, idet der er tale om en avanceret model, som på baggrund af datamængderne forsøger at forudsige, hvilken tekst, billede, lyd, video eller andet, der med størst sandsynlighed tilfredsstiller brugeren.²⁴ Generativ AI bygger bl.a. på maskinlæring-teknikker samt dyb læring-teknikker, som indebærer, at en algoritme trænes på meget store datamængder med det formål at kunne lære sammenhængen mellem de forskellige datapunkter. Kendetegnet ved generativ AI er, at algoritmen er i stand til at generere nyt indhold på baggrund af den datamængde, som systemet er trænet på. Værktøjerne bygger endvidere på såkaldte grundmodeller, som er udviklet på en stor og bred mængde af umærkede data (billeder, tekst, lyd, video m.fl.), dvs. data, der er tilgængeligt på internettet, og kan derfor – modsat mange andre former for AI – tilpasses til mange forskellige opgaver. Typeeksemplerne på generativ AI er ChatGPT, Microsoft Copilot 365, Google Gemini m.m.

²³ Etiske [retningslinjer](#) for anvendelse af kunstig intelligens (AI) og data inden for undervisning og læring til brug for undervisere, s. 36, 2022, EU-publikationer.

²⁴ [Guide til myndigheder \(digst.dk\)](#)

Centralt begreb	Definition
Prompt	Brugernes inputs til en AI-løsning, eksempelvis til ChatGPT, kaldes "prompts", og er de spørgsmål eller kommandoer, som brugeren giver til værktøjet for at få et brugbart output. ²⁵

Tabel 1 – Oversigt over centrale begreber inden for AI.

3.2 Eksempler på anvendelse af AI på uddannelsesområdet

AI anvendes i stigende grad til at styrke undervisnings-, lærings- og evalueringsprocesser. AI's anvendelse spænder bredt og omfatter løsninger, der retter sig mod studerende, undervisere og uddannelsessystemer som helhed. De gængse AI-løsninger på skoleområdet dækker en bred vifte af funktioner, f.eks. til sproglæring og automatiseret feedback. Desuden anvendes platforme som Duolingo, der tilbyder realtidsfeedback på udtale og grammatik, og systemer som Grammarly, der automatisk vurderer skriftlige opgaver.

Flere centrale anvendelsescases illustrerer det potentiale, som AI har på dette område. Særlig vigtig er generativ AI, som kan skabe nyt indhold, herunder tekst og opgaver. Dette gør det muligt at generere personaliserede læringsmaterialer, der er skræddersyet til elevernes behov og læringsniveauer. Generativ AI anvendes også til at simulere komplekse scenarier, som giver studerende mulighed for at interagere med realistiske læringsmiljøer.

AI anvendes også til at sikre akademisk integritet gennem tilsyn og overvågning af snyd. Løsninger som plagiatovervågningssystemer analyserer skriftlige opgaver og identificerer potentielle overtrædelser, mens mere avancerede systemer kan opdage uregelmæssigheder i elevernes adfærd eller arbejde, der tyder på uautoriseret hjælp.

En anden central anvendelse er evaluering af de studerendes uddannelsesbehov. AI-systemer som intelligente vejledningsprogrammer analyserer præstationer og anbefaler læringsstier baseret på elevernes individuelle færdigheder og interesser. Læringsanalyseværktøjer giver undervisere indblik i elevernes styrker og svagheder og hjælper med at planlægge, støtte og intervenere.

Derudover anvendes AI til at forbedre den formative og summative evaluering. Automatiske karaktersystemer kan vurdere skriftlige opgaver ud fra kriterier som grammatik, argumentation og struktur, hvilket effektiviserer lærernes arbejdsbyrde og giver eleverne hurtigere feedback.

På systemniveau understøtter AI også ressourceplanlægning og diagnostik. For eksempel bruges AI til at forudsige frafald, planlægge klassefordeling og identificere elever med indlæringsvanskeligheder på et tidligt stadie. Dette gør det muligt for uddannelsesinstitutionerne at optimere deres ressourcer og målrette støtte til de elever, der har størst behov.

²⁵ [Microsoft Word - Guide til offentlige myndigheder om ansvarlig anvendelse af generativ kunstig intelligens.docx \(digst.dk\)](#), s. 1.

4. Vejledning til uddannelsesinstitutionerne

4.1 Overblik

Dette afsnit indeholder en overordnet beskrivelse af AI-forordningens og databeskyttelsesforordningens anvendelsesområde samt centrale bestemmelser heri.

AI-forordningen har et bredt anvendelsesområde og finder anvendelse på offentlige myndigheder og private virksomheder, herunder bl.a. omsætning og brug af AI-systemer. Dette indebærer også, at uddannelsessektoren som udgangspunkt vil være omfattet af AI-forordningen.

De centrale aktører, som reguleres i AI-forordningen, er udbydere og idriftsættere af AI-systemer, idet AI-forordningen dog som udgangspunkt regulerer alle led i værdikæden for produktion og omsætning af AI-systemer.

Ved en udbyder forstås en fysisk eller juridisk person, en offentlig myndighed, etagentur eller et andet organ, der udvikler eller får udviklet et AI-system og bringer det i omsætning eller ibrugtager det under eget navn eller varemærke, enten mod betaling eller gratis.²⁶

En idriftsætter er enhver fysisk eller juridisk person, offentlig myndighed eller ethvertagentur eller andet organ, der anvender et AI-system under sin myndighed.²⁷

4.2 Risikobaseret tilgang

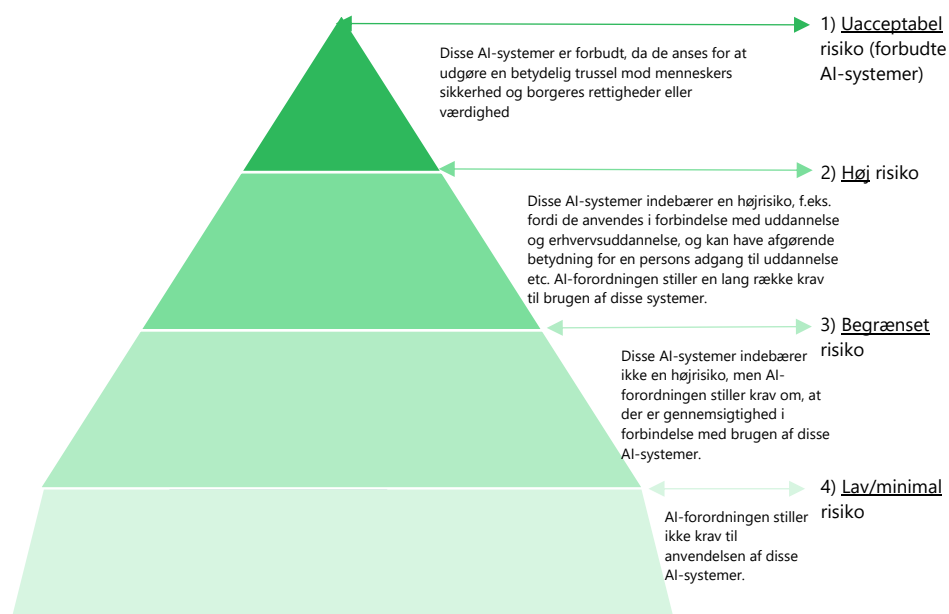
Med AI-forordningen indføres en risikobaseret tilgang. Det betyder, at AI-forordningen opererer med forskellige niveauer af forpligtelser, alt efter hvilken risiko anvendelsen af det enkelte AI-system m.v. medfører samt hvilken rolle (udbyder/idriftsætter) har efter AI-forordningen.

Denne risikobaserede tilgang kan illustreres med en pyramide bestående af fire niveauer, jf. figuren nedenfor. Øverst i pyramiden på niveau 1 er placeret uacceptabel risiko, derunder høj risiko, så begrænset risiko og nederst i pyramiden findes minimal risiko.

Risikoniveauerne er desuden beskrevet yderligere i trin 4 (afsnit 4.5.4) i denne vejledning. Det bemærkes dog, at jo større risikoen er, jo flere krav vil I i udgangspunktet være forpligtet til at efterleve:

²⁶ Jf. AI-forordningens artikel 3, nr. 2.

²⁷ Jf. AI-forordningens artikel 3, nr. 4.



Figur 2 - Pyramide, der illustrerer de fire risikoniveauer efter AI-forordningen.

På niveau 1 i risiko-pyramiden er placeret AI-systemer med en uacceptable risiko og dermed de forbudte AI-systemer. De forbudte former for AI-praksis følger af AI-forordningen artikel 5 og anses for at udgøre en betydelig trussel mod menneskers sikkerhed og borgeres rettigheder eller værdighed. Den forbudte AI-praksis ville f.eks. indebære anvendelse af manipulerende eller vildledende teknikker til at overtale en bruger til at træffe en bestemt beslutning til skade for brugeren eller brug af AI-løsninger til at udlede følelser hos en fysisk person på arbejdspladser og uddannelsesinstitutioner.

På niveau 2 i risiko-pyramiden er placeret højrisiko-AI-systemer.²⁸ Dette omfatter bl.a. selvstændige AI-systemer uafhængige af et produkt, hvor systemet er omfattet af en eller flere af de kritiske områder eller use cases som er angivet i AI-forordningens Bilag III og dermed udgør en høj risiko for menneskers sundhed, sikkerhed eller grundlæggende rettigheder.²⁹ Dette omfatter bl.a. visse former for brug af AI til personaleadministration samt på uddannelses- og erhvervsuddannelsesområdet. I afsnit 4.5.3. er det uddybet, hvilke AI-systemer inden for uddannelse og erhvervsuddannelse der anses for højrisiko-AI-systemer.

For udbydere og idriftsættere af højrisiko-AI-systemer er der en række krav i AI-forordningen, som skal overholdes, og som behandles i afsnit 4.5. og 4.6.

På niveau 3 i risiko-pyramiden er placeret AI-systemer med begrænset risiko. Disse systemer skal overholde specifikke gennemsigtighedskrav, der fremgår af AI-forordningens artikel 50. Disse regler er til for at sikre, at mennesker informeres, når de interagerer med AI-løsninger, når det er nødvendigt og dermed fremmer tilliden. For eksempel skal brugere, der taler eller skriver med en Chatbot, gøres opmærksomme på, at det er et AI-system, og udbydere skal sikre, at AI-genereret indhold kan identificeres.

²⁸ Disse højrisiko-AI-systemer er defineret i AI-forordningens artikel 6, stk. 1, og 2.

²⁹ Jf. AI-forordningen artikel 6, stk. 2.

På niveau 4 i risiko-pyramiden er placeret AI-systemer med minimal eller ingen risiko. AI-forordningen giver mulighed for fri anvendelse af denne form for AI-systemer, herunder anbefalingssystemer i streamingplatforme, der foreslår film eller musik, AI-aktiverede videospil eller spamfiltre m.v.

4.3 Databeskyttelsesforordningens anvendelsesområde

Reglerne i databeskyttelsesforordningen gælder, når I foretager automatisk (elektronisk) behandling af oplysninger, der kan henføres til en fysisk person ("personoplysninger"). Der er tale om en "personoplysning", når det ud fra de pågældende oplysninger eller i kombination med andre oplysninger er muligt at identificere en fysisk person.³⁰ Man taler således om oplysninger, som er "personhenførbare". En personoplysning kan eksempelvis være oplysninger om en elevs/studerendes navn, adresse, skoleskema, skolebillede, risikoscore m.v. Den, som personoplysningen vedrører, kaldes i den databeskyttelses-retlige terminologi for "den registrerede".

Der skelnes mellem fire kategorier af personoplysninger³¹ :

- 1) Personoplysninger (ikke-følsomme personoplysninger) (såsom navn, adresse, e-mail, telefonnummer etc.)
- 2) Særlige kategorier af personoplysninger (følsomme personoplysninger) (oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data og biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering).
- 3) Oplysninger om strafbare forhold
- 4) Fortrolige personoplysninger (CPR-nummer, økonomiske forhold, karakterer etc.).

Det er i udgangspunktet forbudt at behandle følsomme personoplysninger. Der findes dog en række forskellige undtagelser, som alligevel medfører, at I kan behandle følsomme personoplysninger.³²

Alle registrerede, eksempelvis elever/studerende og medarbejdere, har en række rettigheder efter de databeskyttelsesretlige regler. Det betyder konkret, at når I behandler personoplysninger om fysiske personer – det vil sige, hvis I indsamler, opbevarer, bruger, videregiver og sletter mm. oplysninger om eleverne, de studerende og medarbejderne ved brug af AI-løsningerne – har I pligt til at efterleve de databeskyttelsesretlige regler. Der findes mange forskellige behandlingsformer, og begrebet "behandling" skal derfor forstås i bred forstand.³³ I vil derfor i udgangspunktet behandle personoplysninger, lige så snart I kommer i berøring med oplysninger om elever/de studerende og medarbejdere ved brug af AI-løsningerne.

³⁰ Jf. databeskyttelsesforordningens artikel 4, nr. 1.

³¹ Jf. databeskyttelsesforordningens artikel 6, 9 og 10 samt databeskyttelseslovens § 11.

³² Jf. databeskyttelsesforordningens artikel 9, stk. 2.

³³ Jf. databeskyttelsesforordningens artikel 4, nr. 2.

Det er i den sammenhæng vigtigt at være opmærksom på, hvilken rolle I har i forbindelse med jeres behandling(er) af personoplysninger ved brugen af AI-systemer, idet de databeskyttelsesretlige regler skelner mellem den "dataansvarlige" og "databehandlere".³⁴ Den dataansvarlige er tildelt det største ansvar efter databeskyttelsesretten. For en nærmere beskrivelse af rollerne henvises til trin 2 og afsnit 4.5.2 nedenfor.

Når I behandler personoplysninger, har I pligt til at sikre, at seks grundlæggende principper³⁵ altid er opfyldt:

Grundlæggende princip	Beskrivelse
Princippet om lovlighed, rimelighed og gennemsigtighed	I skal sikre, at behandlingen altid overholder de databeskyttelsesretlige regler, samt at behandlingen foregår på en gennemsigtig måde.
Princippet om formålsbegrænsning	Når I indsamler personoplysninger, skal det fremgå klart, til hvilke saglige formål personoplysningerne skal anvendes. Det indebærer også, at en senere behandling (viderebehandling) af disse personoplysninger <i>ikke</i> må være uforenelig med det oprindelige formål.
Princippet om dataminimering	I skal sikre, at behandlingen, herunder også opbevaringen, er begrænset til det, som er nødvendigt for at opfylde formålet med behandlingen.
Princippet om rigtighed	I skal sikre, at I kun behandler rigtige personoplysninger om de registrerede. Personoplysningerne skal derfor berigtiges, slettes eller anonymiseres, såfremt de er forkerte.
Princippet om opbevaringsbegrænsning	I skal sikre, at I kun opbevarer personoplysninger, så længe dette er nødvendigt til de formål, som personoplysningerne behandles i medfør af. Såfremt det ikke længere er nødvendigt at opbevare personoplysningerne, skal I slette eller (effektivt) anonymisere dem.
Princippet om integritet og fortrolighed	I skal sikre, at personoplysningerne behandles fortroligt. Det indebærer bl.a., at uvedkommende ikke må få indsigt i personoplysningerne, samt at personoplysningerne ikke må gå tabt eller blive beskadiget.

Tabel 2 – Oversigt over de grundlæggende principper i databeskyttelsesforordningen.

For en nærmere beskrivelse af de grundlæggende principper i relation til brugen af AI-systemer, henvises til trin 3 og afsnit 4.5.3. nedenfor.

Før I behandler personoplysninger om eksempelvis eleverne, de studerende og medarbejdere m.fl. i jeres AI-løsninger, skal I sikre jer, at I har et lovligt og gyldigt behandlingsgrundlag (hjemmel) til denne behandling. Der findes i de databeskyttelsesretlige regler flere forskellige lovlige og gyldige behandlingsgrundlag, og de varierer afhængigt af kategorien af personoplysningerne (ikke-følsomme, fortrolige eller følsomme personoplysninger).³⁶

³⁴ Jf. databeskyttelsesforordningens artikel 4, nr. 7 og 8.

³⁵ Jf. databeskyttelsesforordningens artikel 5, stk. 1, litra a-f.

³⁶ Jf. bl.a. databeskyttelsesforordningens artikel 6, 9 og 10 samt databeskyttelseslovens § 8 og § 11.

Et gyldigt og lovligt behandlingsgrundlag kan eksempelvis være, at:

- 1) I har indhentet et gyldigt samtykke fra den, som personoplysningerne vedrører.
- 2) I har behov for at behandle personoplysningerne for at kunne opfylde en aftale (eksempelvis en ansættelseskontrakt), som I har indgået med den, som personoplysningerne vedrører.
- 3) I er forpligtet til at behandle personoplysningerne efter anden lovgivning.
- 4) I udfører en opgave i samfundets interesse eller for en offentlig myndighed.
- 5) I har en særlig interesse i at behandle personoplysningerne, der ikke medfører gener eller konsekvenser for den, som personoplysningerne vedrører.

Det skal understreges, at I altid skal sikre, at I har et lovligt behandlingsgrundlag for hver enkelt behandling, herunder indsamling, videregivelse og anvendelse i nye sammenhænge.

De registrerede, eksempelvis eleverne/de studerende og medarbejderne på uddannelsesinstitutionen, er tildelt en række rettigheder efter de databeskyttelsesretlige regler, som I skal sørge for at efterleve.³⁷ Rettighederne er som følger:

Rettighed	Artikel i databeskyttelsesforordningen
Ret til oplysning (oplysningspligt)	Artikel 13-14
Ret til indsigt (indsigtsret)	Artikel 15
Ret til berigtigelse	Artikel 16
Ret til sletning	Artikel 17
Ret til begrænsning af behandling	Artikel 18
Underretningspligt i forbindelse med berigtigelse, sletning af personoplysninger eller begrænsning af behandling	Artikel 19
Ret til dataportabilitet	Artikel 20
Ret til indsigelse	Artikel 21
Ret til ikke at være genstand for en afgørelse, som alene er baseret på automatisk behandling, herunder profilering.	Artikel 22

Tabel 3 – Oversigt over de registreredes rettigheder i databeskyttelsesforordningen.

I skal være opmærksom på, at oplysningspligten kræver, at I selv tager initiativ til at opfylde oplysningspligten, mens de øvrige rettigheder i artikel 15-21 kun skal iagttages efter anmodning fra de registrerede, jf. nærmere herom afsnit 4.5.5. nedenfor.

³⁷ Der henvises til databeskyttelsesforordningens kapitel III, artikel 12-22.

4.3.1 Risikovurdering ift. databeskyttelse som dataansvarlig

Når I som dataansvarlig behandler personoplysninger, skal I tillige være opmærksomme på, at I har ansvaret for at sikre, at behandlingen foregår på betryggende vis og således med et passende niveau af sikkerhed og beskyttelse.³⁸ De databeskyttelsesretlige regler stiller således særskilte krav til, at I som dataansvarlige forholder jer til risikoen for de registreredes rettigheder og frihedsrettigheder (eksempelvis retten til indsigt, jf. GDPR artikel 15, retten til berigtigelse, jf. GDPR artikel 16 og retten til sletning, jf. GDPR artikel 17), og kan dokumentere de overvejelser og konklusioner, som dette har givet anledning til. De databeskyttelsesretlige regler udgør således en risikobaseret tilgang til behandling af personoplysninger.

Det følger bl.a. af reglerne, at sikkerhedsniveauet for den pågældende behandling skal afspejle den konkrete risiko for, at personoplysningerne eksempelvis bliver stjålet, mistes, beskadiges eller behandles uden et lovligt behandlingsgrundlag. I skal med andre ord indtænke sikkerhed i alle dele af jeres arbejdsprocesser ved anvendelse af AI-løsninger, hvori der sker en behandling af personoplysninger. Det kan eksempelvis være sikkerhed i form af rettighedsstyring, brug af sikkert internet m.v.

Jeres sikkerhedsniveau skal fastlægges ud fra en samlet risikovurdering bestående af:

- Det aktuelle tekniske niveau, f.eks. brugen af end-to-end kryptering. Hvis der behandles følsomme personoplysninger, bør systemet anvende kryptering af høj standard for at sikre, at data ikke kan læses af uautoriserede parter, selv hvis de bliver opsnappet.
- Implementeringsomkostningerne, hvilke kan omfatte omkostninger bestående af både tekniske udgifter (licenser til de forskellige tekniske sikkerhedsløsninger, f.eks. hardware tokens eller en autentifikationsapp) samt tidsforbruget til implementering og oplæring af medarbejdere.
- Den pågældende behandlings karakter, omfang, sammenhæng og formål samt
- Risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

En tommelfingerregel er, at jo flere følsomme personoplysninger I behandler, jo større vil beskyttelsesbehovet af personoplysningerne i udgangspunktet være. Det skal understreges, at risikovurderingen udelukkende omhandler risici for fysiske personers rettigheder og frihedsrettigheder, og således ikke risici for eksempelvis uddannelsesinstitutionens omdømme mv.

Når sikkerhedsniveauet er fastlagt, skal I som dataansvarlig implementere tekniske foranstaltninger, det vil sige foranstaltninger indarbejdet direkte i AI-systemet. I skal også implementere organisatoriske foranstaltninger, det vil sige eksempelvis retningslinjer for medarbejderne om brugen af AI-løsningen på en sikker måde. De tekniske og organisatoriske

³⁸ Der henvises til databeskyttelsesforordningens artikel 32.

foranstaltninger skal sikre et sikkerhedsniveau, der kan imødegå de risici, I har identificeret i forbindelse med risikovurderingen. For en nærmere beskrivelse af reglerne om behandlingssikkerhed i relation til AI-systemer henvises til trin 4 og afsnit 4.5.4 nedenfor.

De databeskyttelsesretlige regler stiller endvidere krav om, at I som dataansvarlig forud for iværksættelsen af en behandling gennemfører en konsekvensanalyse vedrørende databeskyttelse (en såkaldt "DPIA" efter det engelske "data protection impact assessment"), hvis I i forbindelse med jeres risikovurdering konkluderer, at jeres behandling af personoplysninger sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.³⁹ En DPIA er særlig relevant, når I ønsker at behandle personoplysninger ved brug af ny teknologi.⁴⁰ Det er Datatilsynets opfattelse, at AI skal anses som "ny teknologi", samt at risikoen for fysiske personers rettigheder og frihedsrettigheder normalt vil være høj ved udvikling og brug af AI-løsninger.⁴¹

Kort sagt er en DPIA en analyse, som grundlæggende har til formål, at:

- 1) Beskrive den konkrete behandling af personoplysninger,
- 2) Vurdere behandlingens nødvendighed og proportionalitet samt
- 3) Bidrage til at håndtere de risici for fysiske personers rettigheder og frihedsrettigheder, som vil være forbundet med behandlingen.⁴²

Foruden kravet om behandlingssikkerhed, skal I være opmærksomme på, at der efter de databeskyttelsesretlige regler gælder en række krav, hvis jeres behandling af personoplysninger indebærer, at personoplysningerne overføres til et (usikkert) tredjeland eller en international organisation uden for EU/EØS.⁴³ Ved en overførsel forstås, at I (som dataeksportør) videregiver eller på anden måde stiller personoplysninger til rådighed for personer/virksomheder (dataimportøren), der befinder sig i et land uden for EU/EØS.⁴⁴ I har som dataansvarlig derfor pligt til – inden I påbegynder en behandling af personoplysninger – at kortlægge, om der i forbindelse med jeres behandling af personoplysninger sker en overførsel af disse oplysninger til et tredjeland/international organisation, samt hvilket tredjeland der er tale om.

Hvis I konkluderer, at der sker en overførsel til et tredjeland/international organisation, skal I herefter vurdere, om denne overførsel lovligt kan finde sted efter de databeskyttelsesretlige regler, det vil sige, at I skal have et såkaldt overførselsgrundlag.⁴⁵ Det indebærer også, at I skal fastlægge, om oplysningerne overføres til et sikkert eller et usikkert tredjeland, da overførselsgrundlaget afhænger heraf.⁴⁶ Såfremt I konkluderer, at overførslen vil ske til et usikkert tredjeland, har I som dataansvarlig pligt til at udarbejde en såkaldt "Transfer Impact Assessment" ("TIA"), der indeholder jeres kortlægning af overførslerne samt jeres vurdering af

³⁹ Jf. databeskyttelsesforordningens artikel 35.

⁴⁰ Artikel 29-gruppens [retningslinjer](#) for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679, WP248, side 9.

⁴¹ [Offentlige myndigheders brug af kunstig intelligens: Inden I går i gang \(Datatilsynet.dk\)](#), side 36-37.

⁴² [Offentlige myndigheders brug af kunstig intelligens: Inden I går i gang \(Datatilsynet.dk\)](#), side 36.

⁴³ Jf. databeskyttelsesforordningens kapitel V.

⁴⁴ Jf. Datatilsynets [vejledning](#) om overførsel af personoplysninger til tredjelande, side 6.

⁴⁵ Jf. databeskyttelsesforordningens kapitel V.

⁴⁶ Jf. Datatilsynets [hjemmeside](#), som indeholder en oversigt over sikre tredjelande/organisationer.

lovligheden af disse overførsler.⁴⁷ AI-løsninger leveret af store internationale cloudleverandører vil ofte indebære overførsler til tredjelande.

4.4 Databeskyttelse i et AI-system

Endelig indeholder de databeskyttelsesretlige regler tillige krav om, at I (som dataansvarlig) skal indtænke databeskyttelse gennem design og standardindstillinger i jeres systemer, herunder AI-systemer.⁴⁸ Der er tale om et krav, som både relaterer sig til selve udviklingen og den efterfølgende drift af AI-systemerne. Og kravet gælder også i forhold til jeres køb og brug af standardløsninger fra en leverandør.

Databeskyttelse gennem design og standardindstillinger betyder med andre ord, at databeskyttelsesreglerne allerede skal indtænkes fra start, når I skal designe, indrette, udvikle, indkøbe eller tilpasse jeres AI-systemer. Det indebærer eksempelvis, at AI-systemet fra starten skal designes og indrettes således, at systemet automatisk sletter personoplysninger efter et forudbestemt tidsrum. I skal således sikre, at når I som dataansvarlig anvender et AI-system til at behandle personoplysninger, skal de indstillingsmuligheder, som systemet indeholder, som standard være indstillet på en måde, som understøtter reglerne i databeskyttelsesforordningen, herunder om formålsbegrænsning og dataminimering.

Databeskyttelse gennem design og standardindstillinger omfatter derfor både tekniske foranstaltninger (altså foranstaltninger indbygget direkte i AI-systemet) og organisatoriske foranstaltninger (altså de almindelige forretningsgange, der understøtter databeskyttelse). For en nærmere beskrivelse af reglerne om databeskyttelse gennem design og standardindstillinger i relation til AI-systemer, henvises til trin 3 og afsnit 4.5.3 nedenfor.

4.5 De 7 trin

De følgende afsnit 4.5.1.-4.5.7. er opbygget i syv trin, og indeholder konkrete anbefalinger til jeres brug af AI-systemer med afsæt i databeskyttelsesforordningen og AI-forordningen, herunder hvilke forpligtelser I har.

- Trin 1: Kortlæg jeres AI-løsninger, deres risikoniveau og behandlinger af personoplysninger (afsnit 4.5.1.)
- Trin 2: Kortlæg jeres rolle i forhold til AI-systemerne (afsnit 4.5.2.)
 - Jeres rolle i forhold til databehandlingen (afsnit 4.5.2.1.)
 - Jeres rolle i forhold til AI-forordningen (afsnit 4.5.2.2.)
- Trin 3: Vurdér lovligheden af AI-systemerne (afsnit 4.5.3.)
 - Lovlighed efter AI-forordningen (afsnit 4.5.3.1.)
 - Lovlighed ud fra principperne for behandling af personoplysninger (afsnit 4.5.3.2.)
- Trin 4: Vurdér og håndtér risici og sikkerhed (afsnit 4.5.4.)

⁴⁷ I kan læse mere herom i Datatilsynets [vejledning](#) om overførsel af personoplysninger til tredjelande, april 2024, 4. udgave.

⁴⁸ Jf. databeskyttelsesforordningens artikel 25.

- Trin 5: Oplys de registrerede om behandlingen af deres personoplysninger og håndter deres rettigheder (afsnit 4.5.5.)
 - Oplysningspligten efter databeskyttelsesforordningen (afsnit 4.5.5.1.)
 - Gennemsigtighedsforpligtelser efter AI-forordningen (afsnit 4.5.5.2.)
 - Øvrige forpligtelser efter databeskyttelsesforordningen (afsnit 4.5.5.3.)
- Trin 6: Fastsæt centrale politikker og retningslinjer (afsnit 4.5.6.)
- Trin 7: Undervis medarbejderne i AI-færdigheder og jeres politikker og procedurer (afsnit 4.5.7.)

4.5.1 Trin 1: Kortlæg jeres AI-løsninger, deres risikoniveau og behandlinger af personoplysninger

Reglerne i AI-forordningen finder anvendelse på AI-systemer,⁴⁹ og det er derfor vigtigt, at I som det første kortlægger jeres AI-løsninger, herunder hvad der er AI, og hvad der ikke er AI.

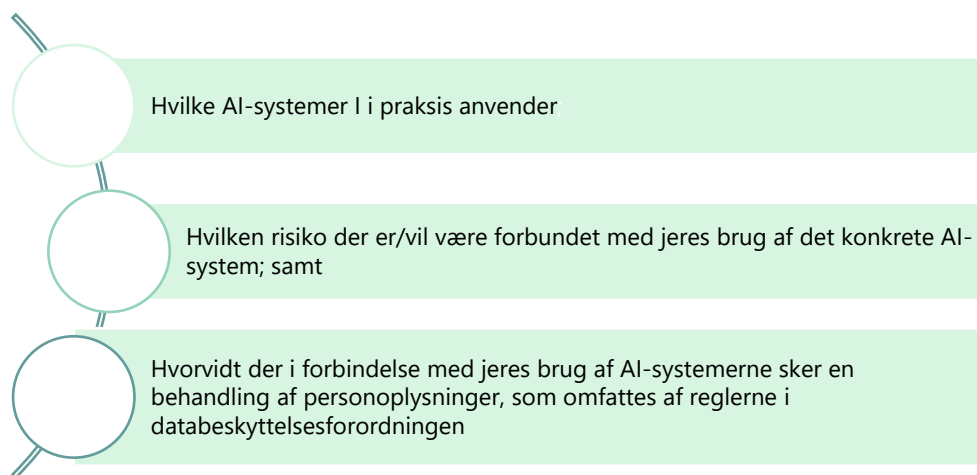
AI-systemer adskiller sig fra de enklere traditionelle softwaresystemer eller programmeringstilgange og omfatter ikke systemer, der er baseret på de regler, der udelukkende er defineret af fysiske personer til automatisk at udføre operationer, se eksempler herpå i afsnit 3.1. En central egenskab ved AI-systemer er derimod deres evne til at udlede fra det input, de modtager, hvordan de kan generere output såsom forudsigelser, indhold, anbefalinger eller beslutninger.

De teknikker, der muliggør denne evne til at udlede i et AI-system, omfatter maskinlæringstilgange, hvor systemet af data lærer, hvordan bestemte mål kan nås, og logik- og videnbaserede tilgange, der udleder indhold fra indkodet viden eller symbolsk repræsentation af den opgave, der skal løses. Et AI-systems evne til at udlede går derfor videre end grundlæggende databehandling ved at muliggøre læring, ræsonnement eller modellering.⁵⁰

Det er derfor afgørende, at I kortlægger, hvilke AI-systemer der udgør en del af jeres systemlandskab. Dette særligt med henblik på, at I kan få et ajourført overblik over følgende:

⁴⁹ Som "AI-system" forstås: "et maskinbaseret system, som er udformet med henblik på at fungere med en varierende grad af autonomi, og som efter idriftsættelsen kan udvise en tilpasningsevne, og som til eksplicitte eller implicitte mål af det input, det modtager, udleder, hvordan det kan generere output såsom forudsigelser, indhold, anbefalinger eller beslutninger, som kan påvirke fysiske eller virtuelle miljøer", jf. AI-forordningens artikel 3, nr. 1.

⁵⁰ Jf. AI-forordningens præambelbetragtning nr. 12.



Figur 1 – Overblik over centrale spørgsmål i forbindelse med jeres kortlægning. (kilde Kammeradvokaten)

Hovedreglen er således, som nævnt i afsnit 4.3, at databeskyttelsesforordningen finder anvendelse på al elektronisk behandling af personoplysninger.⁵¹ Det indebærer, at reglerne i databeskyttelsesforordningen vil finde anvendelse, når I designer, udvikler, herunder træner, idriftsætter, vedligeholder og opdaterer et AI-system, hvis der i forbindelse med disse aktiviteter sker en behandling af personoplysninger. I skal således være opmærksomme på, at databeskyttelsesforordningen vil finde anvendelse, hvis der eksempelvis i jeres inputdata via prompts og i AI-systemets outputdata fremgår personoplysninger om eleverne/de studerende eller ansatte.

4.5.1.1 Praktisk tilgang til kortlægning af jeres AI-løsninger

Det fremgår ikke direkte af AI-forordningen, hvordan I i praksis skal foretage denne kortlægning og få et overblik over jeres AI-systemer.

I jeres kortlægningsarbejde kan I med fordel tage udgangspunkt i tabellen i Bilag B. Tabellen består af en række indledende og centrale spørgsmål vedrørende jeres anvendelse af AI-systemer. I skal være opmærksomme på, at såfremt jeres systemlandskab består af flere forskellige AI-systemer, skal jeres udfyldning af nedenstående tabel afspejle alle AI-systemerne.

Endelig bemærkes det, at tabellen er udbygget således, at den også består af temaer, der tager afsæt i de efterfølgende trin i afsnit 4.5.2.-4.5.7. nedenfor.

I bør holde jeres kortlægninger regelmæssigt opdateret, således at I har et ajourført overblik over, hvilke AI-systemer der er en del af jeres systemlandskab samt behandlingen af personoplysninger heri. Dette med henblik på, at I kan dokumentere jeres anvendelse af AI-systemer og efterlevelsen af de krav, som følger af AI-forordningen og databeskyttelsesforordningen over for de danske tilsynsmyndigheder, herunder Datatilsynet og Digitaliseringsstyrelsen.

⁵¹ Jf. databeskyttelsesforordningens artikel 1.

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

4.5.2.1 *Jeres rolle i forhold til databehandlingen*

Det er vigtigt, at I har taget stilling til jeres rolle i forhold til databehandlingen. Der er nemlig forskel på de krav, som gælder, afhængig af, om man efter databeskyttelsesforordningen anses for at være dataansvarlig eller databehandler.

Den dataansvarlige vil typisk være den, som bestemmer over databehandlingen.

- Den dataansvarlige bestemmer for eksempel, hvad formålet med databehandlingen er, og hvilke hjælpemidler der skal tages i brug.
- En dataansvarlig kan instruere en anden part til at behandle oplysningerne på den dataansvarliges vegne – denne anden part kaldes for databehandler.

I langt de fleste tilfælde vil en uddannelsesinstitution være dataansvarlig, når databehandlingen sker til uddannelsesinstitutionens formål og til brug for at udføre de opgaver, som uddannelsesinstitutionen varetager. Et eksempel på dette er, når I behandler personoplysninger for at få et overblik over, hvordan elever er inddelt i klasser, eller hvornår hver enkelt elev skal til eksamen. Hvis I gør brug af en it-leverandør, vil det også være jer, som er dataansvarlige, mens it-leverandøren som udgangspunkt vil være databehandler, da it-løsningen skal anvendes til brug for at udføre de opgaver, som uddannelsesinstitutionen har ansvaret for at varetage, og it-leverandøren i forhold til behandlingen af personoplysninger om elever, lærere, uddannelsesinstitutionernes øvrige ansatte mv. vil handle efter uddannelsesinstitutionens instruks.

Der er også tilfælde, hvor uddannelsesinstitutionen hverken vil være dataansvarlig eller databehandler. Det kan f.eks. være, når en elev af egen drift vælger at downloade og anvende AI-applikationer på sit eget udstyr, f.eks. på elevens egen mobiltelefon, tablet eller computer. I disse tilfælde vil der ikke være tale om behandling af personoplysninger til brug for uddannelsesinstitutionens formål eller ved hjælp af hjælpemidler, som uddannelsesinstitutionen har bestemt, når uddannelsesinstitutionen ikke ejer og har anvist brugen af de pågældende AI-løsninger.

Hvis uddannelsesinstitutionen derimod har udstedt retningslinjer eller på anden vis instrueret eleven i at downloade applikationen – eller hvis uddannelsesinstitutionen stiller udstyr og applikationer til rådighed for en elev og opfordrer denne til at tage det i brug – så vil der ofte være tale om behandling af personoplysninger til brug for uddannelsesinstitutionens formål og ved hjælp af hjælpemidler, som uddannelsesinstitutionen har bestemt. Uddannelsesinstitutionen vil derfor i et sådant tilfælde være data-ansvarlig for behandlingen af personoplysninger.

4.5.2.2 *Jeres rolle i forhold til AI-forordningen*

Det er vigtigt, at I afklarer, om I er idriftsætter eller udbyder af AI-systemer, da omfanget og typen af jeres forpligtelser under AI-forordningen afhænger heraf. Som tidligere nævnt forudsættes det, at I i langt de fleste tilfælde vil fungere som idriftsætter. Dette betyder, at I anvender et standard AI-system, som I har købt af en leverandør (udbyderen).

Vær opmærksom på, at idriftsættere vil blive anset for selv at være udbydere, hvis de markedsfører højrisiko-AI-systemet under eget navn eller tager det i brug, ændrer dets formål eller foretager en væsentlig ændring af systemet.⁵² Se her afsnit 4.6. om egenudvikling af AI-løsninger, hvor kravene til udbydere gennemgås.

4.5.3 Trin 3: Vurdér lovligheden af AI-systemerne

4.5.3.1 Lovlighed efter AI-forordningen

AI-forordningens artikel 5 oplister, hvilke former for AI-praksis der er forbudt, og som en del af undervisningssektoren er der flere elementer, I bør have for øje.

Det er som udgangspunkt forbudt at omsætte, ibrugtage eller anvende AI-systemer, der har et betydeligt potentiale til at manipulere en persons underbevidsthed ved hjælp af subliminale teknikker, eller som udnytter sårbarheder hos specifikke sårbare grupper for væsentligt at forvride deres adfærd på en måde, der sandsynligvis vil forvolde dem eller en anden person psykisk eller fysisk skade. Ved subliminale teknikker forstås teknikker, der formidler et budskab på en skjult måde, så det kun opfattes ubevidst af personen, og dermed er egnet til at påvirke en person udover dennes bevidsthed. Et AI-system, der præsenterer reklamer for uddannelsestilbud eller studieretninger ved hjælp af subliminale beskeder, der påvirker studerendes valg uden deres bevidste samtykke kan herunder i visse tilfælde anses som forbudt under AI-forordningen og er et konkret eksempel på, hvor der bliver benyttet subliminale teknikker.

Følelsesaflæsning af elever i undervisningssammenhæng

Et AI-system, der forsøger at analysere eller aflæse elevers følelsesmæssige tilstande (f.eks. engagement, stress, frustration eller glæde) baseret på ansigtsudtryk, stemmeleje, kropssprog eller biometriske data, er omfattet af forbuddet i artikel 5 i AI-forordningen.

Sådanne systemer vurderes at indebære en høj risiko for indgreb i privatlivets fred og menneskelig værdighed og er derfor ikke tilladt i hverken klasselokalet, eksamenssituationer eller som led i pædagogiske vurderinger. Dette gælder uanset om teknologien bruges til "at støtte undervisningen" eller "forbedre læringsmiljøet".

Eksempel:

Et kamera installeret i et klasseværelse registrerer elevernes ansigtsudtryk og sender data til et AI-system, der estimerer, om den enkelte elev virker motiveret, træt eller uopmærksom. Læreren får herefter anbefalinger til, hvordan undervisningen skal tilpasses. Denne type AI-anvendelse er forbudt.

⁵² Jf. AI-forordningens artikel 25.

Hvad angår kravene til at sikre, at jeres brug af AI-løsninger er lovlige efter AI-forordningen, skal I som idriftsætter af et højrisiko-AI-system være opmærksomme på, at der efter AI-forordningen er en række forpligtelser, I vil skulle overholde⁵³:

1)	Som det første skal I sikre, at AI-systemet anvendes i overensstemmelse med den brugsanvisning, der ledsager systemet.
2)	Dernæst skal I overdrage varetagelsen af det menneskelige tilsyn til de personer, der har den nødvendige kompetence, uddannelse og myndighed samt den nødvendige støtte.
3)	I skal sikre, at inputdataene er relevante og tilstrækkeligt repræsentative ud fra formålet med AI-systemet.
4)	I skal overvåge driften af AI-systemet på grundlag af brugsanvisningen. Hvis I har grund til at tro, at anvendelsen efter brugsanvisningen udgør en risiko, skal I underrette udbyderen eller distributøren og den relevante markedsovervågningsmyndighed.
5)	I skal opbevare de logfiler, der bliver genereret automatisk i AI-systemet, i mindst seks måneder.
6)	Hvis I er arbejdsgiver, informerer I de berørte medarbejdere om, at de vil være omfattet af anvendelsen af et højrisiko-AI-system.
7)	I skal sørge for, at AI-systemet er registreret i en EU-database. ⁵⁴
8)	I skal ofte udarbejde en konsekvensanalyse vedrørende grundlæggende rettigheder for højrisiko-AI-systemer (engelsk: Fundamental Rights Impact Assessment ("FRIA")). ⁵⁵

Tabel 4 – En række af forpligtelserne som skal efterleves, når højrisiko-AI-systemer idriftsættes.

4.5.3.2 Lovlighed ud fra principperne for behandling af personoplysninger

For at sikre, at AI-systemerne er lovlige, skal I som dataansvarlige vurdere, om systemerne lever op til principperne for behandling af personoplysninger.⁵⁶ Det er vigtigt, at beskyttelsen af personoplysninger tænkes ind i processen så tidligt som muligt, således at selve designet af løsningen er udformet med udgangspunkt i databeskyttelse i overensstemmelse med princippet om databeskyttelse igennem design og standardindstillinger, herunder ved screeningen af løsningen i forbindelse med anskaffelse heraf.⁵⁷

Ud fra principperne er det bl.a. relevant at sikre,

- at der altid er et lovligt behandlingsgrundlag (hjemmel)⁵⁸

⁵³ Forpligtelserne fremgår af AI-forordningens artikel 26.

⁵⁴ EU-databasen for højrisiko-AI-systemer, som beskrevet i artikel 71 i EU's AI-forordning, er endnu ikke oprettet. Ifølge artikel 113 træder denne bestemmelse i kraft den 2. august 2026.

⁵⁵ Jf. AI-forordningens artikel 27.

⁵⁶ Jf. databeskyttelsesforordningens artikel 5.

⁵⁷ Jf. databeskyttelsesforordningens artikel 25.

⁵⁸ Et gyldigt retsgrundlag for behandling af personoplysninger kan f.eks. være artikel 6, stk. 1, litra e, i databeskyttelsesforordningen, som ofte bruges af offentlige myndigheder. Det gælder, når myndigheden behandler oplysninger som led i en opgave, der udføres i samfundets interesse eller som led i offentlig myndighedsudøvelse – f.eks. når en gennemfører undervisning af eleverne i henhold til folkeskoleloven etc.

- at behandlingen er rimelig,
- og at der er tilstrækkelig gennemsigtighed om behandlingen i forhold til de personer, hvis oplysninger behandles⁵⁹ samt
- at datakvaliteten af løsningernes output er tilstrækkelig.

Det er således vigtigt at sikre, at behandlingen ikke kan medføre urimelige eller diskriminerende udfald for de personer, der behandles oplysninger om. Dette kan der f.eks. opstå risiko for, hvis AI-systemet er trænet på data, som ikke er tilpas forskelligartet, ikke er egnet til formålet eller afspejler tidligere bias. Det kan også være, at selve opsætningen af systemet fører til urimelige eller diskriminerende udfald, f.eks. hvis systemet er trænet til at lægge vægt på usaglige hensyn eller til at lægge for meget vægt på nogle hensyn på bekostning af andre. Det er også vigtigt, at det er klart for de personer, hvis personoplysninger behandles, hvordan og hvorledes oplysningerne behandles, og at dette kan beskrives i f.eks. en oplysningsskrivelse eller i en databehandlingspolitik.⁶⁰

Hermed nogle konkrete eksempler på de nævnte problematikker i AI-systemer, som I skal være særlig opmærksomme på som dataansvarlig:

⁵⁹ Princippet om gennemsigtighed efter artikel 5, stk. 1, litra a, i databeskyttelsesforordningen indebærer, at personer skal have klar og letforståelig information om, hvordan deres personoplysninger bliver brugt. Dette betyder, at man som dataansvarlig skal informere de registrerede om formålet med behandlingen af deres oplysninger, opbevaring og eventuel videregivelse – f.eks. via en privatlivspolitik, jf. databeskyttelsesforordningens artikel 13 og 14.

⁶⁰ Jf. databeskyttelsesforordningens artikel 13 og 14.

Eksempel på et AI-system, der er trænet på data, som ikke er egnet til formålet:

Et AI-system udvikles til at vurdere ansøgninger til en videregående uddannelse, men systemet er primært trænet på data fra en anden sektor, eksempelvis jobrekruttering. Som følge heraf vægter systemet erfaring fra arbejdsmarkedet meget højt, selvom dette ikke er relevant for adgangskravene til den pågældende uddannelse.

Eksempel på et AI-system, hvor opsætningen af systemet fører til urimelige

udfald: Et AI-baseret system til vurdering af eksamensopgaver viser systematisk lavere karakterer for elever fra bestemte skoler eller geografiske områder, fordi det uforholdsmæssigt lægger vægt på tidligere karaktergennemsnit på skolen snarere end den individuelle præstation i opgaven.

Eksempel på et AI-system, der er trænet til at lægge vægt usaglige hensyn:

Et AI-system bruges til at identificere elever, der kan have behov for ekstra støtte i undervisningen, men det giver forslag til beslutninger baseret på irrelevante faktorer som elevernes fornavne, hvilket utilsigtet kan føre til diskrimination af bestemte etniske grupper.

Eksempel på et AI-system, der er trænet til at lægge vægt på nogle hensyn på

bekostning af andre: En AI-model, der skal bruges som beslutningsstøtte til at vurdere optagelse på en prestigefyldt uddannelse, lægger for meget vægt på matematiske testresultater og undervurderer andre relevante kompetencer såsom kreativitet og samarbejdsevner. Dette kan føre til, at ellers kvalificerede ansøgere fravælges, selvom de besidder vigtige egenskaber for studiet.

Det er også vigtigt at sikre, at personoplysninger alene behandles til udtrykkeligt angivne og legitime formål, og at de ikke behandles (f.eks. indsamles eller opbevares), fordi man tænker, at oplysningerne måske en dag kunne blive nyttige at have. Ligeledes er det vigtigt, at der ikke behandles flere personoplysninger, end hvad der er nødvendigt for at opnå det eller de specifikke formål. Oplysningerne må altså heller ikke opbevares i personhenførbart format i længere tid, end hvad der er nødvendigt.

Det skal også sikres, at personoplysningerne, der behandles i AI-systemerne – herunder deres output – er korrekte. Navnlig ved brug af generativ AI baseret på store sprogmodeller skal man være opmærksom på risikoen for faktisk forkerte svar og såkaldte hallucinationer. Hallucinationer omfatter tilfælde, hvor løsningen genererer forkerte eller opdigtede svar. Det kan bl.a. skyldes, at AI-værktøjets data-grundlag ikke er opdateret eller fyldestgørende på det område, som der spørges til. Det kan være svært at gennemskue, hvorvidt der er tale om opdigtet indhold, da AI-værktøjer er gode til at få det til at fremstå troværdigt.⁶¹

Det er også vigtigt, at personoplysninger behandles på en måde, der sikrer tilstrækkelig sikkerhed for personoplysningerne, således, at oplysningerne ikke kan blive tilgængelige for uautoriserede personer eller blive udsat for ulovlig behandling, tab mv.

⁶¹ Se Digitaliseringsstyrelsens Guide til offentlige myndigheder om ansvarlig anvendelse af generativ kunstig intelligens, 11. marts 2024, s. 5.

Dertil skal det ved behandling af personoplysninger i AI-systemer kunne bevises, at alle de ovennævnte principper er overholdt, hvorfor det anbefales, at vurderingerne om muligt udarbejdes skriftligt og opbevares et sted, hvor de nemt kan tilgås, også i tilfælde af, at de f.eks. skal forelægges for Datatilsynet.

Endelig skal I sikre, at I har hjemmel til at behandle personoplysninger i forbindelse med brug (drift) af AI-systemet. Det følger af Datatilsynets praksis, at brug (drift) af AI-løsninger til behandling af personoplysninger kan skærpe kravene til klarheden af det retsgrundlag, som skal danne baggrund for behandlingen af personoplysningerne i løsningen.

AI-forordningen regulerer ikke spørgsmålet om, hvorvidt offentlige myndigheder, herunder uddannelsesinstitutioner har hjemmel til anvendelsen af AI-systemet eller behandling af personoplysninger forbundet med driften heraf. I skal derfor undersøge og vurdere, om der i jeres særlovgivning på uddannelsesområdet sammenholdt med de generelle bestemmelser i databeskyttelsesforordningen og databeskyttelsesloven⁶² er hjemmel til at behandle personoplysninger i de løsninger, som I anvender.

Databeskyttelsesforordningen indeholder i artikel 6-10 regler om behandling af ikke-følsomme personoplysninger, følsomme personoplysninger samt oplysninger om strafbare forhold. Disse behandlingsregler suppleres af hjemmelsregler i databeskyttelsesloven. Hjemmelskravet gælder principielt for hver enkelt behandlingsform, der skal behandles for sig, herunder indsamling, videregivelse m.v. i forbindelse med drift af AI-systemet.⁶³

⁶² Lovbekendtgørelse nr. 289 af 8. marts 2024 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

⁶³ Jf. herved også Kristian Korfits Nielsen og Anders Lottrup: Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 1. udg., DJØF, 2020, s. 345.

Eksempel: Brug af AI-system til understøttelse af fraværsindsats på en skole

En skole ønsker at anvende et AI-baseret system til at identificere elever med bekymrende fraværsmønstre og forudsige risiko for yderligere fravær. Systemet behandler oplysninger om elevers fremmøde, karakterer, tidligere fravær, eventuelle fritekstkommentarer fra lærere samt oplysninger fra elevplaner.

Der skal foretages en trinvis vurdering af behandlingsgrundlaget for hver behandlingsform:

- **Indsamling af personoplysninger:**

AI-systemet indsamler oplysninger fra skolens eksisterende elevsystemer. Behandlingsgrundlaget for dette kan være databeskyttelsesforordningens artikel 6, stk. 1, litra e (nødvendig for udførelse af en opgave i samfundets interesse/offentlig myndighedsudøvelse), da skolen som offentlig myndighed har til opgave at føre fraværsregistrering og understøtte elevtrivsel. Hvis oplysningerne omfatter følsomme oplysninger (f.eks. helbredsoplysninger i lærernotater), skal der desuden være hjemmel efter artikel 9, stk. 2.

- **Analyse og profilering:**

Når AI-systemet anvender de indsamlede data til at udarbejde en risikovurdering eller "fraværsscore", er der tale om en ny, selvstændig behandlingsform, som kræver et særskilt behandlingsgrundlag. Det skal dokumenteres, hvordan formålet med analysen stemmer overens med skolens lovbestemte opgaver.

- **Videregivelse:**

Hvis systemets resultater deles med f.eks. elevens kontaktlærer, skoleledelsen eller eksterne aktører som kommunen, skal der være et særskilt behandlingsgrundlag for hver form for videregivelse.

- **Opbevaring og sletning:**

Oplysninger, herunder analyseresultater og risikoprofiler, må kun opbevares så længe, det er nødvendigt for formålet. Behandlingsgrundlaget skal dokumenteres også for opbevaringsfasen, og der skal fastsættes slettefrister i overensstemmelse med databeskyttelsesforordningens artikel 5, stk. 1, litra e.

I ovenstående eksempel illustreres det, hvordan hver enkelt behandlingsform (indsamling, analyse, videregivelse mv.) skal have sit eget behandlingsgrundlag i databeskyttelsesforordningen. Det er ikke tilstrækkeligt at have én generel hjemmel – man skal dokumentere hjemmelsgrundlaget for hver fase af databehandlingen.

Behandlingen af ikke-følsomme personoplysninger kan efter databeskyttelsesforordningen ske, hvis et af de seks behandlingsgrundlag i databeskyttelsesforordningens artikel 6 finder

anvendelse.⁶⁴ De forskellige hjemler i bestemmelsen er sidestillede, hvilket betyder, at behandling af personoplysninger lovligt kan ske, hvis blot én ud af de seks behandlingsgrundlag er opfyldt. Det relevante hjemmelsgrundlag at overveje for jer ved "harmløse" behandlinger af personoplysninger ved brug (drift) af AI-løsninger, vil oftest være databeskyttelsesforordningens artikel 6, stk. 1, litra e, om offentlig myndighedsudøvelse, som kan udgøre et selvstændigt hjemmelsgrundlag. For mere indgribende behandlinger skal der derimod være et mere klart hjemmelsgrundlag i national lovgivning til brugen (driften) af AI-løsningen.

Hvis der er tale om en harmløs behandling, vil kravene til behandlingen af oplysninger ikke være særlig store. Denne type behandling indebærer en minimal risiko for de registrerede personer og kan typisk foretages direkte med hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra e (offentlig myndighedsudøvelse), hvis behandlingen sker som led i en offentlig opgave.

Eksempel: AI-system til automatisk sortering af afleverede opgaver

En skole anvender et AI-system, der hjælper lærerne med at sortere og gruppere elevers afleverede opgaver ud fra emne og opgavetype (f.eks. analyse, diskussion, refleksion). Systemet behandler oplysninger som elevens navn, klasse og selve opgaveteksten, men foretager ikke vurdering, karaktergivning eller profilering af eleven.

Formålet er rent administrativt: at understøtte lærerens forberedelse og skabe bedre overblik. Systemet anvendes kun internt og har ingen indflydelse på elevens vurdering eller videre skoleforløb. Da behandlingen sker som led i skolens opgave som offentlig undervisningsinstitution, kan behandlingen af personoplysninger ske med hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra e – behandling nødvendig for udførelse af en opgave i samfundets interesse/offentlig myndighedsudøvelse. Der er ingen behandling af følsomme oplysninger, og der foretages ingen videregivelse eller automatiseret beslutningstagning.

Behandlingen vurderes derfor som harmløs med lav risiko for de registrerede.

Er der derimod tale om en mere indgribende behandling, stilles der større krav til klarheden af lovgrundlaget, f.eks. i national lovgivning, da disse behandlinger indebærer større risici for de registrerede personer, og kan påvirke borgernes rettigheder og friheder i højere grad.

⁶⁴ Jf. databeskyttelsesforordningens artikel 6, stk. 1, litra a-f.

Eksempel: AI-system til automatisk tildeling af specialpædagogisk støtte baseret på elevdata

En kommune ønsker at anvende et AI-system til at analysere data om elevers karakterer, fravær, sociale forhold og historik for støttebehov med det formål at profilere elever og automatisk foreslå tildeling af specialpædagogisk støtte. Systemet genererer en risikoprofil og tildeler elever en støttekategori, hvorefter systemets anbefalinger sendes videre til skoleledelsen.

Systemet foretager profilering, som kan få indflydelse på elevens undervisningstilbud, selvom den endelige beslutning foretages af et menneske (beslutningsstøtte). Der er dermed tale om en behandling, der kan have væsentlige konsekvenser for de registrerede personer.

Da der behandles følsomme oplysninger (artikel 9, f.eks. helbredsoplysninger), og da beslutningerne kan have retlige eller tilsvarende væsentlige konsekvenser for den registrerede, stilles der høje krav til hjemmelsgrundlaget.

Hvis I behandler følsomme personoplysninger, kræver det, at I kan identificere en undtagelse til forbuddet i databeskyttelsesforordningens artikel 9, stk. 1, jf. artikel 9, stk. 2, eller bestemmelser i databeskyttelsesloven, der gennemfører databeskyttelsesforordningens artikel 9. Jeres behandling af følsomme personoplysninger skal, foruden en hjemmel i artikel 9, også have et lovligt grundlag for denne behandling i databeskyttelsesforordningens artikel 6. Det relevante hjemmelsgrundlag for jer at overveje ved drift af en AI-løsning, hvor der behandles følsomme personoplysninger, kan f.eks. være databeskyttelsesforordningens artikel 9, stk. 2, litra f, hvis behandlingen er nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares.

Det er dog vigtigt, at I altid foretager en selvstændig og konkret vurdering af hjemmelsgrundlaget, når I har påtænkt jer at behandle personoplysninger ved drift af en AI-løsning.

Vær endvidere opmærksom på, at AI-løsninger, som I anvender, ofte leveres af store, internationale cloudleverandører. Det er her vigtigt at læse vilkårene grundigt for, hvad disse leverandører bruger jeres personoplysninger til. F.eks. er det vigtigt at kontrollere, om cloudleverandøren behandler jeres personoplysninger om de studerende til cloudleverandørens egne formål i form af produktudvikling, herunder træning af nye løsninger, markedsføring m.v. Der vil normalt ikke være hjemmel til, at I videregiver personoplysninger om de studerende til cloudleverandøren på denne måde.

4.5.4 Trin 4: Vurdér og håndtér risici og sikkerhed

Som anført ovenfor i trin 3 (afsnit 4.5.3), skal I være opmærksomme på, at jeres AI-system ikke har en uacceptabel risiko og dermed er forbudt efter AI-forordningen. Ligeledes skal I være opmærksomme på, hvorvidt AI-systemet er højrisiko, da I i så fald vil ifalde særskilte forpligtelser efter AI-forordningen.

Som anført i afsnit 4.2 omfatter højrisiko-AI-systemer også andre selvstændige AI-systemer – uafhængige af et produkt – hvor systemet er omfattet af en eller flere af de kritiske områder eller use cases som angivet i AI-forordningens bilag III.⁶⁵

Af bilag III til AI-forordningen fremgår bl.a. kategorien "Uddannelse og erhvervsuddannelse". AI-systemer, der anvendes inden for uddannelse eller erhvervsuddannelse, navnlig til at:

- bestemme adgang eller optagelse,
- fordele personer på uddannelsesinstitutioner eller uddannelser på alle niveauer,
- evaluere personers læringsudbytte,
- bedømme en persons nødvendige uddannelsesniveau og væsentligt påvirke den uddannelse, som den pågældende person vil modtage eller vil kunne få adgang til, eller
- overvåge og opdage forbudt adfærd bl.a. studerende under prøver,

Disse ovennævnte eksempler på AI-systemer er klassificeret som højrisiko-AI-systemer, da de kan afgøre en persons uddannelsesmæssige og arbejdsmæssige livsforløb og dermed kan påvirke denne persons mulighed for at sikre sig et livsgrundlag.⁶⁶

AI-forordningen definerer ikke lavrisiko-AI-systemer. Lavrisiko-AI-systemer omfatter derfor de systemer, der ikke er omfattet af de andre kategorier. Disse systemer kan I derfor anvende frit, men der er mulighed for, at I kan underlægge jer krav frivilligt gennem adfærdscodekser.

De centrale risici for fysiske personer ved brug af AI-systemer, som I skal være opmærksomme på, vil ofte være risici forbundet med at være "udsat" for kunstig intelligens, hvor dette kan medføre negative konsekvenser for personen. Det kan f.eks. være tilfældet, når AI-systemer er trænet på utilstrækkelige datasæt eller data, som er uegnet til formålet, eller som er påvirket af bias, således at personer kan blive udsat for unøjagtige eller urimelige afgørelser, hvis der ikke sker tilstrækkelig menneskeligt review.

Manglende gennemsigtighed eller mulighed for at forklare AI-løsningens output kan også udgøre en risiko for fysiske personer, da det kan føre til, at de registrerede ikke forstår, hvordan deres oplysninger behandles, hvordan AI-løsningen kan påvirke personerne, og hvordan personerne kan udøve deres rettigheder som registrerede. Desuden kan der være risici for manglende fortrolighed og integritet i forhold til behandlingen af personoplysninger, hvis der på grund af manglende sikkerhed f.eks. lækkes fortrolige eller private personoplysninger.

4.5.4.1 Konsekvensanalyse vedrørende databeskyttelse (DPIA)

Det er derfor væsentligt, at I forud for ibrugtagning af AI-systemet danner jer et overblik over samtlige af systemets risici for fysiske personer, og vurderer disse. I skal bl.a. vurdere, om der skal udarbejdes en konsekvensanalyse vedrørende databeskyttelse (DPIA), jf. afsnit 4.3.1. og 4.5.4.1.⁶⁷

⁶⁵ Jf. AI-forordningens artikel 6, stk. 2.

⁶⁶ Jf. AI-forordningens præambelbetragtning nr. 56.

⁶⁷ Jf. databeskyttelsesforordningens artikel 35.

Det følger af databeskyttelsesforordningen, at pligten til at fastsætte foranstaltninger, som kan nedbringe identificerede risici, skal ses i relation til de specifikke, identificerede risici ved behandlingen af personoplysninger. Det betyder, at jo større risici, en behandling forventes at indebære, des højere er kravet til fastsættelse af foranstaltninger, som kan imødegå de identificerede risici. Når det kommer til behandling af personoplysninger i AI-systemer, vil der næsten altid være et vist niveau af risiko for de registrerede på grund af den komplekse måde, som AI-systemer behandler data på, og derfor vil der også ofte være pligt til, at der skal udarbejdes en DPIA.

4.5.4.2 Konsekvensanalyse vedrørende grundlæggende rettigheder (FRIA)

Som idriftsætter af et højrisiko-AI-system, skal I ligeledes efter AI-forordningen ofte foretage en konsekvensanalyse vedrørende grundlæggende rettigheder, som anvendelsen af systemet kan medføre, også kaldet FRIA (fra engelsk "Fundamental Rights Impact Assessment").⁶⁸

Denne konsekvensanalyse skal bestå af:

- En beskrivelse af de processer, hvor højrisiko-AI-systemet vil blive anvendt i overensstemmelse med dets tilsigtede formål.
- En beskrivelse af den periode og hyppighed, hvor højrisiko-AI-systemet tilsigtes anvendt.
- De kategorier af fysiske personer og grupper, som forventes at blive påvirket af højrisiko-AI-systemets anvendelse i den specifikke kontekst, herunder de specifikke risici for skade, der sandsynligvis vil påvirke de kategorier af fysiske personer eller grupper af personer, som er identificeret.
- En beskrivelse af gennemførelsen af foranstaltninger til menneskeligt tilsyn i overensstemmelse med brugsanvisningen.
- De foranstaltninger, der skal træffes, hvis disse risici opstår, herunder ordningerne for intern ledelse og klagemekanismer.

4.5.4.3 Risikovurdering af behandlingssikkerheden efter databeskyttelsesforordningens artikel 32

Som beskrevet under afsnit 4.2, skal I være opmærksomme på, at de databeskyttelsesretlige regler generelt udgør en risikobaseret tilgang til databeskyttelse.

Det betyder med andre ord, at I i forbindelse med behandling af personoplysninger ved brug af et AI-system, har pligt til at foretage en risikovurdering. Det vil sige en kortlægning af de risici for de registreredes rettigheder og frihedsrettigheder, som vil være forbundet med den konkrete behandling, hvor der anvendes et AI-system. Herefter skal I foretage en afvejning af disse risici i forhold til de foranstaltninger, der bør træffes for at beskytte disse rettigheder, jf. databeskyttelsesforordningens artikel 32. En risiko for de registrerede kan eksempelvis være identitetstyveri, og en passende (teknisk) foranstaltning for at imødegå denne risici kan være kryptering af den kommunikation, der indeholder personoplysninger.

Risikovurderingen består således af flere dele:

⁶⁸ Jf. AI-forordningens artikel 27.

- 1) en kortlægning og identifikation af alle de risici, som behandlingen vil medføre, og en kategorisering af disse risici (scoring, sandsynlighed og alvorlighed) samt
- 2) identifikation og en vurdering af, hvilke passende tekniske og organisatoriske foranstaltninger der bør implementeres med henblik på at imødegå de kortlagte risici og sikre, at de databeskyttelsesretlige regler overholdes, og at dette kan dokumenteres.

Kort sagt skal jeres risikovurdering danne grundlag for, at I på forhånd kan vurdere, hvor godt I skal passe på de registreredes personoplysninger, der behandles i forbindelse med udvikling, drift og anvendelse af et konkret AI-system. En tommelfingerregel er, at jo mere følsomme personoplysninger, der vil blive behandlet i AI-systemet, desto strengere krav bør der i udgangspunktet stilles til beskyttelsen af personoplysningerne og dermed jeres sikkerhedsniveau. Hvis forskellige kategorier af personoplysninger behandles i AI-systemet, skal I indrette jeres sikkerhedsforanstaltninger efter de mest følsomme personoplysninger.

Der er tale om en konkret vurdering i forhold til, hvilket sikkerhedsniveau der vil være passende for den pågældende behandling, idet de databeskyttelsesretlige regler ikke indeholder konkrete retningslinjer herfor. Det er den dataansvarlige, som beslutter, hvilke tekniske og organisatoriske foranstaltninger der vil være passende for at imødegå de identificerede risici.

Tekniske foranstaltninger er foranstaltninger, som er indarbejdet direkte i AI-systemet, og kan eksempelvis være kryptering, logning, løbende opdateringer og vedligeholdelse af systemet, adgangskontrol baseret på to-faktor-godkendelse, firewalls mm. Organisatoriske foranstaltninger er alle andre former for foranstaltninger, som ikke er tekniske, og kan eksempelvis være træning af medarbejdere, løbende awareness, politikker og vejledning mm.⁶⁹

I bør derfor også med løbende mellemrum (gen)overveje behandlingssikkerheden, da risikobilledet for de registreredes rettigheder og frihedsrettigheder kan ændres, bl.a. som følge af trusler fra omverdenen eller ændringer i jeres organisation. Det er derfor ikke tilstrækkeligt, at I kun foretager en risikovurdering ved behandlingens påbegyndelse.

Hvis I, efter at have foretaget en risikovurdering af behandlingssikkerheden, konkluderer, at der sandsynligvis er en høj risiko for de registreredes rettigheder og frihedsrettigheder, skal I være opmærksomme på, at I efter databeskyttelsesforordningens artikel 35 er forpligtet til at udarbejde en DPIA, jf. afsnit 4.3.1. og 4.5.4.1.

4.5.4.4 Krav til udbyderens sikkerhed

Under AI-forordningen vil I ligeledes have en pligt til at have styr på sikkerheden. Hvis I er udbyder, skal I sikre, at AI-systemet er udviklet på en sådan måde, at det opnår et passende niveau af nøjagtighed, robusthed og cybersikkerhed, og at dette er konsekvent i hele AI-systemets livscyklus.⁷⁰ Dette indebærer at:

⁶⁹ Der henvises til Datatilsynets [vejledning](#) om behandlingssikkerhed samt databeskyttelse gennem design og standardindstillinger, juni 2018, side 12.

⁷⁰ AI-forordningens artikel 15.

- Niveauet og relevante parametre med hensyn til nøjagtighed skal angives i den ledsagende brugsanvisning.
- AI-systemet er modstandsdygtig over for fejl, svigt og uoverensstemmelser, der kan forekomme i systemet eller i det miljø, som systemet fungerer i, navnlig på grund af systemets interaktion med fysiske personer eller andre systemer. Dette kan opnås ved hjælp af tekniske redundans, som kan omfatte backupplaner eller fejlsikre planer.
- AI-systemer skal være modstandsdygtige over for uautoriserede tredjeparters forsøg på at ændre deres anvendelse, output eller ydeevne ved at udnytte systemsårbarheder. I kan indføre tekniske systemer til afhjælpning af AI-systemets sårbarheder, f.eks. foranstaltninger til forebyggelse og kontrol af angreb, der forsøger at manipulere træningsdatasættet ("data-forgiftning"), input, der har til formål at få modellen til at begå fejl ("fjendtlige eksempler"), eller modelfejl.

Ovenstående sikkerhedsmæssige tiltag skal være med til at sikre, at I på forhånd har forberedt jer mod alle de (kendte) sikkerhedsmæssige risici, dvs. trusler, som der vil være forbundet med jeres brug af AI. I skal generelt være opmærksomme på, at truslerne både kan være interne og eksterne. De største (kendte) sikkerhedsmæssige trusler ved brugen af AI er bl.a.:

1) Risikoen for forgiftning af data (fra engelsk "data poisoning"):

Der er således en risiko for, at interne eller eksterne aktører ændrer data med henblik på at manipulere outputtet. Sådanne ændringer kan bl.a. ske ved at der ændres direkte i træningsdata (af interne eller eksterne aktører) eller, hvis algoritmen er selvlærende, ved at sende den en stor mængde af inputdata af en bestemt art. Et eksempel herpå er Microsofts chatbot Tay, hvor twitter-brugere på under et døgn "lære" Tay at skrive vulgært om ømtålelige emner på twitter.

2) Risikoen for manipulation af data (fra engelsk "adversarial attacks"):

Her er der tale om, at interne eller eksterne aktører, typisk uden egentlig adgang til algoritmen, bevidst sender inputdata til modellen, som indeholder en marginal ændring (f.eks. ændring af én pixel i et billede eller ændre bølgelængden på tale) med henblik på at "snyde" modellen til at opnå et ønsket resultat.

3) Risikoen for såkaldt "bagdørsangreb" (fra engelsk "backdoor attack"):

Her er der tale om, at interne eller eksterne aktører får adgang til algoritmens produktionskode og ændrer denne (implementerer en bagdør) for at muliggøre et ønsket udfald ved en atypisk eller teoretisk umulig kombination af input variable.

4) Risikoen for såkaldt dataekstraktion (fra engelsk "data extraction"):

Her er der tale om, at interne eller eksterne aktører benytter information fra output til ét af to formål; 1) at bygge en surrogat/kopi af modellen eller 2) at forstå bias i modellen. Ved førstnævnte kan den nye model f.eks. sælges, bruges til at underbyde på markedet, eller til at rekonstruere træningsdata. Ved sidstnævnte kan identifikation af bias gøre det muligt at identificere kombinationer af inputdata, som resulterer i et ønsket udfald (også benævnt impersonation), hvilket bl.a. kan bruges i "adversarial attacks".

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

4.5.5.1 Oplysningspligten efter databeskyttelsesforordningen

Når I indkøber, udvikler eller anvender et AI-system, hvori der vil ske en behandling af personoplysninger, og hvor I er dataansvarlige, er det klare udgangspunkt, at I på eget initiativ har pligt til at informere eleverne/de studerende m.fl. (de registrerede) om, at I indsamler personoplysninger om dem.⁷¹ Udover at informere dem om, at I behandler personoplysninger om dem, skal I også give en række yderligere informationer, bl.a. om hvad I skal bruge personoplysningerne til, og hvor længe I planlægger at gemme personoplysningerne.

Hvis I får personoplysningerne fra eleven/den studerende m.fl. selv, skal I give informationerne på det tidspunkt, hvor I modtager personoplysningerne fra vedkommende. Hvis I derimod får personoplysningerne fra andre end eleven/den studerende m.fl. selv, eksempelvis fra offentlige

⁷¹ Jf. databeskyttelsesforordningens artikel 13-14.

myndigheder, skal I give informationerne til eleven/den studerende m.fl. hurtigst muligt og senest én måned efter, at I har modtaget personoplysningerne om vedkommende.⁷²

I skal give informationerne på en måde, som er letforståelig for eleven/den studerende m.fl.⁷³ Informationerne kan med fordel gives i en databeskyttelsespolitik, som I kan linke til. I skal dog være opmærksomme på, at det er jer som dataansvarlig, der har pligt til at tage aktive skridt med henblik på at informere eleven/de studerende m.fl. om behandlingen, og det er derfor ikke tilstrækkeligt, at I blot henviser eleven/den studerende m.fl. til uddannelsesinstitutionens hjemmeside.

Hvilke konkrete informationer I skal give til eleverne/de studerende m.fl. afhænger af, hvem personoplysningerne er indsamlet hos.

Hvis I har indsamlet personoplysningerne om eleven/den studerende hos vedkommende selv, giver I som dataansvarlig på det tidspunkt, hvor I indsamler personoplysningerne, eleven/den studerende m.fl. en række informationer, såsom identiteten og kontaktoplysningerne på den, der indsamler personoplysningerne, og på en eventuel udpeget databeskyttelsesrådgiver (DPO), formålene med og grundlaget for behandlingen (hjemlen), eventuelle modtagere af personoplysningerne mv. De konkrete informationer fremgår udtrykkeligt af databeskyttelsesforordningens artikel 13, stk. 1-2, hvorfor der henvises hertil.

Hvis I har indsamlet personoplysningerne om eleven/den studerende m.fl. hos andre end den pågældende selv, skal I som dataansvarlig give de samme informationer, som når personoplysningerne er indsamlet hos eleven/den studerende m.fl. selv. Derudover skal I også oplyse eleven/den studerende m.fl. om de berørte kategorier af personoplysninger, det vil sige, hvorvidt de indsamlede personoplysninger er almindelige, fortrolige og/eller følsomme. De konkrete informationer, som I skal give, fremgår udtrykkeligt af databeskyttelsesforordningens artikel 14, stk. 1-2, hvorfor der henvises hertil.

Det skal understreges, at såfremt I anvender en AI-løsning, som indebærer, at der træffes automatiske, individuelle afgørelser, herunder profilering, der har en retsvirkning eller betydeligt påvirker eleven/den studerende m.fl., har I pligt til at informere eleven/den studerende m.fl. om dette samt om betydningen heraf og de forventede konsekvenser for eleven/den studerende m.fl., der vil være forbundet med denne behandling.⁷⁴ Denne information skal som minimum indeholde meningsfulde oplysninger om logikken bag AI-systemet. Dette særligt med henblik på at sikre, at eleven/den studerende m.fl. sættes i stand til at udøve deres rettigheder. For en nærmere beskrivelse af rettighederne, se umiddelbart nedenfor.

Hvis jeres AI-løsning indebærer, at I foretager profilering af den registrerede – uden at der er tale om en egentlig automatisk, individuel afgørelse – vil I endvidere skulle informere den registrerede om tilstedeværelsen af profileringen og konsekvenserne heraf.⁷⁵

⁷² Jf. databeskyttelsesforordningens artikel 12, stk. 1.

⁷³ Jf. databeskyttelsesforordningens artikel 12, stk. 1.

⁷⁴ Jf. databeskyttelsesforordningens artikel 13, stk. 2, litra f, artikel 14, stk. 2, litra g, og præambelbetragtning nr. 60.

⁷⁵ Se præambelbetragtning 60 til databeskyttelsesforordningen.

Såfremt I har indsamlet personoplysningerne direkte hos eleven/den studerende selv m.fl., bør I også informere vedkommende om, hvorvidt eleven/den studerende faktisk er forpligtet til at dele sine personoplysninger med jer, herunder hvad konsekvenserne vil være, hvis eleven/den studerende m.fl. ikke vil dele sine personoplysninger med jer.

Der findes imidlertid en række undtagelser til oplysningspligten. Eksempelvis har I som dataansvarlig ikke pligt til at give eleverne/de studerende m.fl. informationerne, hvis de allerede er bekendt med de informationer, som I er forpligtet til at give. Undtagelsens anvendelighed afhænger af, hvilke informationer I har givet eleven/den studerende m.fl. i forbindelse med den oprindelige indsamling af deres personoplysninger. Det er således afgørende, at eleven/den studerende m.fl. på indsamlingstidspunktet blev oplyst om, at vedkommendes personoplysninger vil blive behandlet i forbindelse med brugen af et AI-system. Hvis det ikke er tilfældet, kan undtagelsen ikke anvendes, og I har derfor pligt til at informere på ny. Undtagelserne til oplysningspligten kan findes i databeskyttelsesforordningens artikel 13, stk. 4, og artikel 14, stk. 5, samt databeskyttelseslovens §§ 22-23. I kan også læse mere om disse i Datatilsynets vejledning om de registreredes rettigheder, jf. også kapitel 5 nedenfor.

4.5.5.2 Gennemsigthedsforpligtelser efter AI-forordningen

AI-forordningen indeholder ligeledes forskellige forpligtelser til at underrette elever, studerende m.fl. om, at de interagerer med et AI-system.

Hvis I er idriftsætter af et af de i AI-forordningens bilag III omhandlede højrisiko-AI-systemer, der træffer beslutninger eller bistår med at træffe beslutninger vedrørende fysiske personer, skal I underrette de fysiske personer om, at de er genstand for anvendelsen af et højrisiko-AI-system.⁷⁶

Ligeledes skal udbydere sikre, at AI-systemer, der er beregnet til at interagere direkte med fysiske personer, udformes og udvikles på en sådan måde, at fysiske personer oplyses om, at de interagerer med et AI-system, medmindre dette er indlysende ud fra omstændighederne og anvendelsessammenhængen. Udbydere af AI-systemer, der genererer syntetisk lyd, billede, video eller tekst, skal ligeledes sikre, at outputtet er markeret med et maskinlæsbart format og kan spores som kunstigt genereret eller manipuleret.⁷⁷

Hvis I er idriftsætter af et AI-system til følelsesgenkendelse, skal I underrette de fysiske personer, der udsættes herfor, om driften af systemet. Ligeledes, hvis I er idriftsætter af et AI-system, der genererer eller manipulerer billed-, lyd- eller videoindhold, der i væsentlig grad ligner faktiske personer, genstande, steder eller andre enheder eller begivenheder, og som fejlagtigt vil fremstå ægte eller sandfærdigt ("deepfake"), skal I oplyse, at indholdet er blevet genereret kunstigt eller manipuleret.⁷⁸

4.5.5.3 Øvrige forpligtelser efter databeskyttelsesforordningen

Foruden jeres pligt til efter databeskyttelsesforordningen på eget initiativ at give eleverne/de studerende m.fl. en række informationer, når I behandler personoplysninger om dem

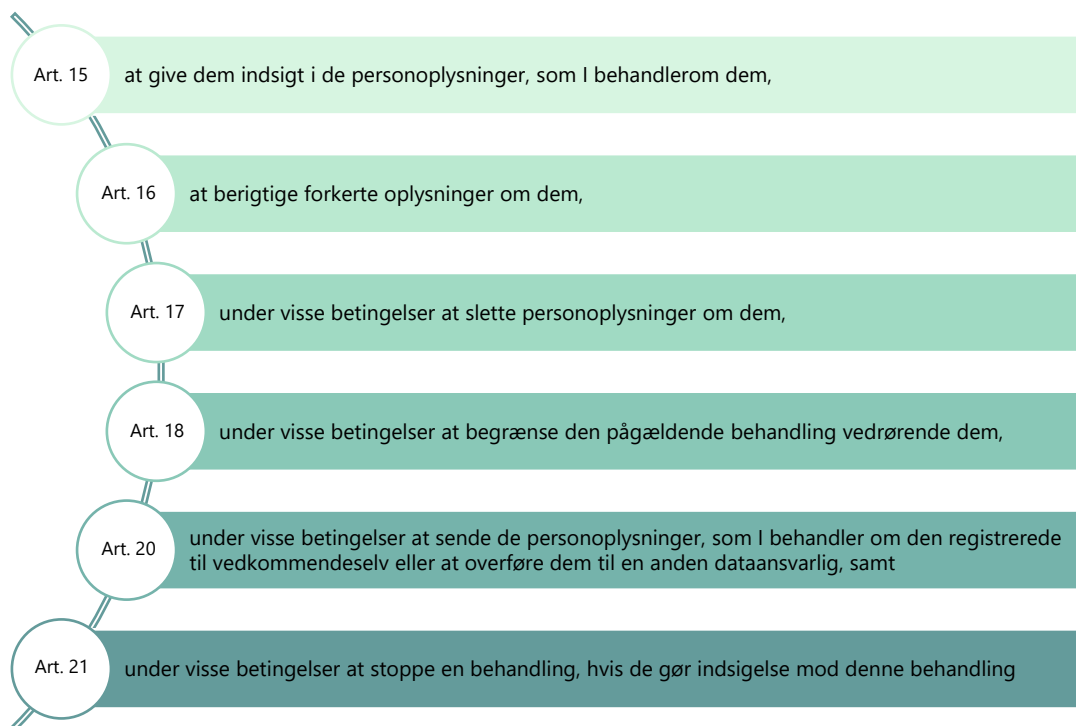
⁷⁶ Jf. AI-forordningens artikel 26, stk. 11.

⁷⁷ Jf. AI-forordningens artikel 50, stk. 1 og 2.

⁷⁸ Jf. AI-forordningens artikel 50, stk. 3 og 4.

(oplysningspligten), skal I som dataansvarlig på sædvanlig vis også være i stand til at kunne håndtere de øvrige rettigheder, som eleverne/de studerende m.fl. er tildelt efter databeskyttelsesforordningens kapitel III.

Det indebærer, at I efter anmodning fra eleverne/de studerende m.fl. skal være i stand til:



Figur 3 - Overblik over de registreredes rettigheder.

I forlængelse heraf skal I generelt være opmærksomme på, at der efter databeskyttelsesforordningens artikel 22 gælder et forbud mod anvendelse af automatiske, individuelle afgørelser, herunder profilering, i tilfælde, hvor afgørelsen har en betydelig påvirkning for eleven/den studerende. Automatiske, individuelle afgørelser er afgørelser, hvor der ikke har været en fysisk person involveret undervejs.⁷⁹

Disse former for afgørelser kan dog være lovlige, hvis én af undtagelserne til forbuddet er opfyldt, det vil sige:

- 1) Hvis behandlingen er nødvendig for indgåelse eller opfyldelse af en kontrakt mellem den registrerede og jer som dataansvarlig (eksempelvis en ansættelseskontrakt),
- 2) hvis behandlingen har hjemmel i EU-retten eller dansk ret, eller
- 3) hvis der forudgående indhentes et udtrykkeligt samtykke fra den registrerede.

Selvom den automatiske, individuelle afgørelse er lovlig, hvis en af ovenstående betingelser er opfyldt, har de studerende/eleverne m.fl. dog i en række situationer ret til at anmode om, at I

⁷⁹ [Ret til ikke at være genstand for en automatisk afgørelse \(datatilsynet.dk\)](https://datatilsynet.dk)

genoptager sagen og foretager en fornyet behandling ved menneskelig involvering i afgørelsen.⁸⁰

I skal svare på en anmodning om indsigt, sletning, berigtigelse mv. fra eleverne/de studerende hurtigst muligt, men senest en måned efter, I har modtaget anmodningen. I har dog mulighed for at forlænge svarfristen med yderligere to måneder, hvis der er tale om en anmodning, som er kompliceret. I så fald skal I senest en måned efter, I har modtaget anmodningen, gøre den registrerede opmærksom på sagsbehandlingstiden og samtidig give en begrundelse herfor.

Med henblik på at sikre en korrekt håndtering af elevernes/de studerendes rettigheder, anbefales det generelt, at I på forhånd har fastsat klare procedurer for den praktiske håndtering af efterlevelsen af de registreredes rettigheder.

I kan læse mere om hver enkelt rettighed i Datatilsynets vejledning om de registreredes rettigheder, jf. også kapitel 4 nedenfor.

4.5.5.4 Øvrige forpligtelser efter AI-forordningen

AI-forordningen er i udgangspunktet ikke en rettighedsforordning i modsætning til databeskyttelsesforordningen. AI-forordningen indeholder dog følgende rettigheder:

- 1) Enhver fysisk eller juridisk person, der har grund til at mene, at der er sket en overtrædelse af bestemmelserne i AI-forordningen, kan indgive en klage til den nationale tilsynsmyndighed.⁸¹
- 2) Enhver berørt person, der er omfattet af en afgørelse truffet af idriftsætteren på grundlag af output fra et højrisiko-AI-system opført i Bilag III, og som har retsvirkninger eller på tilsvarende måde i væsentlig grad påvirker den pågældende person på en måde, som personen anser for at have negativ indvirkning på vedkommendes sundhed, sikkerhed eller grundlæggende rettigheder, har ret til at få en klar og meningsfuld forklaring fra idriftsætteren om AI-systemets rolle i beslutningsprocessen og hovedelementerne i den trufne afgørelse.⁸²

4.5.6 Trin 6: Fastsæt centrale politikker og retningslinjer

Det følger af databeskyttelsesforordningen, at I, som nævnt i afsnit 4.5.5, har pligt til som udgangspunkt at oplyse om alle behandlinger af personoplysninger og at have procedurer på plads i forhold til håndteringen af en række databeskyttelsesretlige forpligtelser – f.eks. pligten til at varetage et tilstrækkeligt niveau af behandlingssikkerhed, pligten til at håndtere rettighedsanmodninger fra de registrerede mv. Der følger også krav fra AI-forordningen, som med fordel kan håndteres i politikker og procedurer.

Når elever m.fl. på uddannelsesinstitutionerne får udleveret it-udstyr eller bliver opfordret af institutionen til at downloade bestemte applikationer eller anvende bestemt it-udstyr i uddannelsesøjemed, er det således væsentligt, at eleverne m.fl. bliver gjort opmærksomme

⁸⁰ Jf. databeskyttelsesforordningens artikel 22, stk. 3.

⁸¹ Jf. AI-forordningens artikel 85.

⁸² Jf. AI-forordningens artikel 86.

på, hvordan deres personoplysninger behandles, samt hvilke begrænsninger AI-løsningerne har, og hvordan de kan anvendes sikkert.

Som minimum anbefales det, at I udarbejder følgende:

Persondatapolitik/Privatlivspolitik: I skal underrette de registrerede om jeres behandling af personoplysninger ved brug af AI-løsningerne, jf. databeskyttelsesforordningens artikel 13-14. Dette kan ske i en privatlivs- eller persondatapolitik. De registrerede er typisk eleverne, deres forældre og pårørende og de ansatte.

Politikken skal indeholde oplysninger om uddannelsesinstitutionen som dataansvarlig, herunder uddannelsesinstitutionens kontaktoplysninger og CVR-nr. Politikken skal også indeholde oplysninger om alle behandlinger af personoplysninger, som uddannelsesinstitutionen foretager, herunder ved brug af kunstig intelligens, med angivelse af behandlingernes formål, hjemmel i databeskyttelsesforordningen, behandlingernes tidsmæssige udstrækning, de specifikke typer af personoplysninger, som behandles, samt hvem personoplysningerne eventuelt indhentes fra eller deles med. De registreredes rettigheder skal endvidere fremgå af dokumentet, herunder den registreredes ret til at søge indsigt i behandlingerne og til at klage til Datatilsynet.

Bemærk, at I skal give de registrerede oplysningerne i medfør af oplysningspligten i databeskyttelsesforordningens artikel 13-14, f.eks. i brev eller pr. e-mail. Det betyder, at I ikke kan opfylde jeres oplysningspligt ved blot at have en hjemmeside med en persondata-/privatlivspolitik. Men I kan godt henvise de registrerede i et link, i en mail eller et brev til jeres hjemmeside, hvor de kan finde informationerne.

Retningslinjer for brug af jeres AI-værktøjer: Disse retningslinjer skal danne rammerne om jeres anvendelse af AI-løsninger og skal være rettet mod jeres ansatte, lærerne m.v.

Det er vigtigt, at medarbejderne er klar over, hvilke løsninger de må anvende, dvs. som er ledelsesgodkendte til brug i uddannelsesinstitutionen, herunder hvad der må anvendes af eleverne. Retningslinjerne bør også vejlede om korrekt brug og kan måske give eksempler på, hvordan gode prompts kan formuleres m.v.

Retningslinjerne skal sikre, at I kan anvende løsningerne korrekt, herunder i overensstemmelse med brugsvejledningen, og at brugerne er opmærksomme på faldgruberne, risiciene og begrænsningerne ved løsningerne. Retningslinjerne skal også understøtte, at løsningerne kan anvendes sikkert.

Retningslinjerne bør både forholde sig til behandling af personoplysninger, men også behandling af andre typer af data, f.eks. oplysninger som er fortrolige for uddannelsesinstitutionen.

Procedurer for behandling af rettighedsanmodninger fra de registrerede: Det er nødvendigt, at der er klare retningslinjer for håndteringen af anmodninger fra de registrerede om at udøve deres rettigheder, så det sikres, at disse altid håndteres korrekt og inden for de gældende tidsfrister. I proceduren skal det specifikt fremgå, hvem der er den ansvarlige person eller afdeling for håndteringen, hvordan fremsendelse af anmodninger skal håndteres, hvordan det sikres, at besvarelsen af anmodninger håndteres korrekt mv.

Det er vigtigt, at I i ovennævnte politikker og procedurer slår fast, hvem der har ansvaret for de forskellige aktiviteter, f.eks. med angivelse af den specifikke person (stillingsbetegnelse) eller afdeling. Det er også væsentligt, at den angivne person eller afdeling er bekendt med ansvaret og har de nødvendige ressourcer til at håndtere ansvaret tilstrækkeligt.

Hvis uddannelsesinstitutionen har en databeskyttelsesrådgiver – også kaldet en DPO (fra engelsk "Data Protection Officer") – skal databeskyttelsesrådgiveren inddrages hvor nødvendigt, herunder i forhold til udarbejdelse af konsekvensanalyser, ved brud på persondatasikkerheden og i forbindelse med kontakt med Datatilsynet. Det kan i denne forbindelse også være hensigtsmæssigt at udarbejde en procedure for inddragelse af databeskyttelsesrådgiveren med henblik på at gøre ansatte medarbejdere opmærksomme på, hvornår og hvorledes databeskyttelsesrådgiveren skal inddrages.

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

Trin nr. 7 handler om, at I både efter de databeskyttelsesretlige regler og AI-forordningen gennem undervisning og uddannelse skal sikre, at jeres medarbejdere, herunder undervisere og administrative medarbejdere, har det fornødne kendskab til, hvordan man håndterer AI-systemerne og behandlingen af personoplysningerne korrekt og lovligt.

I kan med fordel sammentænke jeres uddannelsesindsatser efter både databeskyttelsesforordningen og AI-forordningen (og andre retsgrundlag), så I effektivt og sammenhængende kan gennemføre jeres uddannelsesindsatser.

Databeskyttelsesreglerne indeholder forpligtelser, hvorefter risici ved behandlingen af personoplysninger skal håndteres ved passende organisatoriske og tekniske foranstaltninger. Dette omfatter normalt også, at I underviser og instruerer jeres medarbejdere i at kunne behandle personoplysninger lovligt og kunne være opmærksom på risiciene for de registrerede m.v., når de anvender jeres AI-løsninger.

Det følger også af AI-forordningen⁸³, at I, når I anvender eller udbyder AI-systemer, har pligt til at sikre "AI-færdigheder"⁸⁴ hos jeres medarbejdere. Forpligtelsen er bred, og den finder derfor anvendelse i forhold til alle involverede AI-systemer i hele systemets livscyklus, herunder også ved udviklingen af et AI-system, uanset om der er tale om højrisikosystemer⁸⁵ eller ej.

Forpligtelsen til at sikre AI-færdigheder gælder allerede fra den 2. februar 2025. Pligten til AI-færdigheder gælder, inden jeres medarbejdere bruger AI-systemerne, og I bør derfor sikre jer, at nye såvel som gamle medarbejdere, der kommer i berøring med AI-systemerne i forbindelse med deres arbejde, uddannes fra start.

⁸³ Der henvises til AI-forordningens artikel 4.

⁸⁴ I AI-forordningens artikel 3, nr. 56, defineres AI-færdigheder som "færdigheder, viden og forståelse, der giver udbydere, idriftsættere og berørte personer mulighed for under hensyntagen til deres respektive rettigheder og forpligtelser i forbindelse med denne forordning at idriftsætte AI-systemer på et informeret grundlag samt at øge bevidstheden om muligheder og risici ved AI og den mulige skade, som den kan forvolde".

⁸⁵ Der henvises til AI-forordningens Bilag III for en beskrivelse af, hvilke AI-systemer der udgør højrisikosystemer.

4.5.7.1 AI-færdigheder afhænger af AI-systemet og medarbejdernes rolle

Graden af nødvendige AI-færdigheder vil typisk være relateret til de arbejdsfunktioner, som medarbejderen er involveret i. Således vil grader af AI-færdigheder variere i forhold til, om der er tale om medarbejdere, der udvikler AI-systemet, en leder, der har ansvaret for udvikling og idriftsættelse, eller medarbejdere, som anvender AI-systemet. Ligeledes vil nogle medarbejdere, allerede når de indtræder på arbejdspladsen besidde de nødvendige AI-færdigheder.

Det vil derfor være nødvendigt at vurdere fra person til person, i hvilken udstrækning det er nødvendigt at løfte medarbejderens AI-færdigheder.

Samtidig vil graden af nødvendige AI-færdigheder afhænge af AI-systemet, både ift. kompleksiteten i systemet samt anvendelsesområdet, herunder om der er tale om minimal eller høj risiko for indvirkning på grundlæggende rettigheder og sikkerhed.

For at håndtere det i praksis kan uddannelsesinstitutionerne eksempelvis opstille nogle organisatoriske rammer, der skaber tydelighed om roller og relaterede forventninger til AI-færdigheder for de enkelte AI-systemer.⁸⁶

Forpligtelsen gælder således i forhold til alle jeres medarbejdere, herunder også undervisere/lærere og administrative medarbejdere, som er involveret på et hvilket som helst stadie af et AI-systems livscyklus, det vil sige udvikling, test, drift og/eller overvågning. Det indebærer samtidig, at det ikke er samtlige af jeres medarbejdere, som skal have AI-færdigheder efter AI-forordningen, da betingelsen er, at den enkelte medarbejder på den ene eller anden måde skal være involveret i udvikling, test, drift og/eller anvendelse af et AI-system. Således gælder uddannelsesforpligtelsen f.eks. ikke for servicemedarbejdere, herunder rengøringspersonale, pedeller mm., som typisk ikke vil være involveret i udvikling, test, drift og/eller anvendelse af et AI-system.

Forpligtelsen til at sikre AI-færdigheder gælder imidlertid ikke kun for jeres egne medarbejdere, men også for andre personer der er under uddannelsesinstitutionens instruktionsbeføjelse. I kan derfor også være forpligtet til at sikre AI-færdigheder hos tredjeparter, herunder jeres databehandlere, vikarer, indlånede medarbejdere mm., idet omfang disse er under uddannelsesinstitutionens instruktionsbeføjelse og er involveret i udvikling, test, drift og/eller anvendelse af et AI-system.

AI-færdigheder omfatter både medarbejdernes færdigheder, viden og forståelse om AI-systemer. Formålet med at sikre AI-færdigheder er at gøre jeres medarbejdere i stand til at anvende AI-systemerne på et informeret grundlag samt at øge deres bevidsthed om mulighederne og risici ved AI og den mulige skade, som AI kan forvolde.⁸⁷

Det er imidlertid ikke specificeret i lovgivningen, hvilke tiltag man som udbyder eller idriftsætter skal igangsætte for at sikre et tilstrækkeligt niveau af AI-færdigheder hos medarbejderne. Det er derfor op til hver enkelt uddannelsesinstitution at lave en vurdering af, hvad der er tilstrækkelige AI-færdigheder i deres kontekst.

⁸⁶ Vejledning om AI-færdigheder, Digitaliseringsstyrelsen, s. 2.

⁸⁷ Der henvises til artikel 3, nr. 56 i AI-forordningen.

4.5.7.2 Typer af AI-færdigheder

AI-færdigheder kan opdeles i forskellige kategorier, såsom teknologisk, praktisk og etisk forståelse af AI-teknologien. Eksemplerne i hver kategori hænger ofte sammen, hvorfor de også vil gå på tværs af beskrivelserne.

- **Teknologiske færdigheder:** Disse færdigheder handler om forståelse for, hvordan AI-systemer er udviklet. De konkrete færdigheder vil afhænge af, hvilken type af kunstig intelligens der benyttes i organisationen, f.eks. maskinlæring, generativ kunstig intelligens mv. Med disse færdigheder opnår man endvidere viden om, hvilke datakilder der ligger til grund for træningen af AI-systemet, og hvordan AI-systemet behandler, vægter, tolker og præsenterer informationer.
- **Praktiske færdigheder:** Disse færdigheder handler om evnen til at kunne anvende et AI-system efter hensigten. Dette kan eksempelvis være viden om, hvordan AI-systemet anvendes, hvilke arbejdsopgaver det må bruges til, og hvilke forholdsregler der eventuelt skal tages i anvendelsen. For opbygningen af sådanne færdigheder, kan der opstilles retningslinjer og oplæring i brugen af et specifikt AI-system. Retningslinjerne vil afhænge af typen af kunstig intelligens, hvordan løsningen fungerer, og de risici, der er forbundet med anvendelsen.
- **Etiske færdigheder:** Disse færdigheder handler om forståelsen for de implikationer, som indførelsen af et AI-system kan have både på medarbejdere og samfundet i øvrigt. Etiske færdigheder kan indeholde, at man klæder sine medarbejdere på til at kunne opdage og reflektere over etiske problemstillinger ved udvikling og brug af kunstig intelligens.⁸⁸

Nedenfor er et eksempel på en trinvis tilgang, som man kan tage for at sikre AI-færdigheder:

⁸⁸ Vejledning om AI-færdigheder, Digitaliseringsstyrelsen, s. 2-3.

Trin 1 - Skab overblik over brugen af AI

Identificér de situationer, hvor der benyttes AI, som falder inden for AI-forordningen.

**Trin 2 – Skab overblik over de medarbejdere der er involveret i brugen af AI**

Identificér medarbejderne og deres roller. Inkludér både medarbejdere der arbejder direkte med AI og dem, der indirekte berøres heraf.

**Trin 3 – Afklar nødvendige AI-færdigheder inden for de forskellige roller**

Overvej hvilke AI-færdigheder, der er nødvendig for de identificerede medarbejdere.

**Trin 4 – Eksekvering**

Planlæg organisatoriske tiltag. Se eksempler på disse nedenfor.

4.5.7.3 Eksempler på typer af organisatoriske tiltag, der medvirker til at sikre AI-færdigheder:⁸⁹

Eksempler på organisatoriske tiltag:

- E-læringskurser for medarbejdere og ledere, der målretter de forskellige typer af færdigheder og niveauer.
- Lokale AI-fagfællesskaber
- AI-færdighedsambassadører inden for organisationen
- E-mails, nyhedsbreve og anden skriftlig kommunikation om AI-færdigheder
- Awarenesskampagner.

I skal være opmærksomme på, at AI-forordningen ikke opstiller klare betingelser for, hvornår I – som enten udbyder eller idriftsætter – i praksis har efterlevet forpligtelsen om at sikre AI-færdigheder. Det vil i stedet bero på en konkret vurdering, hvori jeres rolle (som udbyder eller idriftsætter) bl.a. skal indgå samt følgende tre forhold:

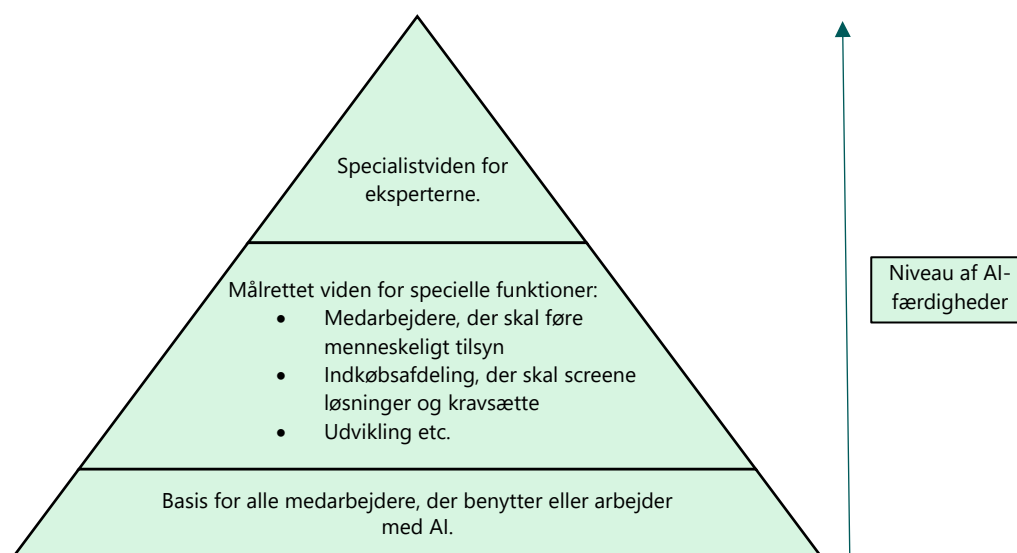
- 1) Personernes (som anvender AI-systemet) tekniske viden, erfaring og uddannelse;
- 2) Konteksten, hvori AI-systemet anvendes, det vil sige hvilken forretningsmæssig funktion systemet understøtter (evaluering af eleverne/de studerende contra at understøtte en læringsproces) samt de risici, som er forbundet med anvendelsen af systemet; og

⁸⁹ Vejledning om AI-færdigheder, Digitaliseringsstyrelsen, s. 4.

3) Hvilke personer/grupper af personer, AI-systemet skal anvendes på.

Ovenstående indebærer også, at I bør udarbejde et uddannelsesprogram i forskellige niveauer, da kravet til AI-færdigheder vil variere væsentligt alt afhængigt af den enkelte medarbejders brug af AI-systemet.

Formålet med et differentieret uddannelsesprogram er, at I på den måde fastsætter forskellige uddannelsesmæssige krav og indsatser på tværs af de forskellige områder/kontekster, hvor jeres medarbejdere anvender AI-systemer. Det indebærer samtidig, at de af jeres medarbejdere, som kun periodisk/kortvarigt vil komme i berøring med AI-systemerne, ikke nødvendigvis behøver at have de samme AI-færdigheder, som eksempelvis de medarbejdere der på daglig basis er i berøring med AI-systemerne. Dette kan også illustreres på følgende måde:



Figur 5 - Eksempel på et uddannelsesprogram opdelt i forskellige niveauer.⁹⁰

Man kan eksempelvis forestille sig i relation til folkeskolen, at den praktiske anvendelse af AI-systemerne vil variere væsentligt afhængigt af klassetrin, således at AI-systemerne i langt højere grad anvendes af en lærer i relation til elever på mellemtrinnet og udskolingen, end en lærer som underviser elever i indskolingen. Det vil medføre, at kravet om AI-færdigheder højst sandsynligt vil være større for læreren, som underviser mellemtrinnet og udskolingen, end læreren, som underviser i indskolingen.

AI-forordningen indeholder imidlertid ikke specifikke krav til, hvordan jeres uddannelsesprogram i praksis skal gennemføres, det vil sige hvilket format (fysisk undervisning, e-learning mm.), I skal anvende, samt med hvilken frekvens. Det er således op til den enkelte uddannelsesinstitution at beslutte denne fremgangsmåde og behovet herfor.

⁹⁰ Menneskeligt tilsyn: Tilsyn, hvor et menneske fører tilsyn med løsningen, herunder om løsningen performer korrekt, med korrekt output og fortsat er sikker mv.

4.6 Særligt vedrørende egenudvikling af AI-løsninger

Som anført ovenfor er udgangspunktet i denne vejledning, at I som oftest vil handle som idriftsættere efter AI-forordningen. Der kan dog også være tilfælde, hvor I er udbydere, hvis I udvikler og ibrugtager jeres egen AI-løsning.

I vil endvidere som idriftsætter blive anset som udbyder af et højrisiko-AI-system, og dermed også underlagt forpligtelserne for en udbyder i AI-forordningen, i følgende tilfælde:

- I anbringer jeres navn eller varemærke på et højrisiko-AI-system
- I foretager en væsentlig ændring af et højrisiko-AI-system
- I ændrer det tilsigtede formål med et AI-system på en sådan måde, at det pågældende AI-system bliver et højrisiko-AI-system.

Hvis I kan anses som udbyder af et højrisiko-AI-system oplister AI-forordningen bl.a. følgende overordnede krav, som I skal opfylde:⁹¹

- Sikre overholdelse af de visse krav for højrisiko-AI-systemer⁹² og foretage korrigerende foranstaltninger, hvis kravene ikke er opfyldt.
- Indføre et kvalitetsstyringssystem.
- Udarbejde den tekniske dokumentation for højrisiko-AI-systemet.
- Opbevare de logfiler, der automatisk genereres af deres højrisiko-AI-systemer, når logfilerne er under deres kontrol.
- Sørge for at gennemføre overensstemmelsesvurdering for systemet.
- Kunne påvise overholdelse af kravene til tilsynsmyndighederne.

AI-forordningens artikel 9-15 indeholder de tekniske krav til højrisiko-AI-systemer, som I, når I optræder som udbyder, skal overholde. Disse krav vil dog også være relevante for jer, selvom I ikke ifalder rollen som udbyder, da I bør overveje, om udbyderen overholder kravene i AI-forordningen. De tekniske krav er som følger:

Tekniske krav	Artikel i AI-forordningen
Der skal etableres et risikostyringssystem til højrisiko-AI-systemer. Systemet skal implementeres, vedligeholdes og dokumenteres gennem hele AI-systemets levetid. Det skal samtidig gennemgås og opdateres regelmæssigt for at sikre, at systemet fortsat er effektivt.	Artikel 9

⁹¹ AI-forordningen artikel 16, der oplister samtlige krav.

⁹² Se figur 5.

Tekniske krav	Artikel i AI-forordningen
Såfremt AI-systemet involverer træning af modeller med data, skal de pågældende datasæt om data og datastyring efterleve en række kvalitetskriterier, herunder bl.a. for passende datastyring- og data-forvaltningspraksis, samt at datasæt skal være relevante, repræsentative, fejlfri og fuldstændige.	Artikel 10
Der skal udarbejdes teknisk dokumentation, der påviser, at højrisiko-AI-systemet overholder de krav, der er fastsat i forordningen, og således at alle de oplysninger, der er nødvendige for at vurdere AI-systemets overholdelse af disse krav, gives til de nationale kompetente myndigheder og bemyndigede organer.	Artikel 11
Højrisiko-AI-systemer skal udformes og udvikles på en sådan måde, at hændelser ("logfiler") registreres automatisk, når højrisiko-AI-systemet er i drift.	Artikel 12
Systemerne skal udformes og udvikles på en sådan måde, at deres drift er tilstrækkelig gennemsigtig til, at brugerne kan fortolke systemets output og anvende det korrekt. Samtidig skal systemet ledsages af brugsanvisninger i et passende digitalt format eller på anden vis, som indeholder kortfattede, fuldstændige, korrekte og klare oplysninger, som er relevante, tilgængelige og forståelige for brugerne.	Artikel 13
Højrisiko-AI-systemer skal udformes og udvikles på en sådan måde, herunder med passende menneske-maskine-grænseflade-værktøjer, at fysiske personer kan føre effektivt tilsyn med dem i den periode, hvor AI-systemerne er i brug.	Artikel 14
Højrisiko-AI-systemer skal udformes og udvikles på en sådan måde, at de i lyset af deres tilsigtede formål har et passende niveau af nøjagtighed, robusthed og cybersikkerhed i hele deres livscyklus.	Artikel 15

Tabel 5 – Oversigt over de tekniske krav til højrisiko-AI-systemer som en udbyder skal overholde.

Såfremt I måtte have behov for at udvikle AI-løsninger til egen brug, f.eks. til et nyt it-system, er det også væsentligt at indtænke databeskyttelse på et så tidligt stadie som muligt. I skal nemlig efter data-beskyttelsesforordningen sikre, at de databeskyttelsesretlige krav og beskyttelseshensyn varetages som en integreret del i hele behandlingsforløbet i AI-løsningen. Det betyder, at I skal overveje, om der til brug for udvikling af løsningen behandles personoplysninger, og om behandlingen lever op til behandlingsprincipperne som beskrevet ovenfor under afsnit 4.3. De datasæt, som anvendes til træning, test og validering af en AI-løsning, kan hver især indeholde personoplysninger, og bestemte behandlinger (f.eks. samkøring af flere typer af personoplysninger) kan resultere i, at behandlingen bliver mere risikofyldt, f.eks. ved at der på grund af behandlingen kan udledes følsomme personoplysninger om de registrerede.

AI-løsningen skal også rent teknisk kunne understøtte, at man kan overholde databeskyttelsesreglerne, f.eks. at man kan udtrække personoplysninger i løsningen, så man kan give indsigt heri, samt at løsningen skal kunne slette personoplysninger effektivt m.v. AI-

løsningsen kan designes ved brug af teknologier, der fremmer privatlivsbeskyttelse, såsom dataminimeringsforanstaltninger, anonymisering og pseudonymisering af personoplysninger, adgangskontrol og brugerstyring samt kryptering af personoplysninger i transit og i hvile m.v.

Det vil i de fleste tilfælde være nødvendigt at gennemføre en konsekvensanalyse vedrørende databeskyttelse, da behandling af personoplysninger i forbindelse med udvikling og brug af en AI-løsning med stor sandsynlighed vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

Ved egenudvikling af AI-løsninger skal I altså være opmærksomme på, at der udvælges og implementeres passende tekniske og organisatoriske foranstaltninger, som er egnede til at mitigere de risici, der vurderes at være ved behandlingen af personoplysninger. Foranstaltningerne skal være designet med henblik på at sikre en effektiv implementering af de grundlæggende behandlingsprincipper, som er principperne om lovlighed, rimelighed og gennemsigtighed, princippet om formålsbegrænsning, princippet om dataminimering, princippet om korrekte og ajourførte personoplysninger, princippet om opbevaringsbegrænsning og princippet om sikkerhed.

5. Hvis I vil vide mere

I har mulighed for at få yderligere hjælp og vejledning fra flere officielle kilder, herunder Datatilsynet og Digitaliseringsstyrelsen. I kan derfor læse mere om, hvad I skal være opmærksomme på, når I bruger kunstig intelligens, samt yderligere information om kravene i databeskyttelsesforordningen og AI-forordningen her:

- Databeskyttelsesforordningen (Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)).⁹³
- Databeskyttelsesloven (Lovbekendtgørelse nr. 289 af 8. marts 2024 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)), der supplerer bestemmelserne i databeskyttelsesforordningen.⁹⁴
- AI-forordningen (Europa-Parlamentets og Rådets forordning (EU) 2024/1689 af 13. juni 2024 om harmoniserede regler for kunstig intelligens og om ændring af forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 og (EU) 2019/2144 samt direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (forordningen om kunstig intelligens)).⁹⁵
- Styrelsen for Undervisning og kvalitets anbefalinger for brug af generativ kunstig intelligens, november 2024.⁹⁶ I skal være opmærksomme på, at disse anbefalinger er af mere generel karakter, og derfor ikke har fokus på de juridiske problematikker.
- Digitaliseringsstyrelsen har udarbejdet to guides (til virksomheder og offentlige myndigheder) til ansvarlig anvendelse af generativ kunstig intelligens, januar 2024.⁹⁷
- Datatilsynet har udarbejdet en vejledning om offentlige myndigheders brug af AI og kortlægning af AI på tværs af den offentlige sektor, oktober 2024.⁹⁸
- Datatilsynet har udarbejdet en vejledning om de registreredes rettigheder, juli 2018.⁹⁹

⁹³ EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/ 679 - af 27. april 2016 - om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/ 46/ EF (generel forordning om databeskyttelse)

⁹⁴ [Databeskyttelsesloven](#)

⁹⁵ [Europa-Parlamentets og Rådets forordning \(EU\) 2024/1689 af 13. juni 2024 om harmoniserede regler for kunstig intelligens og om ændring af forordning \(EF\) nr. 300/2008, \(EU\) nr. 167/2013, \(EU\) nr. 168/2013, \(EU\) 2018/858, \(EU\) 2018/1139 og \(EU\) 2019/2144 samt direktiv 2014/90/EU, \(EU\) 2016/797 og \(EU\) 2020/1828 \(forordningen om kunstig intelligens\)EØS-relevant tekst.](#)

⁹⁶ [Nu kommer anbefalinger for brug af generativ kunstig intelligens i undervisningen på landets ungdomsuddannelser | Børne- og Undervisningsministeriet](#)

⁹⁷ [Nye guides til ansvarlig anvendelse af generativ kunstig intelligens](#)

⁹⁸ [Ny vejledning om offentlige myndigheders brug af AI og kortlægning af AI på tværs af den offentlige sektor](#)

⁹⁹ [Registreredes rettigheder.pdf](#)

- Datatilsynet har udarbejdet en vejledning om databeskyttelsesretlige konsekvensanalyser (DPIA), marts 2018.¹⁰⁰
- Datatilsynet har udarbejdet en vejledning om behandlingssikkerhed og databeskyttelse gennem design og standardindstillinger, juni 2018.¹⁰¹
- Ekspertgruppen for ChatGPT og andre digitale hjælpemidler har i april 2024 afgivet en række anbefalinger til, hvordan ChatGPT mv. kan håndteres ved prøver.¹⁰²
- Dansk Industri har i fællesskab med en række private og offentlige aktører, herunder bl.a. Digitaliseringsstyrelsen og Erhvervsstyrelsen, udarbejdet en hvidbog vedrørende ansvarlig brug af AI-assistenter i den offentlige og private sektor, 2024.¹⁰³
- Europa-Kommissionens generaldirektorat for Uddannelse, Unge, Idræt og Kultur har i 2022 udgivet etiske retningslinjer for anvendelse af kunstig intelligens (AI) og data inden for undervisning og læring til brug for undervisere.¹⁰⁴

¹⁰⁰ [Vejledning om konsekvensanalyse](#)

¹⁰¹ [Vejledning om behandlingssikkerhed og databeskyttelse gennem design og standardindstillinger](#)

¹⁰² [Ekspertgruppe klar med anbefalinger for brug af ChatGPT ved prøver - Styrelsen for Undervisning og Kvalitet](#)

¹⁰³ [di-digitaliseringspolitik-2024-ai-hvidbog-lang-version-web.pdf](#)

¹⁰⁴ [Etiske retningslinjer for anvendelse af kunstig intelligens \(AI\) og data inden for undervisning og læring til brug for undervisere - Publications Office of the EU](#)

Bilag A: Ordliste med centrale termer

Dette bilag A indeholder en ordliste over centrale termer inden for kunstig intelligens og databeskyttelsesretten, som anvendes i de forskellige afsnit i denne vejledning. Det bemærkes, at en række af de centrale begreber inden for kunstig intelligens er defineret i tabel 1 i vejledningens afsnit 3.1 ("Hvad er AI").

Begreb	Definition	Relevans for uddannelsesinstitutioner m.fl.
Anonymisering	Personoplysninger kan anonymiseres, hvilket betyder, at ingen fysiske personer kan identificeres ud fra oplysningerne eller i kombination med andre oplysninger. Denne type af oplysninger udgør ikke personoplysninger, hvis anonymiseringen er uigenkaldelig. ¹⁰⁵	Anonymisering af personoplysninger er generelt et effektivt værktøj at anvende eksempelvis ifm. udvikling af AI-løsninger, da dette medfører – forudsat at anonymiseringen er uigenkaldelig – at reglerne i databeskyttelsesforordningen ikke skal efterleves. Det skal konkret vurderes, om en anonymisering er uigenkaldelig, eller om det fortsat er muligt at identificere den fysiske person. Alle relevante hjælpemidler skal tages i brug ved denne vurdering. ¹⁰⁶

¹⁰⁵ [Hvad er personoplysninger \(datatilsynet.dk\)](https://datatilsynet.dk)

¹⁰⁶ [Hvad er personoplysninger \(datatilsynet.dk\)](https://datatilsynet.dk)

Begreb	Definition	Relevans for uddannelsesinstitutioner m.fl.
Bias, f.eks. automation bias	Bias vedrører en forudindtaget holdning mod en person, genstand eller holdning. Bias kan opstå på mange måder i f.eks. AI-systemer. I AI-systemer, som oftest er baseret på en stor mængde af data, f.eks. systemer der bygger på maskinlæringsteknikker, kan bias i forbindelse med dataindsamling og oplæring resultere i et AI-system, der udviser bias. Bias kan både være god eller dårlig, bevidst eller ubevidst. I visse tilfælde kan bias have diskriminerende og/eller urimelige udfald (dvs. urimelig bias).¹⁰⁷	Antagelser baseret på algoritmer kan forstærke eksisterende bias, der er indbygget i nuværende uddannelsespraksis, dvs. bias vedrørende køn, race, kultur, muligheder eller handicapstatus. Bias kan også opstå som følge af onlinelæring og tilpasning gennem interaktion. Bias kan derudover også opstå gennem personalisering, hvorved brugere præsenteres for anbefalinger eller informationsfeeds, der er skræddersyet til brugernes præferencer.¹⁰⁸
Chatbot	En Chatbot er et computerprogram, der – ved hjælp af maskinlæringsteknikker – kan kommunikere med mennesker gennem tekst- eller talekommandoer på en måde, der efterligner samtaler mellem mennesker.¹⁰⁹	Chatbots kan anvendes af lærer til at søge viden til brug for undervisningen. Endvidere kan eleverne anvende chatbots til at give yderligere information om emner eksempelvis til brug for opgaveskrivning m.m.
Datasæt	Et datasæt er en samling af organiseret datapunkter, som kan bruges til at træne, validere og teste AI-systemer.¹¹⁰	På uddannelsesområdet leveres og anvendes datasæt hovedsagelig til at støtte ny forskning og til at dele og anvende eksisterende forskning.¹¹¹

¹⁰⁷ [etiske retningslinjer for anvendelse af kunstig intelligens-NC0722649DAN \(1\).pdf](#) s. 33.

¹⁰⁸ [etiske retningslinjer for anvendelse af kunstig intelligens-NC0722649DAN \(1\).pdf](#) s. 33.

¹⁰⁹ [etiske retningslinjer for anvendelse af kunstig intelligens-NC0722649DAN \(1\).pdf](#) s. 33.

¹¹⁰ [etiske retningslinjer for anvendelse af kunstig intelligens-NC0722649DAN \(1\).pdf](#) s. 33.

¹¹¹ [etiske retningslinjer for anvendelse af kunstig intelligens-NC0722649DAN \(1\).pdf](#) s. 33.

Begreb	Definition	Relevans for uddannelsesinstitutioner m.fl.
DPIA	En DPIA/konsekvensanalyse vedrørende databeskyttelses er en proces, hvor formålet er at beskrive behandlingen af personoplysninger, vurdere behandlingens nødvendighed og proportionalitet samt bidrage til at håndtere de risici for fysiske personers rettigheder og frihedsrettigheder, som behandlingen af personoplysninger medfører. ¹¹²	Ved brugen af AI-løsninger på uddannelsesområdet, hvor der sker en behandling af personoplysninger, vil der generelt være en forpligtelse til at udarbejde en konsekvensanalyse vedrørende databeskyttelse.
Inputdata	Inputdata udgør enhver information, der gives til en computer.	På uddannelsesområdet skal det sikres, at inputdata er relevante for AI-systemets formål.
Kryptering	Kryptering er en teknisk proces, hvor information ændres til en hemmelig kode og således skjuler de data, som sendes, modtages eller gemmes. Oplysningerne kan vises i klartekst ved hjælp af en dekrypteringsnøgle.	Kryptering vil oftest udgøre en effektiv teknisk sikkerhedsforanstaltning, når man behandler personoplysninger.
Menneskeligt review	Menneskeligt review beskriver bl.a. den proces, hvor en fysisk person gennemgår outputtet af en AI-løsning med henblik på at vurdere, om det er korrekt.	På uddannelsesområdet er det vigtigt, at man ved brug af AI-løsninger indarbejder et menneskeligt review med henblik på at sikre, at løsningernes output er korrekte.

¹¹² [Konsekvensanalyser \(datatilsynet.dk\)](https://datatilsynet.dk/konsekvensanalyser)

Begreb	Definition	Relevans for uddannelsesinstitutioner m.fl.
Metadata	Metadata er oplysninger, der anvendes til at beskrive, henvise til, kontekstualisere eller karakterisere en datafil såsom en webside, et billede, en video, et dokument eller en fil. Det er således data, der beskriver data, men det er ikke selve dataene.¹¹³	Lærer kan ved hjælp af metadata lettere hente og evaluere undervisnings- og læringsressourcer, så de har flere valgmuligheder med hensyn til det materiale, de vælger til eleverne/de studerende Dette kan også hjælpe med at dirigere den enkelte studerende til indhold i forhold til deres evner eller parathed.¹¹⁴
Output	Output udgør den information, som en AI-løsning generer baseret på dets inputdata og løsningens algoritme.	N/A
Pseudonymisering	Personoplysninger kan pseudonymiseres, hvilket betyder, at personoplysningerne ikke længere kan henføres til en bestemt fysisk person uden brug af supplerende oplysninger. Det er forudsat, at disse supplerende oplysninger opbevares separat og er underlagt tekniske/organisatoriske foranstaltninger, således at de ikke kan henføres til en identificeret eller identificerbar fysisk person. ¹¹⁵	N/A
Registrerede	Personer, om hvem personoplysninger behandles.	På uddannelsesområdet vil de registrerede typisk være eleverne/de studerende, lærerne/underviserne, forældre, administrativt personale, ledelsen m.fl.

¹¹³ [etiske retningslinjer for anvendelse af kunstig intelligens-NC0722649DAN \(1\).pdf](#), s. 35.

¹¹⁴ [etiske retningslinjer for anvendelse af kunstig intelligens-NC0722649DAN \(1\).pdf](#), s. 35.

¹¹⁵ [Hvad er personoplysninger \(datatilsynet.dk\)](#)

Bilag B: Kortlægning af AI-løsninger

[Uddannelsesinstitutionens navn] kortlægning af brugen af AI-systemer samt behandlingen af personoplysninger heri

Emne	Spørgsmål om anvendelse af AI	Institutionens svar
1. BRUGEN AF AI-SYSTEMER	<i>Anvender I et AI-system?</i>	[Indsæt ja/nej + hvis ja, indsæt navnet/navnene på AI-systemet/AI-systemerne]
<i>1.1</i>	<i>Hvad anvender I AI-systemet til? Hvad er systemets formål?</i>	[Indsæt en beskrivelse af, hvad AI-systemet anvendes til i praksis, herunder dets formål, eksempelvis understøttelse af evaluering af elevernes skriftlige opgaver eller understøtter undervisning af eleverne]
2. BEHANDLING AF PERSONOPLYSNINGER	<i>Behandler I personoplysninger i AI-systemet?</i>	[Indsæt ja/nej + hvis ja, beskriv kategorierne af personoplysningerne der behandles i systemet, dvs. almindelige, fortrolige og/eller følsomme personoplysninger]
<i>2.1</i>	<i>Hvilke kategorier af registrerede behandles der personoplysninger om i AI-systemet?</i>	[Indsæt beskrivelse af, hvilke kategorier af registrerede, der behandles personoplysninger om i AI-systemet, f.eks. elever/studerende, ansatte, forældre, ledelse, leverandører]

Emne	Spørgsmål om anvendelse af AI	Institutionens svar
2.2	<i>Hvilke kategorier af personoplysninger behandler I i AI-systemet om de forskellige kategorier af registrerede?</i>	[Indsæt beskrivelse af, hvilke personoplysninger I behandler om hver enkelt kategori af registrerede, f.eks.: - Ansatte = almindelige personoplysninger (navn, adresse, e-mail), fortrolige oplysninger (CPR-nummer) - Elever = almindelige personoplysninger (navn, skolebillede etc.)]
2.3	<i>Hvad er formålet med behandlingen af personoplysningerne i AI-systemet?</i>	[Indsæt formålet med behandlingen, f.eks.: "Formålet med behandlingen af personoplysningerne er at kunne understøtte undervisningen af eleverne ved brug af et AI-system"]
3. RISIKONIVEAU EFTER AI-FORORDNINGEN	<i>Hvilken risiko indebærer anvendelsen af AI-systemet?</i>	[Indsæt en beskrivelse af AI-systemets risikoniveau, dvs. 1) forbudt, 2) højrisiko, 3) begrænset risiko, 4) lav risiko]
4. JERES ROLLE EFTER DATABESKYTTELSES-FORORDNINGEN	<i>Hvilken databeskyttelsesretlig rolle har I vedrørende behandlingen af personoplysninger, der foregår i forbindelse med anvendelsen af AI-systemet?</i>	[Indsæt en beskrivelse af, hvorvidt I er dataansvarlig eller databehandler i forbindelse med den behandling af personoplysninger, der foregår ved brugen af AI-systemerne – sontringen er vigtig i forhold til jeres forpligtelser efter databeskyttelsesforordningen]

Emne	Spørgsmål om anvendelse af AI	Institutionens svar
5. JERES ROLLE EFTER AI-FORORDNINGEN	<i>Hvilken rolle har I efter AI-forordningen?</i>	[Indsæt en beskrivelse af, hvorvidt I for hver enkelt AI-system er udbyder eller idriftsætter samt en begrundelse herfor – sontringen er vigtig i forhold til jeres forpligtelser efter AI-forordningen]
6. BEHANDLINGSGRUNDLAG EFTER DATABESKYTTELSES-FORORDNINGEN	<i>Hvilke(t) databeskyttelses-retligt behandlingsgrundlag benytter I, når der sker behandling af personoplysninger i forbindelse med jeres brug af AI-systemet?</i>	[Indsæt en beskrivelse af, hvilke(n) lovlige hjemmelsgrundlag I anvender efter databeskyttelsesforordningen, når I behandler personoplysninger i AI-systemet]
7. TREDJELANDS-OVERFØRSLER	<i>Sker der overførsel af personoplysninger til tredjelande i forbindelse med brugen af AI-systemet?</i>	[Indsæt ja/nej + hvis ja, indsæt en beskrivelse af tredjelandsoverførslerne samt en henvisning til jeres selvstændige kortlægning af dataflowet og de potentielle tredjelandsmodtagere]
8. DATABESKYTTELSESRET-LIG RISIKOVURDERING	<i>Har I gennemført en databeskyttelsesretlig risikovurdering vedrørende behandlingssikkerhed efter databeskyttelsesforordningens artikel 32?</i>	[Indsæt ja/nej - (husk I er forpligtet hertil både som dataansvarlig og databehandler)]
9. DATABESKYTTELSESRET-LIG KONSEKVENSA-ANALYSE (DPIA)	<i>Har I vurderet, hvorvidt I er forpligtet til at gennemføre en konsekvensanalyse efter databeskyttelsesforordningens artikel 35?</i>	[Indsæt ja/nej - (husk I er kun forpligtet til dette, hvis I er dataansvarlig og behandlingsaktiviteten er omfattet af kravet om at gennemføre en konsekvensanalyse)]

Emne	Spørgsmål om anvendelse af AI	Institutionens svar
10. KONSEKVENNS-ANALYSE EFTER AI-FORORDNINGEN (FRIA)	<i>Hvis I er idriftsætter og anvender et højrisiko-AI-system:</i> <i>Har I foretaget en konsekvensanalyse vedrørende grundlæggende rettigheder (FRIA) efter AI-forordningens artikel 27?</i>	[Indsæt ja/nej - (husk I er kun forpligtet til dette, hvis der er tale om et højrisiko-AI-system og I er idriftsættere af systemet)]
11. DEN DATABASE-SKYTTELSESRETTLIGE OPLYSNINGS-PLIGT	<i>Hvis I er dataansvarlig og behandler personoplysninger i forbindelse med anvendelsen af AI-systemet:</i> <i>Har I iagttaget jeres oplysningspligt rettidigt?</i>	[Indsæt ja/nej - (husk I er kun forpligtet til dette, hvis I er dataansvarlige samt, at der er forskel på, hvilke information I skal give til de registrerede afhængigt af, hvem oplysningerne er blevet indsamlet hos)]
12. POLITIKKER, RETNINGSLINJER OG UDDANNELSE M.V.	<i>Har I udarbejdet centrale politikker og retningslinjer for jeres anvendelse af AI-systemer, der sikrer efterlevelse af AI-forordningen og databeskyttelsesforordningen?</i>	[Indsæt ja/nej - Hvis ja, indsæt gerne navnet på jeres politikker/retningslinjer samt en henvisning til, hvor de kan findes]
12.1	<i>Har I sikret jer, at jeres medarbejdere m.fl., som anvender AI-systemerne har de fornødne kompetencer (kravet om AI-færdigheder) og kendskab til de databeskyttelsesretlige regler?</i>	[Indsæt ja/nej - Hvis ja, indsæt gerne en beskrivelse af, hvordan I har sikret dette]
12.2	<i>Vedlæg relevant materiale.</i>	Dette materiale kan være brugsanvisninger og anden dokumentation vedrørende AI-systemet.

Kolofon

Vejledning om lovlig brug af kunstig intelligens for uddannelsesinstitutionerne

Redaktion:

Marie Sofie Dejgaard, Kontor for It-sikkerhed, Sektorsamarbejde og Jura, Børne- og Undervisningsministeriet

Layout:

Børne- og Undervisningsministeriet

Publikationen kan ikke bestilles, men den kan hentes på Børne- og Undervisningsministeriets hjemmeside

Eventuelle henvendelser af indholdsmæssig karakter rettes til stil@stil.dk

Udgivet af:

Børne- og Undervisningsministeriet, 2025

